

[Тема 1. Основы информационной безопасности и защиты информации](#)

[Тема 2. История криптографии](#)

[Тема 3. Основные термины и определения. Классификация шифров](#)

[Тема 4. Шифры замены](#)

[Тема 5. Шифры перестановки](#)

[Тема 6. Шифры гаммирования](#)

[Тема 7. Квантовое шифрование](#)

[Тема 8. Комбинированные шифры](#)

[Тема 9. Шифрование с открытым ключом](#)

[Тема 10. Хеш-функции](#)

[Тема 11. Криптографические протоколы](#)

[Тема 12. Протоколы обмена ключами](#)

[Тема 13. Протоколы аутентификации \(идентификации\)](#)

[Тема 14. Протоколы электронной цифровой подписи](#)

[Тема 15. Протоколы контроля целостности](#)

[Тема 16. Протоколы электронных платежей](#)

[Тема 17. Протоколы голосования](#)

[Тема 18. Протоколы тайных многосторонних вычислений и разделения секрета](#)

[Тема 19. Некоторые сведения из теорий алгоритмов и чисел](#)

[Тема 20. Основы криптоанализа](#)

[Тема 21. Стеганография](#)

[Тема 22. Кодирование информации](#)

[Список литературы](#)

1.1. Информация и информационная безопасность

Информация (лат. informatio — разъяснение, изложение), первоначально — сведения, передаваемые людьми устным, письменным или другим способом с помощью условных сигналов, технических средств и т.д. С середины 20-го века **информация** является общенаучным понятием, включающим в себя:

- сведения, передаваемые между людьми, человеком и автоматом, автоматом и автоматом;
- сигналы в животном и растительном мире;
- признаки, передаваемые от клетки к клетке, от организма к организму;
- и т.д.

Другими словами, информация носит фундаментальный и универсальный характер, являясь многозначным понятием. Эту мысль можно подкрепить словами Н. Винера (отца кибернетики): «Информация есть информация, а не материя и не энергия».

Согласно традиционной философской точке зрения, информация существует независимо от человека и является свойством материи. В рамках рассматриваемой дисциплины, под **информацией** (в узком смысле) мы будем понимать сведения, являющиеся объектом сбора, хранения, обработки, непосредственного использования и передачи в информационных системах¹.

Опираясь на это определение информации, рассмотрим понятия информационной безопасности и защиты информации.

В Доктрине информационной безопасности Российской Федерации под термином **информационная безопасность** понимается состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В более узком смысле, под **информационной безопасностью** мы будем понимать состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений [18].

Защита информации — комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.

Важно отметить, что информационная безопасность — это одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным состоянием (уровнем) защищенности, а защита информации — это процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы².

Рассмотрим более подробно составляющие этих определений.

Под **субъектами информационных отношений** понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры [18].

К **поддерживающей инфраструктуре** относятся не только компьютеры, но и помещения, системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

Ущерб может быть **приемлемым** или **неприемлемым**. Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений [18].

Информационная угроза — потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере, искажению или разглашению информации.

Таким образом, концепция информационной безопасности, в общем случае, должна отвечать на три вопроса:

- Что защищать?
- От чего (кого) защищать?
- Как защищать?

¹**Информационная система** (автоматизированная информационная система) — это совокупность технических (аппаратных) и программных средств, а также работающих с ними пользователей (персонала), обеспечивающая информационную технологию выполнения установленных функций.

²**Жизненный цикл информационной системы** – непрерывный процесс, начинающийся с момента принятия решения о создании информационной системы и заканчивающийся в момент полного изъятия ее из эксплуатации.

1.2. Основные составляющие информационной безопасности

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие составляющие: обеспечение **доступности**, **целостности** и **конфиденциальности** информационных ресурсов и поддерживающей инфраструктуры.

Иногда в число основных составляющих информационной безопасности включают защиту от несанкционированного доступа (НСД) к информации, под которым понимают доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств³. В то же время обеспечение конфиденциальности как раз и подразумевает защиту от НСД.

Дадим определения основных составляющих информационной безопасности [18].

Доступность информации – свойство системы обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними. Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность информации – свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций⁴)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений. Целостность оказывается важнейшим аспектом информационной безопасности в тех случаях, когда информация служит «руководством к действию». Рецепт лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным.

Конфиденциальность информации – свойство информации быть известной и доступной только правомочным субъектам системы (пользователям, программам, процессам). Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность – какой смысл в информационной услуге, если она содержит искаженные сведения? Наконец, конфиденциальная информация есть как у организаций, так и отдельных пользователей.

Из всего выше приведенного следует два следствия.

1. Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные заведения. В первом случае «пусть лучше все сломается, чем враг узнает хотя бы один секрет», во втором – «да нет у нас никаких секретов, лишь бы все работало».

2. Информационная безопасность не сводится исключительно к защите от НСД к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от НСД, но и от поломки системы, вызвавшей перерыв в работе.

³**Штатные средства** - совокупность программного и аппаратного обеспечения рассматриваемой информационной системы.

⁴**Транзакция** - одно действие или их последовательность, выполняемых одним или несколькими пользователями (прикладными программами) с целью осуществления доступа или изменения информации, воспринимаемых как единое целое и переводящих ее из одного непротиворечивого (согласованного) состояния в другое непротиворечивое состояние.

1.3. Объекты защиты

Основными **объектами защиты** при обеспечении информационной безопасности являются:

- все виды информационных ресурсов. **Информационные ресурсы (документированная информация)** - информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать;
- права граждан, юридических лиц и государства на получение, распространение и использование информации;
- система формирования, распространения и использования информации (информационные системы и технологии, библиотеки, архивы, персонал, нормативные документы и т.д.);
- система формирования общественного сознания (СМИ, социальные институты и т.д.).

1.4. Категории и носители информации

Неотъемлемой частью любой информационной системы является информация. По характеру ограничений (реализации) конституционных прав и свобод в информационной сфере выделяют четыре основных **вида правовой** (регламентированной законами) **информации**:

- информация с ограниченным доступом;
- информация без права ограничения;
- иная общедоступная информация (например, за деньги);
- информация, запрещенная к распространению.

Информация с ограниченным доступом делится на государственную тайну и конфиденциальную.

К **государственной тайне** относятся защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. Владельцем государственной тайны является само государство. Требования по защите этой информации и контроль за их соблюдением регламентируются законом РФ «О государственной тайне» [4]. В нем законодательно установлен Перечень сведений, сопоставляющих государственную тайну, и круг сведений, не подлежащих к отнесению к ней. Предусмотрена судебная защита прав граждан в связи с необоснованным засекречиванием. Определены органы защиты государственной тайны:

- межведомственная комиссия по защите государственной тайны;
- федеральные органы исполнительной власти, уполномоченные в области:
 - обеспечения безопасности - Федеральная служба по техническому и экспортному контролю (ФСТЭК);
 - обороны – Министерство обороны;
 - внешней разведки – Федеральная служба безопасности (ФСБ обеспечивает, в т.ч. криптографическую защиту);
 - противодействия техническим разведкам и технической защиты информации – ФСТЭК;
- другие органы.

Конфиденциальная информация – документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности. Этой информацией владеют различные учреждения, организации и отдельные индивидуумы. В Указе Президента РФ «Перечень сведений конфиденциального характера» [5] конфиденциальная информация разбита на семь видов:

- персональные данные;
- тайна следствия и судопроизводства;
- **служебная тайна** - служебная информация ограниченного распространения о госорганах или подведомственных им организациях, а также информация, получаемая из внешних источников работниками госорганов при исполнении обязанностей;
- **профессиональная тайна** - информация, полученная гражданами (физическими лицами) при исполнении ими

профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности [2] (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);

- **коммерческая тайна** - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам;

- сведения о сущности изобретения, полезной модели или промышленного образца по официальной публикации информации о них;

- сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов.

Под **персональными данными** понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Несмотря на то, что это информация ограниченного доступа, она является полностью открытой для субъекта персональных данных. Только сам субъект решает вопрос о передаче, обработке и использовании своих персональных данных, а также определяет круг субъектов, которым эти данные могут быть сообщены. Некоторая часть персональных данных может не иметь режима защиты, являясь общеизвестными (например, фамилия, имя и отчество). В Законе РФ «О персональных данных» [6] выделены следующие **права субъектов персональных данных** (кроме некоторых категорий граждан: владеющих государственной тайной, осужденных и т.д.):

- информационное самоопределение;
- доступ к своим персональным данным;
- внесение изменений в свои персональные данные;
- блокирование персональных данных;
- обжалование неправомерных действий в отношении персональных данных;
- возмещение ущерба.

В статье 24 Конституции РФ [1] предусмотрена защита некоторой части персональных данных - «1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются».

Государственные органы и организации, органы местного самоуправления имеют право на работу с персональными данными в пределах своей компетенции, установленной действующим законодательством, или на основании лицензии. В последнем случае с ними могут работать также негосударственные юридические и физические лица.

В статье 7 Закона РФ «О государственной тайне» [4] определен перечень сведений, не подлежащих отнесению к государственной тайне и засекречиванию (**информация без права ограничения**):

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах Российской Федерации;
- о состоянии здоровья высших должностных лиц Российской Федерации;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут **уголовную, административную или дисциплинарную** ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суд.

В ряде статей Конституции РФ [1] также прописан беспрепятственный доступ граждан и их объединений к общественно значимой информации:

- статья 24 - «2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом»;
- статья 42 - «Каждый имеет право на благоприятную окружающую среду, достоверную информацию о ее состоянии и на возмещение ущерба, причиненного его здоровью или имуществу экологическим правонарушением».

Информация, запрещенная к распространению, определена в многочисленных нормативных документах. В частности:

- статья 29 Конституции РФ - «2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства»;
- Кодекс Российской Федерации об административных правонарушениях:
 - статья 5.61 «Оскорбление»;
 - статья 5.62 «Дискриминация»;
 - статья 6.13 «Пропаганда наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, новых потенциально опасных психоактивных веществ»;
 - статья 6.17 «Нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию»;
 - статья 6.21 «Пропаганда нетрадиционных сексуальных отношений среди несовершеннолетних»;
 - статья 6.26 «Организация публичного исполнения произведения литературы, искусства или народного творчества, содержащего нецензурную брань, посредством проведения театрально-зрелищного, культурно-просветительного или зрелищно-развлекательного мероприятия»;
 - статья 14.48 «Представление недостоверных результатов исследований (испытаний)»;
 - статья 17.9 «Заведомо ложные показания свидетеля, пояснение специалиста, заключение эксперта или заведомо неправильный перевод»;
 - статья 20.3 «Пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами»;
 - статья 20.29 «Производство и распространение экстремистских материалов»;
 - и другие;
- Уголовный кодекс Российской Федерации:
 - статья 110 «Доведение до самоубийства» - «д) в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть "Интернет")»;
 - статья 119 «Угроза убийством или причинением тяжкого вреда здоровью»;
 - статья 128.1 «Клевета»;
 - статья 142 «Фальсификация избирательных документов, документов референдума»;
 - статья 155 «Разглашение тайны усыновления (удочерения)»;
 - статья 172.1 «Фальсификация финансовых документов учета и отчетности финансовой организации»;
 - статья 205.2 «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма»;
 - статья 207 «Заведомо ложное сообщение об акте терроризма»;
 - статья 217.2 «Заведомо ложное заключение экспертизы промышленной безопасности»;
 - статья 242 «Незаконное изготовление и оборот порнографических материалов или предметов»;
 - статья 280 «Публичные призывы к осуществлению экстремистской деятельности»;
 - статья 303 «Фальсификация доказательств и результатов оперативно-розыскной деятельности»;
 - статья 306 «Заведомо ложный донос»;
 - статья 307 «Заведомо ложные показания, заключение эксперта, специалиста или неправильный перевод»;
 - статья 319 «Оскорбление представителя власти»;
 - статья 354 «Публичные призывы к развязыванию агрессивной войны»;
 - статья 354.1 «Реабилитация нацизма»;

- и другие.

Основными **носителями информации** являются:

- открытая печать (газеты, журналы, отчеты, реклама и т.д.);
- люди;
- средства связи (радио, телевидение, телефон, пейджер и т.д.);
- документы (официальные, деловые, личные и т.д.);
- электронные, магнитные и другие носители, пригодные для автоматической обработки данных.

1.5. Средства защиты информации

Принято различать следующие средства защиты:

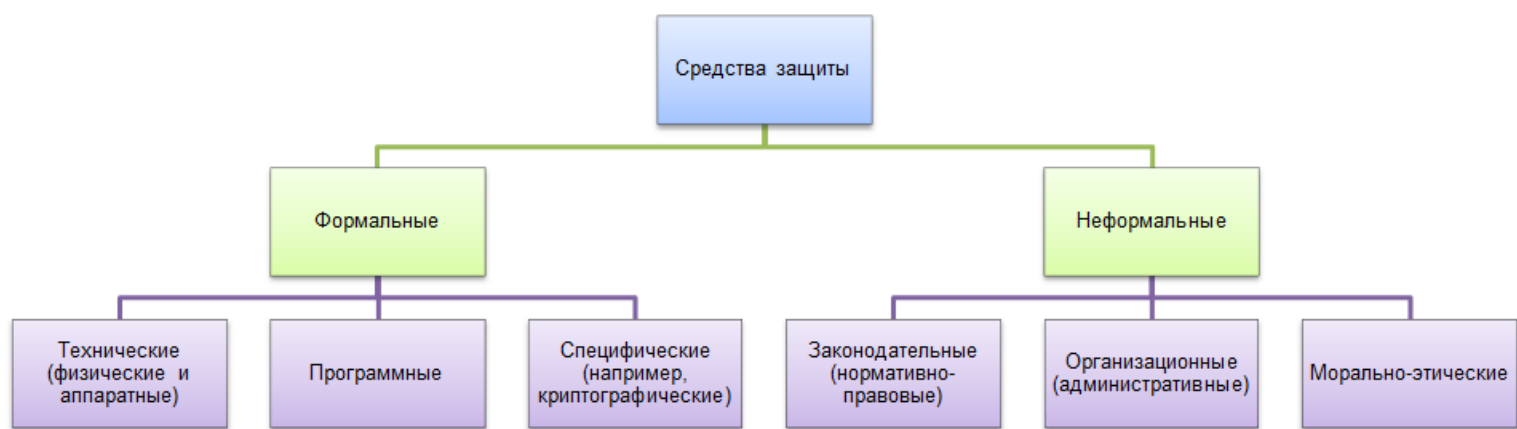


Рис.1.1. Классификация средств защиты

I. Формальные средства защиты – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.

Физические средства - механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно от информационных систем, создавая различного рода препятствия на пути дестабилизирующих факторов (замок на двери, жалюзи, забор, экраны).

Аппаратные средства - механические, электрические, электромеханические, электронные, электронно-механические, оптические, лазерные, радиолокационные и тому подобные устройства, встраиваемые в информационных системах или сопрягаемые с ней специально для решения задач защиты информации.

Программные средства - пакеты программ, отдельные программы или их части, используемые для решения задач защиты информации. Программные средства не требуют специальной аппаратуры, однако они ведут к снижению производительности информационных систем, требуют выделения под их нужды определенного объема ресурсов и т.п.

К **специфическим средствам** защиты информации относятся криптографические методы. В информационных системах криптографические средства защиты информации могут использоваться как для защиты обрабатываемой информации в компонентах системы, так и для защиты информации, передаваемой по каналам связи. Само преобразование информации может осуществляться аппаратными или программными средствами, с помощью механических устройств, вручную и т.д.

II. Неформальные средства защиты – регламентируют деятельность человека.

Законодательные средства – законы и другие нормативно-правовые акты, с помощью которых регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Распространяются на всех субъектов информационных отношений. В настоящее время отношения в сфере информационной безопасности регулируются более чем 80 законами и нормативными документами, иногда достаточно противоречивыми.

Организационные средства - организационно-технические и организационно-правовые мероприятия, осуществляемые в течение всего жизненного цикла защищаемой информационной системы (строительство помещений, проектирование информационных систем, монтаж и наладка оборудования, испытания и эксплуатация информационных систем). Другими словами – это средства уровня организации, регламентирующие перечень лиц, оборудования, материалов и т.д., имеющих отношение к информационным системам, а также режимов их работы и использования. К организационным мерам также относят сертификацию информационных систем или их элементов, аттестацию объектов и субъектов на выполнение требований обеспечения безопасности и т.д.

Морально-этические средства - сложившиеся в обществе или в данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе, ведет к потере престижа и авторитета. Наиболее показательные пример – кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США.

1.6. Способы передачи конфиденциальной информации на расстоянии

Способов передачи конфиденциальной информации на расстоянии существует множество, среди которых можно выделить три основных направления [9].

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами.
2. Использовать общедоступный канал связи, но скрыть сам факт передачи информации.
3. Использовать общедоступный канал связи, но передавать по нему нужную информацию в таком преобразованном виде, чтобы восстановить ее мог только адресат.

Проанализируем эти возможности.

1. С древних времен практиковалась охрана документа (носителя информации) физическими лицами, передача его специальным курьером (человеком (дипломатом) или животным (голубиная почта)) и т.д. Но, документ можно выкрасть, курьера можно перехватить, подкупить, в конце концов, убить. В настоящий момент для реализации данного механизма защиты используются современные телекоммуникационные каналы связи. Однако следует заметить, что данный подход требует значительных капитальных вложений. При современном уровне развития науки и техники сделать такой канал связи между удаленными абонентами для многократной передачи больших объемов информации практически нереально.
2. Разработкой средств и методов скрытия факта передачи сообщения занимается **стеганография**. Первые следы стеганографических методов теряются в глубокой древности. Так, в трудах древнегреческого историка Геродота встречается описание двух методов сокрытия информации: на обритуемую голову раба записывалось необходимое сообщение, а когда его волосы отрастали, он отправлялся к адресату, который вновь брил его голову и считывал доставленное сообщение. Второй способ заключался в следующем: сообщение наносилось на деревянную дощечку, а потом она покрывалась воском, и, тем самым, не вызвала никаких подозрений. Потом воск соскабливался, и сообщение становилось видимым. В настоящий момент стеганографические методы в совокупности с криптографическими нашли широкое применение в целях сокрытия и передачи конфиденциальной информации.
3. Разработкой методов преобразования информации с целью ее защиты от несанкционированного прочтения занимается **криптография**.

Вопросы для самопроверки

1. Дайте определение понятиям: «информация», «информационная безопасность», «защита информации», «информационная угроза».
2. Дайте характеристику основным составляющим информационной безопасности.
3. Перечислите основные объекты защиты.
4. Дайте характеристику понятиям «государственная тайна», «конфиденциальная информация» и «персональные данные».
5. Дайте характеристику средствам защиты информации.
6. Перечислите способы тайной передачи информации на расстоянии.

2. ИСТОРИЯ КРИПТОГРАФИИ

2.1. Введение

В истории развития криптографии можно выделить три этапа [11]:

- наивная криптография;
- формальная криптография;
- математическая криптография.

2.2. Наивная криптография

О важности сохранения информации в тайне знали уже в древние времена, когда с появлением письменности появилась и опасность прочтения ее нежелательными лицами. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. С широким распространением письменности криптография стала формироваться как самостоятельная наука. В документах древних цивилизаций - Индии, Египта, Месопотамии - есть сведения о системах и способах составления шифрованных писем.[9].

Для наивной криптографии (до начала XVI в.) характерно использование любых, обычно примитивных, способов запутывания противника относительно содержания передаваемых сообщений. На начальном этапе для защиты информации использовались методы кодирования и стеганографии, которые родственны криптографии. Шифровальные системы сводились к использованию перестановки или замены букв на различные символы (другие буквы, знаки, рисунки, числа и т.п.). Один и те же способы шифрования использовались повторно, ключи были короткими, использовались примитивные способы преобразования исходной информации в зашифрованное сообщение. Это позволяло, однажды установив алгоритм шифрования, быстро расшифровывать сообщения.

[43] Точное время возникновения этих способов обмена тайной информацией теряется в глубине веков, и установить его невозможно. Историки полагают, что первые протокриптографические приемы появились в Древнем Египте около 4 тыс. лет назад. Писцы, составлявшие жизнеописания правителей, стремились придать стандартным иероглифам необычный вид на монументах и гробницах, чтобы сообщить надписям менее обыденный и более почтительный стиль. Жрецы пользовались этим же приемом при переписывании религиозных текстов, чтобы те выглядели для мирян загадочнее и внушительнее. Такие «переводы» становились все менее понятными простому люду, который в результате оказывался во все большей зависимости от жрецов.

По мере развития египетской цивилизации ширилось использование иероглифов. С увеличением количества надписей, высеченных на стенах храмов, люди теряли к ним интерес. Египтологи считают, что писцы тогда стали еще больше видоизменять некоторые знаки в стремлении пробудить любопытство и привлечь внимание населения. Эти модификации никоим образом не были кодами или шифрами, но они заключали в себе два основных принципа криптологии, а именно: изменение письма и сокрытие его смысла. Бесспорных доказательств, указывающих на широкое использование модификаций иероглифов для сокрытия дипломатических, торговых или военных планов в Древнем Египте, нет.

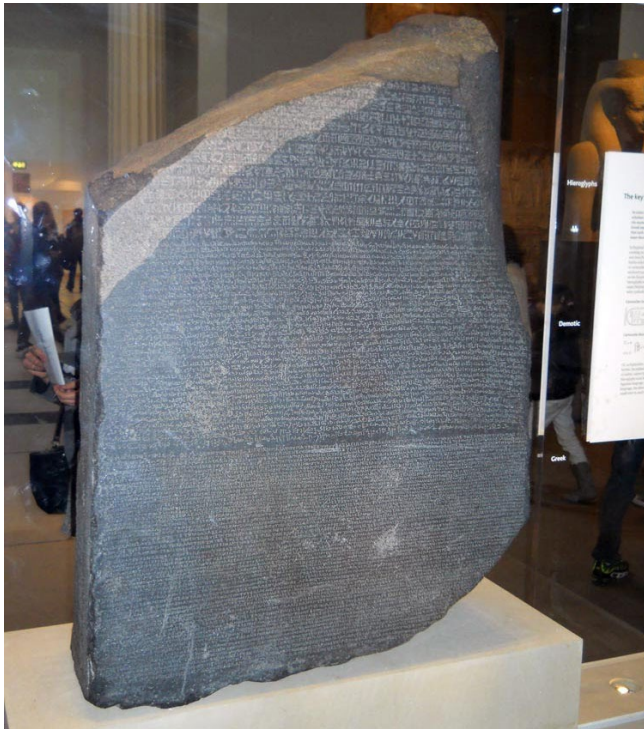


Рис.2.1. Розеттский камень¹

Более явные криптологические примеры дошли до нас от цивилизаций Месопотамии — от вавилонян, ассирийцев, халдеев, использовавших особую систему письма — клинопись. В 1500 г. до н. э. на глиняной табличке был записан тщательно охраняемый рецепт глазури для гончарных изделий. Знаки, определяющие необходимые ингредиенты, были намеренно перемешаны. Таким образом, мы имеем право утверждать, что эта табличка является самой ранней известной секретной записью.

Примерно с 500 г. до н. э. в Индии также широко применялись секретные записи, в частности в доведениях шпионов и текстах, предположительно использовавшихся Буддой. Методы засекречивания включали в себя фонетическую замену, когда согласные и гласные менялись местами, использование перевернутых букв и запись текста под случайными углами. Различные индийские трактаты, ярким примером которых является «Артхашастра» (около 321—300 гг. до н. э.), показывают, что индийцы были хорошо знакомы со способами сокрытия информации. Согласно «Камасутре», классическому произведению об эротике и других видах наслаждений, написанному Ватсаяной около IV в. до н.э., владение приемами составления секретного письма (наряду с музыкой, кулинарией и шахматами) является одним из 64 искусств, которыми должны владеть женщины.

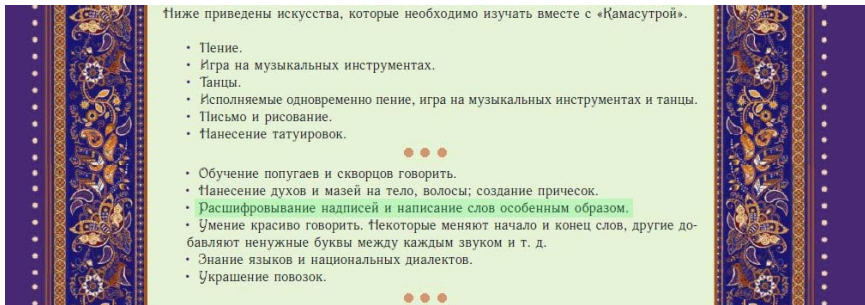


Рис.2.2. Фрагмент «Камасутры»

Одним из первых, документально зафиксированных примеров является **шифр Цезаря**, состоящий в замене каждой буквы исходного текста на другую, отстоящую от нее в алфавите на определенное число позиций. Другой шифр, **полибианский квадрат**, авторство которого приписывается греческому писателю Полибию, является шифром простой однозначной замены. В квадрат выписывались буквы алфавита (для греческого алфавита размер составлял 5x5). Каждая буква исходного текста заменялась на пару цифр – номер строки и столбца на пересечении которых стояла шифруемая буква.

С VIII века н. э. развитие криптографии происходит в основном в арабских странах. Считается, что арабский филолог Халиль аль-Фарахиди первым обратил внимание на возможность использования стандартных фраз открытого текста для дешифрования. Он предположил, что первыми словами в письме на греческом языке византийскому императору будут «Во имя Аллаха», что позволило ему прочитать оставшуюся часть сообщения. Позже он написал книгу с описанием данного метода — «Китаб аль-Муамма» («Книга тайного языка») [17]. В 855 г. выходит «Книга о большом стремлении человека разгадать загадки древней письменности» арабского учёного Абу Бакр Ахмед ибн Али Ибн Вахшия ан-Набати, одна из первых книг о криптографии с описаниями нескольких шифров, в том числе с применением нескольких алфавитов. Также к IX веку относится первое известное упоминание о частотном криптоанализе — в книге Аль-Kindи «Манускрипт о дешифровке криптографических сообщений». В 1412 г. выходит 14-томная энциклопедия Шихаба ал-Калкашанди «Субх ал-Ааша», один из разделов которой «Относительно сокрытия в буквах тайных сообщений» содержит описание семи шифров замены и перестановки, частотного криптоанализа, а также таблицы частоты появления букв в арабском языке на основе текста Корана. В словарь криптологии арабы внесли такие понятия как алгоритм и шифр.

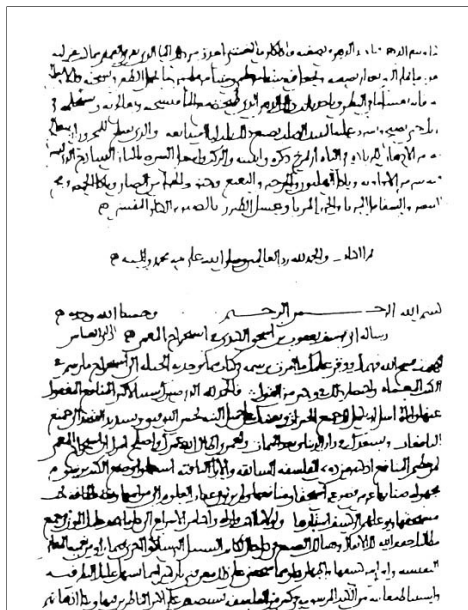


Рис.2.3. Фрагмент первой страницы «Манускрипта о дешифровке криптографических сообщений» Аль-Кинди

В древние времена широкое применение нашли различные простейшие криптографические устройства.

Греческим поэтом Архилохом, жившим в VII веке до н.э., упоминается устройство под названием **сцитала** (греч. σκυτάλη - жезл). Достоверно известно, что сцитала использовалась в войне Спарты против Афин в конце V века до н. э. Оно представляет собой цилиндр (иногда жезл командующего) и узкую полоску пергамента, обмотавшуюся вокруг него по спирали, на которой в свою очередь писалось сообщение [17].



Рис.2.4. Сцитала

Шифруемый текст писался на пергаментной ленте по длине палочки, после того как длина палочки оказывалась исчерпанной, она поворачивалась и текст писался далее, пока либо не заканчивался текст, либо не исписывалась вся пергаментная лента. В последнем случае использовался очередной кусок пергаментной ленты. Для расшифровки адресат использовал палочку такого же диаметра, на которую он наматывал пергамент, чтобы прочитать сообщение. Античные греки и спартанцы в частности, использовали этот шифр для связи во время военных кампаний. Однако такой шифр может быть легко взломан. Например, метод взлома сциталы был предложен ещё Аристотелем. Он состоит в том, что не зная точного диаметра палочки, можно использовать конус, имеющий переменный диаметр и перемещать пергамент с сообщением по его длине до тех пор, пока текст не начнёт читаться - таким образом дешифруется диаметр сциталы.

Другим широко известным криптографическим устройством защиты информации был **«диск Энея»** - инструмент для защиты информации, придуманный Энесом Тактиком в IV веке до н.э. Устройство представляло собой диск диаметром 13-15 см и толщиной 1-2 см с проделанными в нём отверстиями, количество которых равнялось числу букв в алфавите. Каждому отверстию ставилась в соответствие конкретная буква. В центре диска находилась катушка с намотанной на неё ниткой [17].

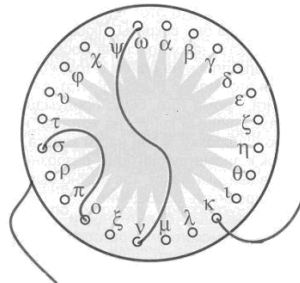


Рис.2.5. Диск Энея

Механизм шифрования был очень прост. Для того, чтобы зашифровать послание, необходимо было поочерёдно протягивать свободный конец нити через отверстия обозначающие буквы исходного не зашифрованного сообщения. В итоге, сам диск, с прорезой в его отверстия ниткой, и являлся зашифрованным посланием. Получатель сообщения последовательно вытягивал нить из каждого отверстия, тем самым получал последовательность букв. Но эта последовательность являлась обратной по отношению к исходному сообщению, то есть он читал сообщение наоборот. Зашифрованное сообщение было доступно к прочтению любому, кто смог завладеть диском. Так как сообщение предавали обычные гонимы, а не воины, Эней предусмотрел возможность быстрого уничтожения передаваемой информации. Для этого было достаточно вытянуть всю нить за один из её концов, либо сломать диск, просто наступив на него. На самом деле «диск Энея» нельзя назвать настоящим криптографическим инструментом, поскольку прочитать сообщение мог любой желающий. Но это устройство стало прародителем первого по истине криптографического инструмента, изобретение которого также принадлежит Энею.

Прибор получил название **«Линейка Энея»**. Она представляла собой устройство, имеющее отверстия, количество которых равнялось количеству букв алфавита. Каждое отверстие обозначалось своей буквой; буквы по отверстиям располагались в произвольном порядке. К линейке была прикреплена катушка с намотанной на неё ниткой. Рядом с катушкой имелась прорезь. При шифровании нить протягивалась через прорезь, а затем через отверстие, соответствующее первой букве шифруемого текста, при этом на нити завязывался узелок в месте прохождения её через отверстие; затем нить возвращалась в прорезь и аналогично зашифровывалась вторая буква текста и т. д. После окончания шифрования нить извлекалась и передавалась получателю сообщения. Получатель, имея идентичную линейку, протягивал нить через прорезь до отверстий, определяемых узлами, и восстанавливал исходный текст по буквам отверстий. Такой шифр является одним из примеров шифра замены: когда буквы заменяются на расстояния между узелками с учетом прохождения через прорезь. Ключом шифра являлся порядок расположения букв по отверстиям в линейке. Посторонний, получивший нить (даже имея линейку, но без нанесенных на ней букв), не сможет прочитать передаваемое сообщение.

¹**Розеттский камень** - плита из гранодиорита, найденная в 1799 г. в Египте возле небольшого города Розетта (теперь Рашид), недалеко от Александрии, с выбитыми на ней тремя идентичными по смыслу текстами, в том числе двумя на древнеегипетском языке и одним на древнегреческом языке. Древнегреческий был хорошо известен лингвистам, и сопоставление трёх текстов послужило отправной точкой для расшифровки египетских иероглифов.

2.3. Формальная криптография

Этап формальной криптографии (конец XV – начало XX вв.) связан с появлением формализованных и относительно стойких к ручному криптоанализу шифров. В европейских странах это произошло в эпоху Возрождения, когда развитие науки и торговли вызвало спрос на надежные способы защиты информации.

К концу XIV в. между итальянскими городами-государствами в переписке уже применялись **«номенклаторы»**² (лат. nomen — «имя» и salator — «раб», «слуга»). Они состояли из кодовых обозначений для слогов, слов и имен, а также алфавитов шифрофразем. Вплоть до XIX в. номенклаторы оставались самой широко используемой системой сокрытия содержания сообщений [43].

Симеоне де Крема (Simeone de Crema) был первым (1401 г.), кто использовал таблицы омофонов для сокрытия частоты появления гласных в тексте при помощи более чем одной шифрозамены (**шифры многозначной замены**).

Отцом западной криптографии называют учёного эпохи Возрождения Леона Баттисту Альберти. Изучив методы вскрытия использовавшихся в Европе моноалфавитных шифров (**шифры однозначной замены**), он попытался создать шифр, который был бы устойчив к частотному криптоанализу. Его «Трактат о шифрах» был представлен в папскую канцелярию в 1466 г. и считается первой научной работой по криптографии. Он предложил вместо единственного секретного алфавита, как в моноалфавитных шифрах, использовать два или более, переключаясь между ними по какому-либо правилу (полиалфавитные шифры).

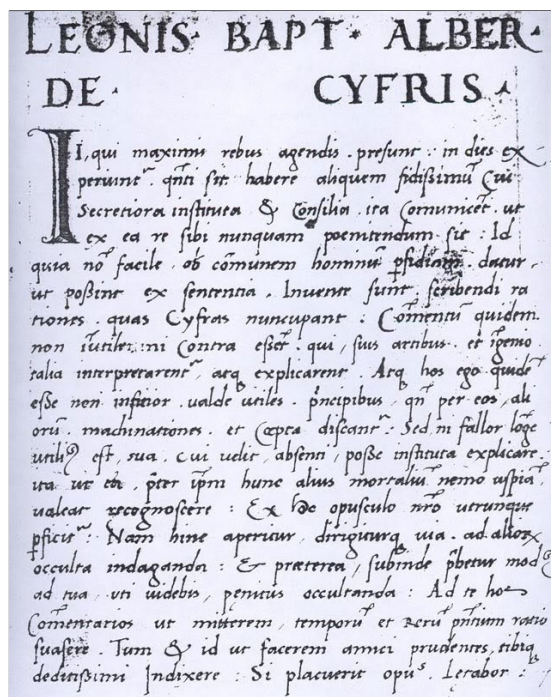


Рис.2.6. Фрагмент первой страницы «Трактата о шифрах» Леона Баттисто Альберти

Однако флорентийский учёный так и не смог оформить своё открытие в полную работающую систему, что было сделано уже его последователями (Блез Виженер).

Другой работой, в которой обобщены и сформулированы известные на тот момент алгоритмы шифрования, является труд «Полиграфия» (1518 г.) немецкого аббата Иоганна Трисемуса (Тритемия). Он же первым заметил, что шифровать можно и по две буквы за раз - биграммами (хотя первый **биграммный шифр** Playfair был предложен лишь в XIX веке).

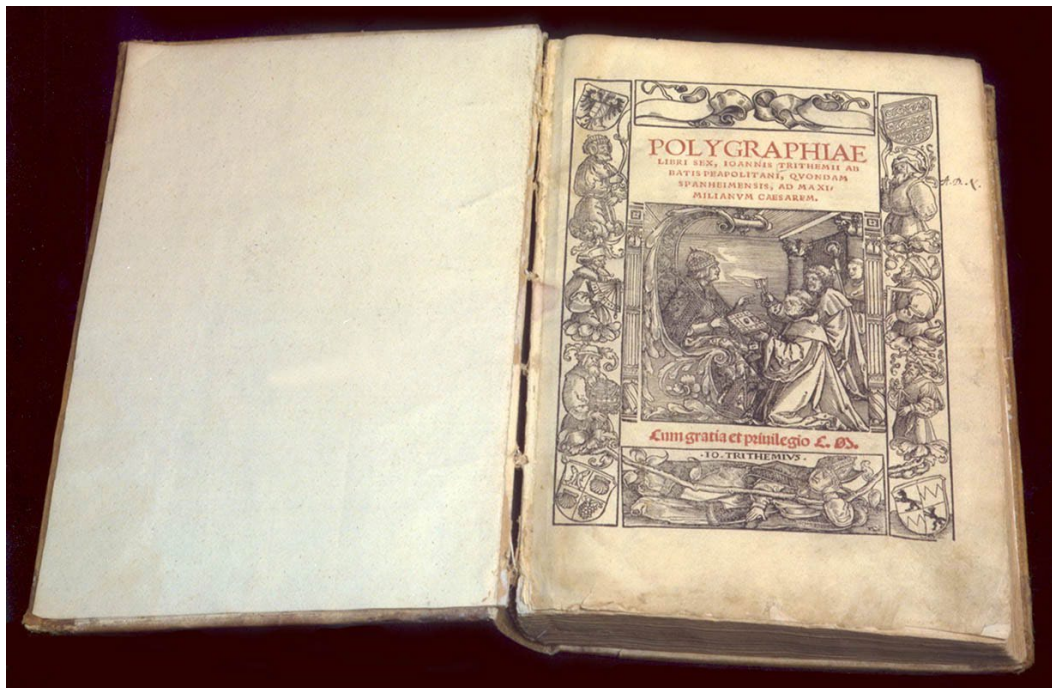


Рис.2.7. Первый печатный труд по криптографии - «Полиграфия» Иоганна Трисемуса [Национальный музей криптографии, США]

В 1550 г. итальянский математик Джероламо Кардано, состоявший на службе у папы римского, предложил новую технику шифрования - решётку Кардано. Этот способ сочетал в себе как стеганографию (искусство скрытого письма), так и криптографию. Затруднение составляло даже понять, что сообщение содержит зашифрованный текст, а расшифровать его, не имея ключа (решётки) в то время было практически невозможно. Решётку Кардано считают первым **транспозиционным шифром**, или, как ещё называют, геометрическим шифром, основанным на положении букв в шифротексте.

Значительный толчок криптографии дало изобретение телеграфа. Сама передача данных перестала быть секретной, и сообщение, в теории, мог перехватить кто угодно. Интерес к криптографии возрос, в том числе, и среди простого населения, в результате чего многие попытались создать индивидуальные системы шифрования. Преимущество телеграфа было явным и на поле боя, где командующий должен был отдавать немедленные приказы на поле сражения, а также получать информацию с мест событий. Это послужило толчком к развитию полевых шифров.

В 1863 г. Фридрих Касиски (англ. Friedrich Kasiski) опубликовал метод, впоследствии названный его именем, позволявшим быстро и эффективно вскрывать практически любые шифры того времени, в т.ч. полнalfавитные. Метод состоял из двух частей - определение периода шифра и дешифровка текста с использованием частотного криптоанализа.



Рис.2.8. Титульный лист «Тайнописи и искусства дешифрования» Фридриха Касиски

В 1883 г. голландец Огюст Керкгоффс³ опубликовал труд под названием «Военная криптография» (фр. «La Cryptographie Militaire»). В нём он описал шесть требований, которым должна удовлетворять защищённая система. Хотя к некоторым из них стоит относиться с подозрением, стоит отметить труд за саму попытку:

1. шифр должен быть физически, если не математически, нескрываемым;
2. система не должна требовать секретности, на случай, если она попадёт в руки врага;
3. ключ должен быть простым, храниться в памяти без записи на бумаге, а также легко изменяемым по желанию корреспондентов;
4. зашифрованный текст должен (без проблем) передаваться по телеграфу;
5. аппарат для шифрования должен быть легко переносимым, работа с ним не должна требовать помощи нескольких лиц;
6. аппарат для шифрования должен быть относительно прост в использовании, не требовать значительных умственных усилий или соблюдения большого количества правил.

Им же был сформулирован известный «**принцип Керкгоффса**» - правило разработки криптографических систем, согласно которому в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен быть открытым. Другими словами, при оценке надёжности шифрования необходимо предполагать, что противник знает об используемой системе шифрования всё, кроме применяемых ключей.

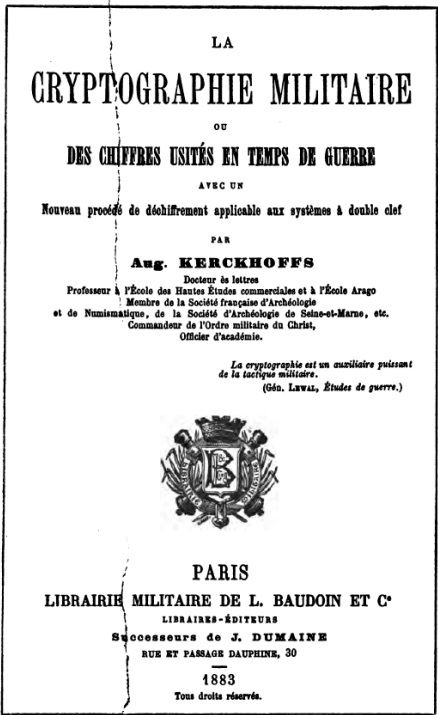


Рис.2.9. Титульный лист брошюры «Военная криптография» Огюста Керкгоффса

В 1920 г. вышла монография американского криптографа российского происхождения Уильяма Ф. Фридмана «Индекс совпадения и его применение в криптографии» (англ. «Index of Coincidence and Its Applications in Cryptography»). Работа вышла в открытой печати, несмотря на то, что была выполнена в рамках военного заказа. Два года позже Фридман ввёл в научный обиход термины **криптология** и **криптоанализ** [13].

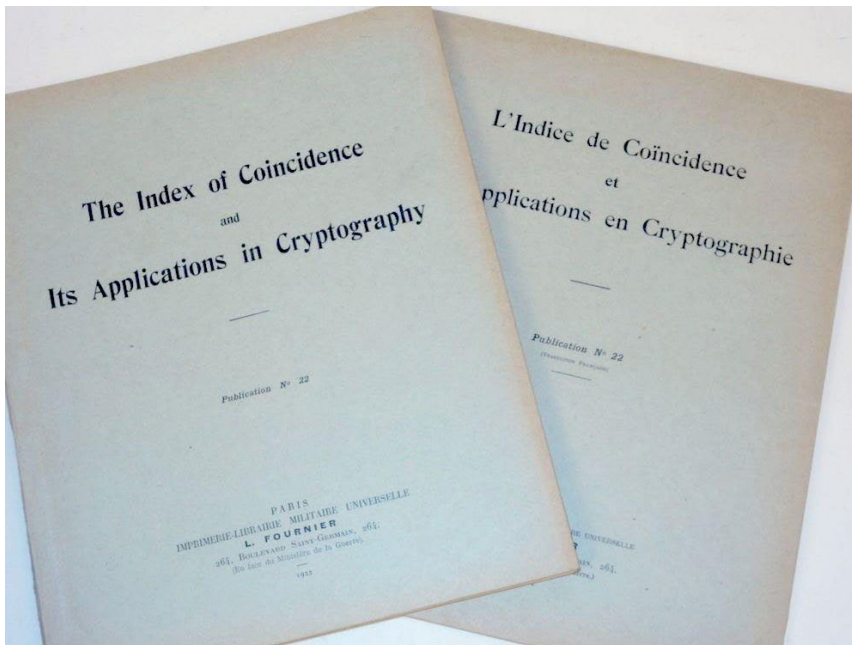


Рис.2.10. «Индекс совпадения и его применение в криптографии» Уильяма Фридмана

Криптография оказала влияние и на **литературу**. Упоминания о криптографии встречаются ещё во времена Гомера и Геродота, хотя они описывали искусство шифрования в контексте различных исторических событий. Первым вымышленным упоминанием о криптографии можно считать роман «Гаргантюа и Пантагрюэль» французского писателя XVI века Франсуа Рабле, в одной из глав которого описываются попытки чтения зашифрованных сообщений. Упоминание встречается и в «Генрих V» Шекспира. Впервые как центральный элемент художественного произведения криптография используется в рассказе «Золотой жук» Эдгара Аллана По 1843 г. В нём писатель не только показывает способ раскрытия шифра, но и результат, к которому может привести подобная деятельность - нахождение спрятанного сокровища. Одним из лучших описаний применения криптографии является рассказ 1903 г. Артура Конан Дойля «Пляшущие человечки». В рассказе великий сыщик Шерлок Холмс сталкивается с разновидностью шифра, который не только прячет смысл написанного, но, используя символы, похожие на детские картинки, скрывает сам факт передачи секретного сообщения. В рассказе герой успешно применяет частотный анализ, а также предположения о структуре и содержании открытых сообщений для разгадывания шифра.

Перед началом Второй мировой войны ведущие мировые державы имели электромеханические шифрующие устройства, результат работы которых считался невскрываемым. Эти устройства делились на два типа - роторные машины и машины на цевочных дисках. К первому типу относят «Энигму», использовавшуюся войсками Германии и её союзников, второго типа - американская **M-209**. В СССР производились оба типа машин.



Энигма 1
(Германия)



M-209
(США)



Коралл
(СССР)

Рис.2.11. Шифровальные устройства [en.wikipedia.org, www.cryptomuseum.com]

Успешные криптоатаки на подобного рода криптосистемы стали возможны только с появлением ЭВМ.

²Первоначально **номенклатором** назывался раб, который обязан был знать и называть своему господину имена граждан города и всех рабов в доме, а также провозглашать названия подаваемых кушаний.

³Огюст Керкгоффс (Auguste Kerckhoffs, 1835 - 1903 гг.) - голландский лингвист и криптограф, профессор Парижской высшей школы коммерции во второй половине XIX века. В русских источниках встречаются разные переводы фамилии - Керкхофф, Киркгоф, Керкгоффс, Керхофс, Керкхоффс. Полное имя, полученное при крещении, - Жан Вильгельм Губерт Виктор Франсуа Александр Огюст Керкгоффс фон Ниувенгоф [17, 43].

2.4. Математическая криптография

После Первой мировой войны правительства стран засекретили все работы в области криптографии. К началу 1930-х годов окончательно сформировались разделы математики, являющиеся основой для будущей науки: общая алгебра, теория чисел, теория вероятностей и математическая статистика. К концу 1940-х годов построены первые программируемые счётные машины, заложены основы теории алгоритмов, кибернетики. Тем не менее, в период после Первой мировой войны и до конца 1940-х годов в открытой печати было опубликовано совсем немного работ и монографий, но и те отражали далеко не самое актуальное состояние дел. Наибольший прогресс в криптографии достигается в военных ведомствах.

Ключевой вехой в развитии криптографии является **фундаментальный труд** Клода Шеннона «Теория связи в секретных системах» (англ. Communication Theory of Secrecy Systems) - секретный доклад, представленный автором в 1945 г., и опубликованный им в «Bell System Technical Journal» в 1949 г. В этой работе, по мнению многих современных криптографов, был впервые показан подход к криптографии в целом как к математической науке.

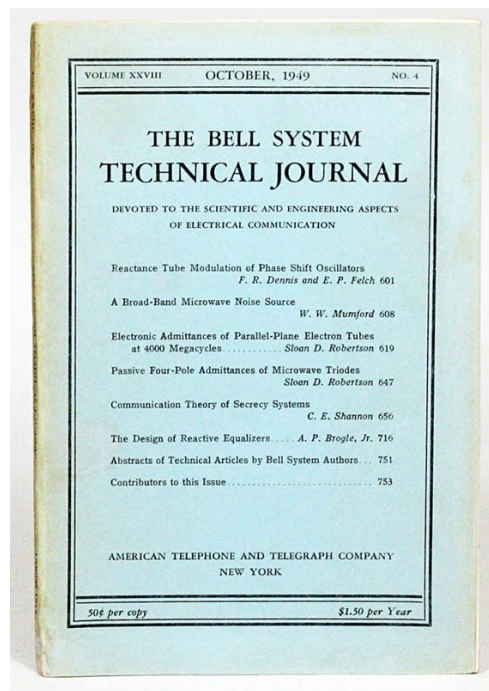


Рис.2.12. Сборник со статьей «Теория связи в секретных системах» Клода Шеннона

В 1960-х годах начали появляться различные блочные шифры, которые обладали большей криптостойкостью по сравнению с результатом работы роторных машин. Однако они предполагали обязательное использование цифровых электронных устройств - ручные или полумеханические способы шифрования уже не использовались.

В 1967 г. выходит книга Дэвида Кана «Взломщики кодов». Хотя книга не содержала сколько-нибудь новых открытий, она подробно описывала имеющиеся на тот момент результаты в области криптографии, большой исторический материал, включая успешные случаи использования криптоанализа, а также некоторые сведения, которые правительство США полагало всё ещё секретными. Но главное - книга имела заметный коммерческий успех и познакомила с криптографией десятки тысяч людей. С этого момента начали понемногу появляться работы и в открытой печати.

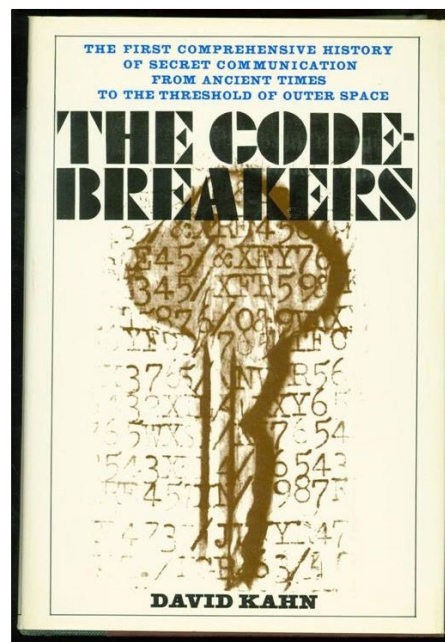


Рис.2.13. Обложка первого издания «Взломщиков кодов» Дэвида Кана

Примерно в это же время Хорст Фейстель переходит из Военно-воздушных сил США на работу в лабораторию корпорации IBM. Там он занимается разработкой новых методов в криптографии и разрабатывает **ячейку Фейстеля**, являющуюся основой многих современных шифров, в том числе шифра Lucifer, ставшего прообразом шифра DES – бывшего стандарта шифрования США, первого в мире открытого государственного стандарта на шифрование данных. На основе ячейки Фейстеля были созданы и другие блочные шифры, в том числе TEA (1994 г.), Twofish (1998 г.), IDEA (2000 г.), а также бывший (ГОСТ 28147-89) и действующий (ГОСТ 34.12-2015) российские стандарты шифрования.

В 1976 г. публикуется работа Уитфилда Диффи и Мартина Хеллмана «Новые направления в криптографии» (англ. «New Directions in Cryptography»). Данная работа открыла новую область в криптографии, теперь известную как **криптография с открытым ключом**. Также в работе содержалось описание алгоритма Диффи - Хеллмана - Меркла, позволявшего сторонам генерировать общий секретный ключ, используя открытый канал связи.

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

The development of computer controlled communication networks promises effortless and inexpensive contact

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D , such that computing D from E is computationally infeasible (e.g., requiring 10^{30} instructions). The en-iphering key E can thus be publicly disclosed without compromising the deciphering key D . Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enciphered in such a way that only the intended receiver is able to decipher it. As such, a public key cryptosystem is a

Рис.2.14. Начало статьи «Новые направления в криптографии» Уитфилда Диффи и Мартина Хеллмана

Хотя работа Диффи-Хеллмана создала большой теоретический задел для открытой криптографии, первой реальной криптосистемой с открытым ключом считают алгоритм RSA (названный по имени авторов - Рон Ривест (R. Rivest), Ади Шамир (A. Shamir) и Леонард Адлеман (L. Adleman)). Опубликованная в августе 1977 г., работа позволила сторонам обмениваться секретной информацией, не имея заранее выбранного секретного ключа. Стоит отметить, что и алгоритм Диффи - Хеллмана - Меркла, и RSA были впервые открыты в английских спецслужбах, но не были ни опубликованы, ни запатентованы из-за секретности.

В России для шифрования с открытым ключом стандарт отсутствует, однако для электронной цифровой подписи (органически связанной с шифрованием с открытым ключом) принят ГОСТ Р 34.10-2001 (ГОСТ Р 34.10-2012), использующий криптографию на эллиптических кривых.

Создание асимметричных криптосистем подтолкнуло математиков и криптоаналитиков к изучению способов факторизации, дискретного логарифмирования, операций над эллиптическими кривыми в конечном поле и т.д.

Относительно новым методом является **вероятностное шифрование**. Вероятностное шифрование предложили Шафи Гольдвассер (Goldwasser) и Сильвио Микали (Micali). Шифрование было названо «вероятностным» в связи с тем, что один и тот же исходный текст при шифровании с использованием одного и того же ключа может преобразовываться в совершенно различные шифротексты. При использовании криптосистем с открытым ключом существует возможность подбора открытого текста сопоставлением перехваченного шифротекста с результатом шифрования. Вероятностное шифрование позволяет на порядки увеличить сложность такого вида атаки.

Чарльз Беннет (Charles Bennett) и Жиль Брассард (Gilles Brassard), опираясь на работу Стивена Уиснера (Stephen Wiesner), разработали теорию **квантовой криптографии**, которая базируется скорее на квантовой физике, нежели на математике. Процесс отправки и приёма информации выполняется посредством объектов квантовой механики (например, при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи). Основанная на принципах квантовой механики, эта система, в отличие от обычной криптографии, теоретически позволяет гарантированно защитить информацию от злоумышленника, даже если тот обладает самой современной технологией и неограниченными вычислительными мощностями. На данный момент, разрабатываются только прототипы квантовых криптосистем.

В то же время эффекты квантовой физики, возможно, смогут использоваться и для криптоанализа. Если будут построены квантовые компьютеры, то это поставит под вопрос существование современной криптографии.

Применение криптографии в решении вопросов аутентификации, целостности данных, передачи конфиденциальной информации по каналам связи и т.п. стало неотъемлемым атрибутом информационных систем. В современном мире криптография находит множество различных применений - она используется в сотовой связи, платном цифровом телевидении, при подключении к Wi-Fi, для защиты билетов от подделок на транспорте, в банковских операциях, в системах электронных платежей и т.д.

Вопросы для самопроверки

1. Назовите основные этапы развития криптографии.

3. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ. КЛАССИФИКАЦИЯ ШИФРОВ

3.1. Основные термины и определения

Одно из основных понятий криптографии - шифр (араб. صفر (sifr) - «ноль», «ничто», «пустота», откуда фр. chiffre - «цифра»; арабы первыми стали заменять буквы на цифры с целью защиты исходного текста).

Под **шифром** понимается совокупность методов и способов обратимого преобразования информации с целью ее защиты от несанкционированного доступа (обеспечения конфиденциальности информации).

Составными элементами шифра являются:

- алфавиты для записи исходных сообщений (защищаемой информации, открытого текста) и шифрованных сообщений (шифртекстов, шифрограмм, криптограмм);
- алгоритмы криптографического преобразования (зашифрования и дешифрования);
- множество ключей.

Азбука или **алфавит** (греч. ἀλφάβητος) - форма письменности, основанная на стандартном наборе знаков, один или набор которых соответствуют фонемам¹ языка. В общем случае **алфавит для записи исходных сообщений** и **алфавит для записи шифрованных сообщений** могут отличаться. Например, исходные сообщения записываются с помощью букв, а шифрограммы с помощью цифр или графических обозначений.

Алгоритм криптографического преобразования — набор правил (инструкций), определяющих содержание и порядок операций по шифрованию и дешифрованию информации.

Шифрование (зашифрование) — процесс применения шифра к защищаемой информации, т.е. преобразование исходного сообщения в зашифрованное.

Дешифрование (расшифрование) — процесс, обратный шифрованию, т. е. преобразование шифрованного сообщения в исходное.

Алгоритмы шифрования и зашифрования, как правило, отличаются друг от друга, но могут и совпадать. В частности, в некоторых комбинированных блочных шифрах (DES, ГОСТ 28147-89) алгоритмы совпадают, но отличаются порядком использования ключа (ключевых элементов). Алгоритм шифрования может включать в себя предварительное кодирование, а алгоритм расшифрования - обратное перекодирование. Например, в аддитивных шифрах перед шифрованием буквы (символы) исходного сообщения заменяются на числа, а результат расшифрования в виде чисел преобразуется в буквы (символы). Аналогичная ситуация имеет место и в некоторых шифрах замены (шифр Хилла), комбинированных блочных шифрах, асимметричных шифрах.

Ключ — переменный параметр шифра, обеспечивающий выбор одного преобразования из совокупности всевозможных для данного алгоритма и сообщения. В общем случае, **ключ** — это минимально необходимая информация (за исключением сообщения, алфавитов и алгоритма), необходимая для шифрования и дешифрования сообщений.

Используя понятие ключа, процессы шифрования и дешифрования можно описать в виде соотношений:

$$f(P, k_1) = C, \quad (3.1)$$

$$g(C, k_2) = P, \quad (3.2)$$

где P (англ. public - открытый) - открытое сообщение;
C (англ. cipher - шифрованный) - шифрованное сообщение;
f - алгоритм шифрования;
g - алгоритм расшифрования;
k₁ — ключ зашифрования, известный отправителю;
k₂ — ключ расшифрования, известный адресату.

В настоящее время разработкой методов шифрования и дешифрования информации (в т.ч. и без знания ключа) занимается **криптология** (греч. κρυπτός — тайный, λόγος — слово, знание). Криптология разделяется на два направления — криптографию и криптоанализ. Цели этих двух направлений криптологии прямо противоположны.

Криптография (греч. κρυπτός — скрытый и γράφω — пишу, рисую) — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Криптоанализ (греч. κρυπτός — скрытый и ἀνάλυση — разложение, расчленение) — наука, занимающаяся вопросами оценки сильных и слабых сторон методов шифрования, а также разработкой методов, позволяющих взламывать криптосистемы.

Следует различать криптографические методы сокрытия информации (шифрование) и кодирование. **Кодирование** — представление информации в альтернативном виде. Шифрование является частным случаем кодирования и предназначено для обеспечения конфиденциальности информации. С точки зрения решения этой задачи, кодирование — это безключевое шифрование, в котором преобразование построено на алгоритме кодирования или кодовой таблице. Различают:

- **общедоступные кодовые системы**, предназначенные для преобразования информации в форму, удобную для передачи, хранения или автоматической обработки (азбука Морзе, Unicode, штрихкод);
- **секретные кодовые системы**, предназначенные, как и криптографические системы, для обеспечения конфиденциальности (номенклатуры, «Код Госдепартамента», «Американский код для окопов», «Речные коды : Потомак»).

Параллельно с этим развивается **теория кодирования** - научное направление, которое разрабатывает и изучает методы защиты информации от случайных искажений в каналах связи. Таким образом, в настоящее время, термины кодирование и шифрование применяются для обозначения самостоятельных научных направлений и употреблять их как синонимы некорректно.

Следует отметить, что исторически в криптографии закрепились некоторые военные слова (противник, атака на шифр и др.) Они наиболее точно отражают смысл соответствующих некоторых криптографических понятий [9].

Криптография занимается методами преобразования информации, которые бы не позволили противнику извлечь ее из перехватываемых сообщений. При этом по каналу связи передается не сама защищаемая информация, а результат ее преобразования, и для противника возникает сложная задача вскрытия шифра. **Вскрытие (взламывание) шифра** - процесс получения защищаемой информации из шифрованного сообщения без знания примененного ключа. Способность шифра противостоять всевозможным атакам на него называют **криптографической стойкостью (криптостойкостью) шифра**. Под **атакой на шифр** понимают попытку вскрытия этого шифра.

Понятие стойкости шифра является центральным для криптографии. Хотя качественно понять его довольно легко, но получение строгих доказуемых оценок стойкости для каждого конкретного шифра - проблема нерешенная. Поэтому стойкость конкретного шифра оценивается только путем всевозможных попыток его вскрытия и зависит от квалификации **криптоаналитиков**, атакующих шифр. Такую процедуру иногда называют **проверкой стойкости**. Она делается из предположения, что противник знает сам алгоритм преобразования, но не знает ключа (см. Огюст Керкгоффс, п.2). Противник также может знать некоторые характеристики открытых текстов, например, общую тематику сообщений, их стиль, некоторые стандарты, форматы и т.д.

Однако помимо перехвата и вскрытия шифра противник может пытаться получить защищаемую информацию многими другими способами. Наиболее известным из таких способов является агентурный, когда противник каким-либо путем склоняет к сотрудничеству одного из законных пользователей и с помощью этого агента получает доступ к защищаемой информации. В такой ситуации криптография бессильна.

Противник может попытаться не получить, а уничтожить или модифицировать защищаемую информацию в процессе ее передачи. Это - совсем другой тип угроз для информации, отличный от перехвата и вскрытия шифра. Для защиты от таких угроз разрабатываются свои специфические методы.

Следовательно, на пути от одного законного пользователя к другому информация должна защищаться различными способами, противостоящими различным угрозам. В данной ситуации, противник будет стремиться найти самое слабое звено, чтобы с наименьшими затратами добраться до информации. А значит, и законные пользователи должны учитывать это обстоятельство в своей стратегии защиты: бессмысленно делать какое-то звено очень прочным, если есть заведомо более слабые звенья.

Что касается применения конкретных криптографических методов, то следует отметить, что не существует единого шифра, подходящего для всех случаев. **Выбор способа шифрования зависит:**

- от вида защищаемой информации (документальная, телефонная, телевизионная, компьютерная и т.д.);
- от объема и требуемой скорости передачи шифрованной информации;
- от ценности защищаемой информации (некоторые тайны [например, государственные, военные и др.] должны сохраняться десятилетиями, а некоторые [например, биржевые] - уже через несколько часов можно разгласить);
- от возможностей владельцев секретной информации, а также от возможностей противника (одно дело - противостоять одиночке, а другое дело - мощной государственной структуре).

Процесс криптографического закрытия данных может осуществляться как программно, аппаратно, так и иными способами. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

¹ **Фонема** (др.-греч. φώνημα - «звук») - минимальная смысловозначимая единица языка.

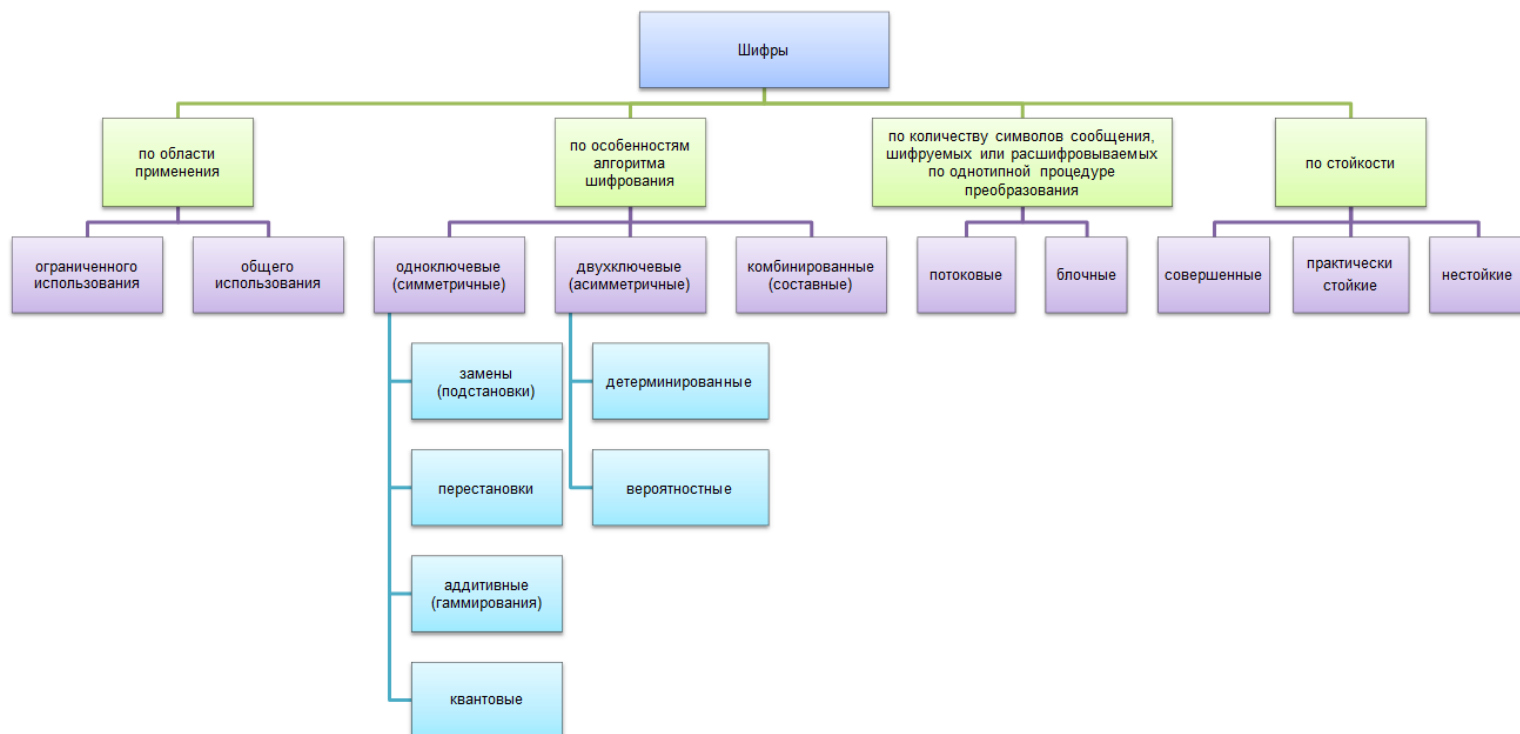
3.2. Основные требования, предъявляемые к криптосистемам

Для современных криптографических систем можно сформулировать следующие требования:

- сложность и трудоёмкость процедур шифрования и дешифрования должны определяться в зависимости от требуемого уровня защиты информации (необходимо обеспечить надежную защиту информации);
- временные и стоимостные затраты на защиту информации должны быть приемлемыми при заданном уровне ее секретности (затраты на защиту не должны быть чрезмерными);
- процедуры шифрования и дешифрования не должны зависеть от длины сообщения;
- количество всех возможных ключей шифра должно быть таковым, чтобы их полный перебор с помощью современных информационных технологий (в т.ч. и распределенных вычислений) был невозможен за приемлемое для противника время;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения;
- избыточность сообщений, вносимая в процессе шифрования, должна быть как можно меньшей (хорошим считается результат, когда длина шифрограммы не превышает длину исходного текста);
- зашифрованное сообщение должно поддаваться чтению только при наличии ключа.

3.3. Классификация шифров

Существует несколько классификаций шифров. Рассмотрим некоторые из них.



I. По области применения различают шифры ограниченного и общего использования.

Стойкость **шифров ограниченного использования** основывается на сохранении в секрете алгоритма криптографического преобразования в силу его уязвимости, малого количества ключей или отсутствия таковых (секретные кодовые системы).

Стойкость **шифров общего использования** основывается на секретности ключа и сложности его подбора потенциальным противником.

II. По особенностям алгоритма шифрования шифры общего использования можно разделить на следующие виды.

В **одноключевых** системах для шифрования и дешифрования используется один и тот же ключ.

В шифрах перестановки все буквы открытого текста остаются в шифрограмме, но меняют свои позиции. В шифрах замены наоборот, позиции букв в шифрограмме остаются теми же, что и у открытого текста, но символы открытого текста заменяются символами другого алфавита.

В аддитивных шифрах буквы алфавита заменяются числами, к которым затем добавляются числа секретной случайной (псевдослучайной) числовой последовательности (гаммы), после чего берется остаток от деления по модулю (операция mod). Если исходное сообщение и гамма представляются в битовом виде, то при шифровании и расшифровании применяется логическая операция «Исключающее ИЛИ» (XOR, сложение по модулю 2).

Квантовая криптография вносит в процесс шифрования естественную неопределенность квантового мира. Процесс отправки и приёма информации выполняется посредством объектов квантовой механики (например, при помощи электронов в электрическом токе или фотонов в линиях волоконно-оптической связи). Самым ценным свойством этого вида шифрования является то, что при передаче сообщения отправляющая и принимающая сторона с достаточно большой вероятностью могут установить факт перехвата противником зашифрованного сообщения.

В **двухключевых** системах для шифрования и дешифрования используется два совершенно разных ключа. В детерминированных шифрах при шифровании одного и того же сообщения одним и тем же ключом всегда будет получаться один и тот же шифртекст. В вероятностных шифрах в процедуре шифрования используется дополнительная случайная величина (число) - в результате при шифровании одного и того же исходного сообщения одним и тем же ключом могут получиться разные шифртексты, которые при расшифровке дадут один и тот же результат (исходное сообщение).

Комбинированные (составные) методы предполагают использование для шифрования сообщения сразу нескольких методов (например, сначала замена символов, а затем их перестановка).

III. По количеству символов сообщения (или его кодовой замены), шифруемых или расшифровываемых по однотипной процедуре преобразования различают:

- **поточковые шифры** – процедура преобразования применяется к отдельному символу сообщения;
- **блочные шифры** – процедура преобразования применяется к набору (блоку) символов сообщения.

Отличить потоковый шифр от блочного можно по следующему признаку - если в результате разбиения исходного сообщения на отдельные элементарные символы и применения к ним однотипной процедуры преобразования получаемая шифрограмма эквивалентна той, которая получается при применении преобразования «как будто ко всему исходному сообщению», то шифр потоковый, иначе блочный.

IV. По стойкости шифры делятся на три группы:

- **совершенные (абсолютно стойкие, теоретически стойкие)** – шифры, заведомо неподдающиеся вскрытию (при правильном использовании). Дешифрование секретного сообщения приводит к нескольким осмысленным равновероятным открытым сообщениям;
- **практически (вычислительно, достаточно) стойкие** – шифры, вскрытие которых за приемлемое время невозможно на современном или перспективном уровне вычислительной техники. Практическая стойкость таких систем базируется на теории сложности и оценивается исключительно на какой-то определенный момент времени с двух позиций:
 - вычислительная сложность полного перебора;
 - известные на данный момент слабости (уязвимости) и их влияние на вычислительную сложность;
- **нестойкие** шифры.

Вопросы для самопроверки

1. Дайте определение понятиям «шифр», «ключ», «дешифрование».
2. Перечислите основные требования, предъявляемые к криптосистемам.
3. Дайте классификацию криптосистем по алгоритму шифрования.
4. Дайте классификацию криптосистем по стойкости шифра.

4. ШИФРЫ ЗАМЕНЫ

4.1. Основы шифрования

Сущность шифрования методом замены заключается в следующем. Пусть шифруются сообщения на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) $M_A, B - M_B, \dots, Я - M_Я$. Шифрозамены выбираются таким образом, чтобы любые два множества (M_i и $M_j, i \neq j$) не содержали одинаковых элементов ($M_i \cap M_j = \emptyset$).

Таблица, приведенная на рис.4.1, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.

А	Б	...	Я
M_A	M_B	...	$M_Я$

Рис.4.1. Таблица шифрозамен

При шифровании каждая буква **А** открытого сообщения заменяется любым символом из множества M_A . Если в сообщении содержится несколько букв **А**, то каждая из них заменяется на любой символ из M_A . За счет этого с помощью одного ключа можно получить различные варианты шифрограммы для одного и того же открытого сообщения. Так как множества $M_A, M_B, \dots, M_Я$ попарно не пересекаются, то по каждому символу шифрограммы можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом.

Приведенное выше описание сущности шифров замены относится ко всем их разновидностям за исключением полиалфавитных шифров, в которых для зашифрования разных символов исходного алфавита могут использоваться одинаковые шифрозамены (т.е. $M_i \cap M_j \neq \emptyset, i \neq j$).

Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»).

Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками, звуками, жестами и т.п. В качестве примера можно привести пляшущих человечков из рассказа А. Конан Дойла (👤👤👤👤👤👤) и рукопись рунического письма (ᚠᚡᚢᚣᚤᚥᚦᚧᚨᚩᚪᚫᚬᚭᚮᚯᚰᚱᚲᚳᚴᚵᚶᚷᚸᚹᚺᚻᚼᚽᚾᚿ) из романа Ж. Верна «Путешествие к центру Земли».

Шифры замены можно разделить на следующие **подклассы** (разновидности).

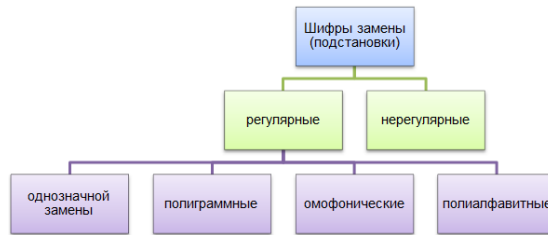


Рис.4.2. Классификация шифров замены

I. Регулярные шифры. Шифрозамены состоят из одинакового количества символов или отделяются друг от друга разделителем (пробелом, точкой, тире и т.п.).

- Шифры однозначной замены (моноалфавитные, простые подстановочные). Количество шифрозамен для каждого символа исходного алфавита равно 1 ($|M_i| = 1$ для одного символа).
- Полиграммные шифры. Аналогичны шифрам однозначной замены за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения ($|M_i| \geq 1$ для блока символов).
- Омофонические шифры (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1 ($|M_i| \geq 1$ для одного символа).
- Полиалфавитные шифры (многоалфавитные). Состоят из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования ($|M_i| > 1$ для одного символа);

II. Нерегулярные шифры. Шифрозамены состоят из разного количество символов, записываемых без разделителей.

4.2. Шифры однозначной замены

Максимальное количество ключей для любого шифра этого вида не превышает $n!$, где n – количество символов в алфавите. С увеличением числа n значение $n!$ растет очень быстро ($1! = 1, 5! = 120, 10! = 3628800, 15! = 1307674368000$). При больших n для приближенного вычисления $n!$ можно воспользоваться формулой Стирлинга

$$n! \approx \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \quad (4.1)$$

Шифр Цезаря. Согласно описаниям историка Светония в книге «Жизнь двенадцати цезарей» данный шифр использовался Гаем Юлием Цезарем для секретной переписки со своими генералами (I век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (**А, Б, ..., Я**), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

Рис.4.3. Таблица шифрозамен для шифра Цезаря

При зашифровке буква **А** заменяется буквой **Г**, **Б** - на **Д** и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «ГДУТПСЕ». Получатель сообщения «ГДУТПСЕ» ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение «АБРАМОВ».

Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33. Существуют различные модификации шифра Цезаря, в частности атбаш и лозунговый шифр.

Атбаш. В Ветхом Завете существует несколько фрагментов из священных текстов, которые зашифрованы с помощью шифра замены, называемого атбаш. Этот шифр состоит в замене каждой буквы другой буквой, которая находится в алфавите на таком же расстоянии от конца алфавита, как оригинальная буква - от начала. Например, в русском алфавите буква **А** заменяется на **Я**, буква **Б** - на **Ю** и т.д. В оригинальном Ветхом Завете использовались буквы еврейского алфавита. Так, в книге пророка Иеремии (25:26) слово «Бабель» (Вавилон) зашифровано как «Шешах».

Лозунговый шифр. Для данного шифра построение таблицы шифрозамен основано на лозунге (ключе) – легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшими в слово-лозунг, в алфавитном порядке. Например, если выбрано слово-лозунг «ДЯДИНА», то таблица имеет следующий вид.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Д	Я	И	Н	А	Б	В	Г	Е	Ё	Ж	З	Й	К	Л	М	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Рис.4.4. Таблица шифрозамен для лозунгового шифра

При шифровании исходного сообщения «АБРАМОВ» по приведенному выше ключу шифрограмма будет выглядеть «ДЯПДКМИ».

В качестве лозунга рекомендуется выбирать фразу, в которой содержатся конечные буквы алфавита. В общем случае, количество вариантов нижней строки (применительно к русскому языку) составляет $33! (\geq 10^{35})$.

Полибианский квадрат. Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (203-120 гг. до н.э.). Применительно к русскому алфавиту и индийским (арабским) цифрам суть шифрования заключалась в следующем. В квадрат 6х6 выписываются буквы (необязательно в алфавитном порядке).

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц

5	ч	ш	щ	ъ	ы	ь
6	э	ю	я	-	-	-

Рис.4.5. Таблица шифрозамен для полибианского квадрата

Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана. Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения вначале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца.

Тюремный шифр. Эта звуковая разновидность полибианского квадрата была разработана заключенными. Система состояла из нескольких ударов, обозначающих строки и столбцы в таблице с буквами алфавита. Один удар, а потом еще два соответствовали строке 1 и столбцу 2, т.е. букве **Б**. Пауза служила разделителем между строками и столбцами. Таким образом, зашифровать исходное сообщение «АБРАМОВ» можно следующим образом.

А	тук	___	тук
Б	тук	___	тук, тук
Р	тук, тук, тук	___	тук, тук, тук, тук, тук, тук
А	тук	___	тук
М	тук, тук, тук	___	тук, тук
О	тук, тук, тук	___	тук, тук, тук, тук
В	тук	___	тук, тук, тук

Рис.4.6. Пример использования тюремного шифра

Шифрующая система Трисемуса (Тритемия). В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.4.7 изображена таблица с ключевым словом «ДЯДИНА».

Д	Я	И	Н	А	Б
В	Г	Е	Ё	Ж	З
Й	К	Л	М	О	П
Р	С	Т	У	Ф	Х
Ц	Ч	Ш	Щ	Ъ	Ы
Ь	Э	Ю	-	-	-

Рис.4.7. Таблица шифрозамен для шифра Трисемуса

Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ЖЗЦЖУФИ».

Шифр масонов. В XVIII в. масоны создали шифр, чтобы скрыть от общественности свои коммерческие сделки. Как повелили те, кто прежде состоял в рядах этого общества, масоны пользовались способом засекречивания, весьма похожим на шифр розенкрейцеров. В «решетке» и в углах находятся точки, которыми заменялись буквы:

c	f	i	
b	e	h	
a	d	g	

l	o	r	
k	n	q	
j	m	p	

s		
v	u	t

w		
z	y	x

Рис.4.8. Шифрозамены шифра масонов

Так как клятвы хранить тайну нарушались не раз, большинство Великих лож масонов в США больше не пользуются письменными шифрами, предпочитая передавать устные инструкции во время закрытых ритуалов.

С помощью шифра масонов можно легко расшифровать следующую фразу.



Рис.4.9. Пример использования шифра масонов

Это первый уровень, на котором находятся все впервые вступившие в общество члены: Blue Lodge (рус. «Голубая (Синяя) лож»).

Одним из существенных **недостатков шифров однозначной замены** является их легкая вскрываемость. При вскрытии шифрограмм используются различные приемы, которые даже при отсутствии мощных вычислительных средств позволяют добиться положительного результата. Один из таких приемов базируется на том, что в шифрограммах остается информация о частоте встречаемости букв исходного текста. Если в открытом сообщении часто встречается какая-либо буква, то в шифрованном сообщении также часто будет встречаться соответствующий ей символ. Еще в 1412 г. Шихаба ал-Калкашанди в своем труде «Субх ал-Ашаш» привел таблицу частоты появления арабских букв в тексте на основе анализа текста Корана. Для разных языков мира существуют подобные таблицы. Так, например, для букв русского алфавита по данным "[Национального корпуса русского языка](#)" такая таблица выглядит следующим образом.

Таблица 4.1. Частота появления букв русского языка в текстах

№ п/п	Буква	Частота, %	№ п/п	Буква	Частота, %
1	О	10.97	18	Ь	1.74
2	Е	8.45	19	Г	1.70
3	А	8.01	20	З	1.65
4	И	7.35	21	Б	1.59
5	Н	6.70	22	Ч	1.44
6	Т	6.26	23	Й	1.21
7	С	5.47	24	Х	0.97
8	Р	4.73	25	Ж	0.94
9	В	4.54	26	Ш	0.73
10	Л	4.40	27	Ю	0.64
11	К	3.49	28	Ц	0.48
12	М	3.21	29	Щ	0.36
13	Д	2.98	30	Э	0.32
14	П	2.81	31	Ф	0.26
15	У	2.62	32	Ъ	0.04
16	Я	2.01	33	Ё	0.04
17	Ы	1.90			

Существуют подобные таблицы для пар букв (биграмм). Например, часто встречаемыми биграммами являются «то», «но», «ст», «по», «ен» и т.д. Другой прием вскрытия шифрограмм основан на исключении возможных сочетаний букв. Например, в текстах (если они написаны без орфографических ошибок) нельзя встретить сочетания «ня», «щя», «ъя» и т.п.

Для усложнения задачи вскрытия шифров однозначной замены еще в древности перед шифрованием из исходных сообщений исключали пробелы и/или гласные буквы. Другим способом, затрудняющим вскрытие, является шифрование **биграммами** (парами букв).

4.3. Полиграммные шифры

Полиграммные шифры замены - это шифры, в которых одна шифрозамена соответствует сразу нескольким символам исходного текста.

Биграмный шифр Порты. Шифр Порты, представленный им в виде таблицы, является первым известным биграмным шифром. Размер его таблицы составлял 20 x 20 ячеек; наверху горизонтально и слева вертикально записывался стандартный алфавит (в нем не было букв J, K, U, W, X и Z). В ячейках таблицы могли быть записаны любые числа, буквы или символы - сам Джованни Порты пользовался символами - при условии, что содержимое ни одной из ячеек не повторялось. Применительно к русскому языку таблица шифрозамен может выглядеть следующим образом.

	А	Б	В	Г	Д	Е (Е)	Ж	З	И (Й)	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
А	001	002	003	004	005	006	007	008	009	010	011	012	013	014	015	016	017	018	019	020	021	022	023	024	025	026	027	028	029	030	031

Б	032	033	034	035	036	037	038	039	040	041	042	043	044	045	046	047	048	049	050	051	052	053	054	055	056	057	058	059	060	061	062
В	063	064	065	066	067	068	069	070	071	072	073	074	075	076	077	078	079	080	081	082	083	084	085	086	087	088	089	090	091	092	093
Г	094	095	096	097	098	099	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124
Д	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155
Е (Ё)	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186
Ж	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217
З	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248
И (Й)	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279
К	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310
Л	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341
М	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372
Н	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403
О	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434
П	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465
Р	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496
С	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527
Т	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558
У	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589
Ф	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620
Х	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651
Ц	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682
Ч	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713
Ш	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744
Щ	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775
Ъ	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806
Ы	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837
Ь	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868
Э	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899
Ю	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930
Я	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961

Рис.4.10. Таблица шифрозамен для шифра Порты

Шифрование выполняется парами букв исходного сообщения. Первая буква пары указывает на строку шифрозамены, вторая - на столбец. В случае нечетного количества букв в исходном сообщении к нему добавляется вспомогательный символ («пустой знак»). Например, исходное сообщение «АБ РА МО В», зашифрованное – «002 466 355 093». В качестве вспомогательного символа использована буква «Я».

Шифр Playfair (англ. «Честная игра»). В начале 1850-х гг. Чарлз Уитстон придумал так называемый «прямоугольный шифр». Леон Плейфер, близкий друг Уитстона, рассказал об этом шифре во время официального обеда в 1854 г. министру внутренних дел лорду Пальмерстону и принцу Альберту. А поскольку Плейфер был хорошо известен в военных и дипломатических кругах, то за творением Уитстона навечно закрепилось название «шифр Плейфера».

Данный шифр стал первым буквенным биграммным шифром (в биграммной таблице Порты использовались символы, а не буквы). Он был предназначен для обеспечения секретности телеграфной связи и применялся британскими войсками в Англо-бурской и Первой мировой войнах. Им пользовалась также австралийская служба береговой охраны островов во время Второй мировой войны.

Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26 x 26 = 676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста.

Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – Х, для русского алфавита - Й). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес ОЯ». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, для лозунга «ДЯДИНА» ключевая таблица выглядит следующим образом.

Д	Я	И	Н	А	Б
В	Г	Е	Ё	Ж	З
Й	К	Л	М	О	П
Р	С	Т	У	Ф	Х
Ц	Ч	Ш	Щ	Ъ	Ы
Ь	Э	Ю	-	1	2

Рис.4.11. Ключевая таблица для шифра Playfair

Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста:

- Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.
- Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.
- Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Пример шифрования.

- биграмма «за» формирует прямоугольник – заменяется на «жб»;
- биграмма «ши» находятся в одном столбце – заменяется на «юе»;
- биграмма «фр» находятся в одной строке – заменяется на «кс»;
- биграмма «ов» формирует прямоугольник – заменяется на «йж»;
- биграмма «ан» находятся в одной строке – заменяется на «ба»;
- биграмма «но» формирует прямоугольник – заменяется на «ам»;
- биграмма «ес» формирует прямоугольник – заменяется на «гт»;
- биграмма «оя» формирует прямоугольник – заменяется на «ка»;
- биграмма «об» формирует прямоугольник – заменяется на «па»;
- биграмма «ще» формирует прямоугольник – заменяется на «щё»;
- биграмма «ни» формирует прямоугольник – заменяется на «ан»;
- биграмма «ея» формирует прямоугольник – заменяется на «ти».

Шифрограмма – «жб юе кс йж ба ам гт ка па шё ан ги».

Для расшифровки необходимо использовать инверсию этих правил, откидывая символы **Я** (или **Х**), если они не несут смысла в исходном сообщении.

Шифр Хилла. Первый практически реализуемый способ шифрования с использованием алгебры был придуман в 1929 г. математиком Лестером Хиллом - профессором из Хантер-колледжа в Нью-Йорке, статья которого «Cryptography in an Algebraic Alphabet» была опубликована в журнале «The American Mathematical Monthly».

Каждой букве алфавита сопоставляется число. Для русского алфавита можно использовать простейшую схему: А = 0, Б = 1, ..., Я = 32. Для зашифрования блок исходного сообщения из n букв рассматривается как n-мерный вектор чисел и умножается на матрицу размером **n x n** по модулю 33. Данная матрица, совместно с кодовой таблицей сопоставления букв алфавита с числами, является ключом зашифрования. Для расшифрования применяется обратная матрица¹ по модулю.

Например, для триграммных замен могут использоваться следующие матрицы зашифрования / расшифрования.

6	27	1
13	16	32

2	26	17
26	20	4

28	17	15
матрица		
зашифрования		

13	30	21
матрица		
расшифрования		

Рис.4.12. Матрицы зашифрования / расшифрования

Исходное сообщение «АБРАМОВ», дополненное двумя вспомогательными буквами «яя» (для кратности трем), после сопоставления букв с числами будет выглядеть следующим образом «0 1 17 0 13 15 2 32 32». После перемножения троек чисел на матрицу зашифрования шифрограмма примет следующий вид «11 32 8 3 28 17 17 11 24» (или в буквенном эквиваленте «КЯЗ ГЪР РКЧ»).

$$\begin{aligned}
 &\text{АБР} - 0 \ 1 \ 17 \\
 &(6 * 0 + 27 * 1 + 1 * 17) \bmod 33 = 11 \quad (\text{К}) \\
 &(13 * 0 + 16 * 1 + 32 * 17) \bmod 33 = 32 \quad (\text{Я}) \\
 &(18 * 0 + 17 * 1 + 15 * 17) \bmod 33 = 8 \quad (\text{З}) \\
 &\text{АМО} - 0 \ 13 \ 15 \\
 &(6 * 0 + 27 * 13 + 1 * 15) \bmod 33 = 3 \quad (\text{Г}) \\
 &(13 * 0 + 16 * 13 + 32 * 15) \bmod 33 = 28 \quad (\text{Ъ}) \\
 &(28 * 0 + 17 * 13 + 15 * 15) \bmod 33 = 17 \quad (\text{Р}) \\
 &\text{Вяя} - 2 \ 32 \ 32 \\
 &(6 * 2 + 27 * 32 + 1 * 32) \bmod 33 = 17 \quad (\text{Р}) \\
 &(13 * 2 + 16 * 32 + 32 * 32) \bmod 33 = 11 \quad (\text{К}) \\
 &(28 * 2 + 17 * 32 + 15 * 32) \bmod 33 = 24 \quad (\text{Ч})
 \end{aligned}$$

Для расшифрования тройки чисел шифрограммы необходимо умножить на матрицу расшифрования.

$$\begin{aligned}
 &\text{КЯЗ} - 11 \ 32 \ 8 \\
 &(2 * 11 + 26 * 32 + 17 * 8) \bmod 33 = 0 \quad (\text{А}) \\
 &(26 * 11 + 20 * 32 + 4 * 8) \bmod 33 = 1 \quad (\text{Б}) \\
 &(13 * 11 + 30 * 32 + 21 * 8) \bmod 33 = 17 \quad (\text{Р}) \\
 &\text{ГЪР} - 3 \ 28 \ 17 \\
 &(2 * 3 + 26 * 28 + 17 * 17) \bmod 33 = 0 \quad (\text{А}) \\
 &(26 * 3 + 20 * 28 + 4 * 17) \bmod 33 = 13 \quad (\text{М}) \\
 &(13 * 3 + 30 * 28 + 21 * 17) \bmod 33 = 15 \quad (\text{О}) \\
 &\text{РКЧ} - 17 \ 11 \ 24 \\
 &(2 * 17 + 26 * 11 + 17 * 24) \bmod 33 = 2 \quad (\text{Б}) \\
 &(26 * 17 + 20 * 11 + 4 * 24) \bmod 33 = 32 \quad (\text{Я}) \\
 &(13 * 17 + 30 * 11 + 21 * 24) \bmod 33 = 32 \quad (\text{Я})
 \end{aligned}$$

В результате будет получен набор чисел «0 1 17 0 13 15 2 32 32», соответствующий исходному сообщению со вспомогательными символами «АБРАМОВяя».

¹Обратная матрица - матрица A^{-1} , при умножении на которую, исходная матрица А дает в результате единичную матрицу Е.

4.4. Омофонические шифры

Другое направление повышения стойкости шифров замены состоит в том, чтобы каждое множество шифрообозначений M_i содержало более одного элемента. При использовании такого шифра одну и ту же букву (если она встречается несколько раз в сообщении) заменяют на разные шифрозамены из M_i . Это позволяет скрыть истинную частоту встречаемости букв открытого сообщения.

Система омофонов. В 1401 г. Симеоне де Крема стал использовать таблицы омофонов для сокрытия частоты появления гласных букв в тексте при помощи более чем одной шифрозамены. Такие шифры позже стали называться **шифрами многозначной замены** или **омофонами**². Они получили развитие в XV веке. В книге «Трактат о шифрах» Леона Баттисты Альберти (итальянский ученый, архитектор, теоретик искусства, секретарь папы Климентия XII), опубликованной в 1466 г., приводится описание шифра замены, в котором каждой букве ставится в соответствие несколько эквивалентов, число которых пропорционально частоте встречаемости буквы в открытом тексте. Так, если ориентироваться на, то число шифрозамен для буквы **О** должно составлять 110, для буквы **Е** – 85 и т.д. При этом каждая шифрозамена должна состоять из 3 цифр и их общее количество равно 1000. На рис.4.12 представлен фрагмент таблицы шифрозамен.

№ п/п	А	Б	В	...	М	...	О	...	Р	...	Я
1	311	128	175	...	037	...	248	...	064	...	266
2	357	950	194	...	149	...	267	...	189	...	333
...	...	...	...	...	...	...	...	...	...	...	...
16	495	990	199	...	349	...	303	...	374	...	749
...	...	...	...	...	...	...	...	...	...	...	...
20	519	...	427	...	760	...	306	...	469	...	845
...	...	...	...	...	...	...	...	...	...	...	...
32	637	...	524	...	777	...	432	...	554	...	...
...	...	...	...	...	...	...	...	...	...	...	...
45	678	...	644	...	...	...	824	...	721	...	...
...	...	...	...	...	...	...	...	...	...	...	...
47	776	...	...	...	...	...	828	...	954	...	...
...	...	...	...	...	...	...	...	...	...	...	...
80	901	...	...	...	...	...	886	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...
110	...	...	...	...	...	...	903	...	...	...	...

Рис.4.13. Фрагмент таблицы шифрозамен для системы омофонов

При шифровании символ исходного сообщения заменяется на любую шифрозамену из своего столбца. Если символ встречается повторно, то, как правило, используют разные шифрозамены. Например, исходное сообщение «АБРАМОВ» после шифрования может выглядеть «357 990 374 678 037 828 175».

Книжный шифр. Заметным вкладом греческого ученого Энея Тактика в криптографию является предложенный им так называемый книжный шифр, описанный в сочинении «Об обороне укреплённых мест». Эней предложил прокалывать малозаметные дырки в книге или в другом документе над буквами секретного сообщения. Интересно отметить, что в Первой мировой войне германские шпионы использовали аналогичный шифр, заменив дырки на точки, наносимые³ на буквы газетного текста. Описанные способы передачи секретных сообщений (с помощью точек) относятся к стеганографическим методам сокрытия информации.

После Первой мировой войны книжный шифр приобрел иной вид. Шифрозамена для каждой буквы определялась набором цифр, которые указывали на номер страницы, строки и позиции в строке.

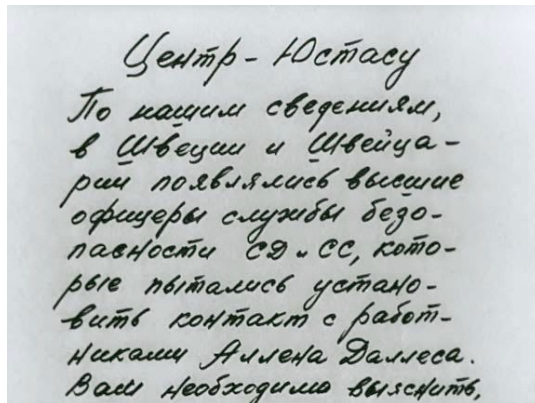
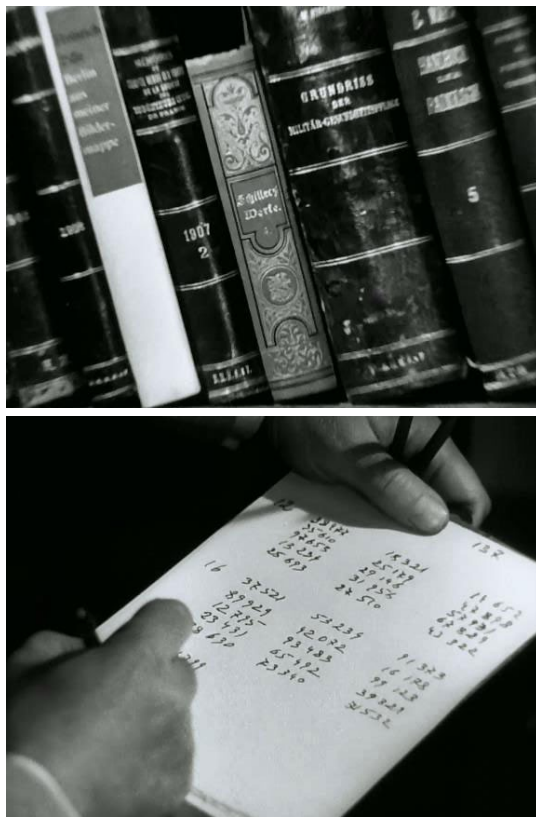


Рис.4.14. Пример использования книжного шифра
(кадры из советского сериала «Семнадцать мгновений весны»)

Количество книг, изданных за всю историю человечества, является величиной ограниченной (по крайней мере, явно меньше, чем 15!). Однако отсутствие полной электронной базы по изданиям делает процедуру вскрытия шифрограмм почти не выполнимой.

Вариантные шифры. Вариантные шифры напоминают полибианский квадрат, но для каждой строки и столбца используется по два буквенных идентификатора. В квадрат (прямоугольник) шифрозамен вначале записывается ключевое слово без повторяющихся букв, а затем дополняется не вошедшими в него буквами по порядку следования в алфавите. Каждой строке и столбцу квадрата ставится в соответствие по две буквы алфавита. Буквы для идентификации строк и столбцов не должны повторяться.

	Й	У	Е	Г	Щ	Х
	Ц	К	Н	Ш	З	Ъ
Ф	Ы	Д	Я	И	Н	А
В	А	В	Г	Е	Ё	Ж
П	Р	Й	К	Л	М	О
О	Л	Р	С	Т	У	Ф
Д	Ж	Ц	Ч	Ш	Щ	Ъ
Э	Я	Ь	Э	Ю	-	-

Рис.4.15. Пример таблицы шифрозамен вариантного шифра с ключевым словом «ДЯДИНА»

Комбинации букв-идентификаторов строки и столбца дают по восемь шифрозамен для каждой буквы исходного текста. Например, для буквы Д возможны шифрозамены: **ФЙ, ЙФ, ФЦ, ЦФ, ЫЙ, ЙЫ, ЫЦ и ЦЫ**. Для таблицы шифрозамен, приведенной на рис. 4.15, исходное сообщение «АБРАМОВ» может быть зашифровано как «ЫЗ ЫХ ОЦ ЗФ ГР РЦ АЙ».

²**Омофоны** (греч. homos - одинаковый и phone - звук) - слова, которые звучат одинаково, но пишутся по-разному и имеют разное значение.

³**Симпатические (невидимые) чернила** — чернила, записи которыми являются изначально невидимыми и становятся видимыми только при определенных условиях (нагрев, освещение, химический проявитель и т. д.).

4.5. Полиалфавитные шифры

Напомним, что полиалфавитные шифры состоят из нескольких шифров однозначной замены и отличаются друг от друга способом выбор варианта алфавита для зашифрования одного символа.

Диск Альберти. В «Трактате о шифрах» Альберти приводит первое точное описание многоалфавитного шифра на основе шифровального диска.



Рис.4.16. Реплика диска Альберти, используемого Конфедерацией во время Гражданской войны в Америке [www.cryptomuseum.com]

Он состоял из двух дисков – внешнего неподвижного и внутреннего подвижного дисков, на которые были нанесены буквы алфавита. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене ее на букву с внутреннего диска, стоящую под ней. После этого внутренний диск сдвигался на одну позицию и шифрование второй буквы производилось уже по новому шифралафавиту. Ключом данного шифра являлся порядок расположения букв на дисках и начальное положение внутреннего диска относительно внешнего.

Таблица Трисемуса. Одним из шифров, придуманных немецким аббатом Трисемусом, стал многоалфавитный шифр, основанный на так называемой «таблице Трисемуса» - таблице со стороны равной n , где n – количество символов в алфавите. В первой строке матрицы записываются буквы в порядке их очередности в алфавите, во второй – та же последовательность букв, но с циклическим сдвигом на одну позицию влево, в третьей – с циклическим сдвигом на две позиции влево и т.д.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Рис.4.17. Таблица Трисемуса

Первая строка является одновременно и алфавитом для букв открытого текста. Первая буква текста шифруется по первой строке, вторая буква по второй и так далее. После использования последней строки вновь возвращаются к первой. Так сообщение «АБРАМОВ» приобретет вид «АВТГРУЗ».

Система шифрования Виженера. В 1586 г. французский дипломат Блез Вижнер представил перед комиссией Генриха III описание простого, но довольно стойкого шифра, в основе которого лежит таблица Трисемуса.

Перед шифрованием выбирается ключ из символов алфавита. Сама процедура шифрования заключается в следующем. По i -ому символу открытого сообщения в первой строке определяется столбец, а по i -ому символу ключа в крайнем левом столбце – строка. На пересечении строки и столбца будет находиться i -ый символ, помещаемый в шифрограмму. Если длина ключа меньше сообщения, то он используется повторно. Например, исходное сообщение «АБРАМОВ», ключ – «ДЯДИНА», шифрограмма – «ДАФИТЬОЕ».

Справедливости ради, следует отметить, что авторство данного шифра принадлежит итальянцу Джованни Батиста Беллазо, который описал его в 1553 г. История «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то, что он ничего не сделал для его создания». Беллазо предложил называть секретное слово или фразу **паролем** (ит. password; фр. parole - слово).

В 1863 г. Фридрих Касиски опубликовал алгоритм атаки на этот шифр, хотя известны случаи его взлома шифра некоторыми опытными криптоаналитиками и ранее. В частности, в 1854 г. шифр был взломан изобретателем первой аналитической вычислительной машины Чарльзом Бэббиджем, хотя этот факт стал известен только в XX в., когда группа ученых разбирала вычисления и личные заметки Бэббиджа. Несмотря на это шифр Виженера имел репутацию

исключительно стойкого к «ручному» взлому еще долгое время. Так, известный писатель и математик Чарльз Лютвидж Должсон (Льюис Корролл) в своей статье «Алфавитный шифр», опубликованной в детском журнале в 1868 г., назвал шифр Виженера невзламываемым. В 1917 г. научно-популярный журнал «Scientific American» также отозвался о шифре Виженера, как о неподдающемся взлому.

Роторные машины. Иден Альберти и Беллазо использовались при создании электромеханических роторных машин первой половины XX века. Некоторые из них использовались в разных странах вплоть до 1980-х годов. В большинстве из них использовались роторы (механические колеса), взаимное расположение которых определяло текущий алфавит шифрозамен, используемый для выполнения подстановки. Наиболее известной из роторных машин является немецкая машина времен Второй мировой войны «Энигма».

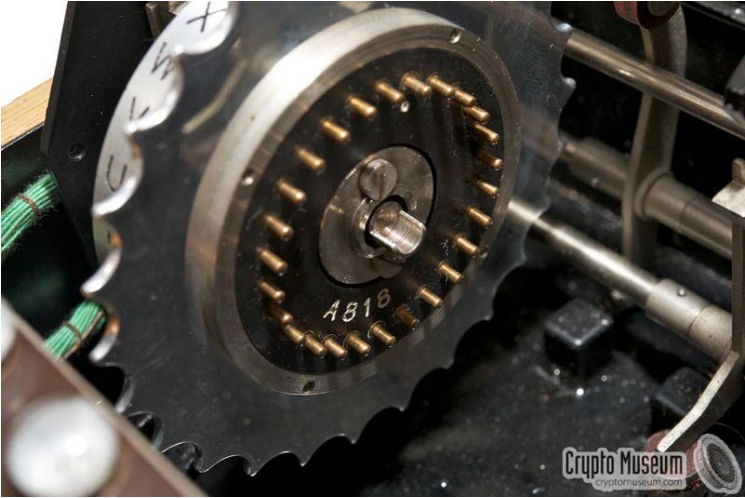


Рис.4.18. Энигма [www.cryptomuseum.com]

Выходные штыри одного ротора соединены с входными штырями следующего ротора и при нажатии символа исходного сообщения на клавиатуре замыкали электрическую цепь, в результате чего загоралась лампочка с символом шифрозамены.



а) четыре последовательно соединённых ротора



б) штыри ротора

Рис.4.19. Роторная система Энигмы [www.cryptomuseum.com]

Шифрующее действие «Энигмы» показано для двух последовательно нажатых клавиш - ток течёт через роторы, «отражается» от рефлектора, затем снова через роторы.

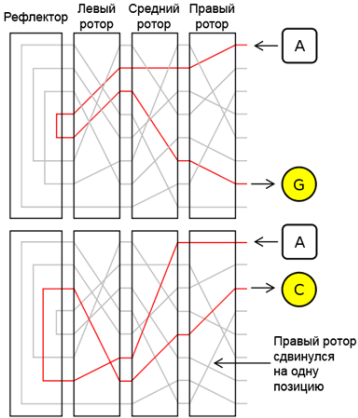


Рис.4.20. Схема шифрования

Примечание. Серыми линиями показаны другие возможные электрические цепи внутри каждого ротора. Буква А шифруется по-разному при последовательных нажатиях одной клавиши, сначала в G, затем в С. Сигнал идет по

другому маршруту за счёт поворота одного из роторов после нажатия предыдущей буквы исходного сообщения.

Шифры Тени. Главными развлечениями для американцев тридцатых годов XX века были бульварное чтиво и радио. Для раскрутки своих книжек издательство Street & Smith проспонсировало радиопередачу, ведущим в которой был Тень (англ. Shadow), загадочный рассказчик со зловещим голосом, который в начале каждого выпуска заявлял: «Кто знает, что за зло прячется в сердцах людей? Тень знает!». Успех радиопередачи подтолкнул издательство к решению начать выпускать серию книг, в которой главным героем был бы Тень. Свои услуги предложил Уолтер Гибсон, большой любитель фокусов и головоломок. Под псевдонимом Максвелл Грант он принялся писать роман за романом, да с такой скоростью, что за свою жизнь написал почти 300 книжек о грозе тех, кто нечист помыслами. В новелле «Цепочка смерти» супергерой воспользовался так называемым кодом направления, хотя на самом деле он действует скорее как шифр, чем как код.

a	b	c	d	e	f	g	h	i	j	k	l	m
n	o	p	q	r	s	t	u	v	w	x	y	z
пробел		1	2	3	4							

Рис.4.21. Таблица шифрозамен и управляющих символов

Управляющие символы в последней строке таблицы служат для изменения кода (выбора шифралфавита) для зашифрования/дешифрования. Линии внутри каждого кружка фактически являются стрелками, подсказывающими адресату, как держать лист бумаги. Символ 1 означает, что лист надо держать как обычно: верх и низ расположены на своих местах, а сообщение читается слева направо. Символ 2 требует поворота на 90° вправо, а символ 3 указывает, что лист бумаги следует перевернуть вверх ногами. Символ 4 обозначает поворот на 90° влево. Эти дополнительные символы могут появляться перед любой строчкой текста, а также в ее середине.

Из нижеприведенного примера можно узнать настоящие имя и фамилию супергероя.

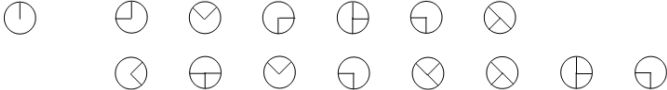


Рис.4.22. Настоящие имя и фамилия Тени

Согласно первому управляющему символу, лист следует держать обычным образом, не поворачивая, и после замены буквы образуют «Lamont Cranston» (Ламонт Крэнстон).

4.6. Нерегулярные шифры

Еще одним направлением повышения стойкости шифров замены заключается в использовании нерегулярных шифров. В приведенных выше шифрах (**регулярных**) шифрозамены состоят из строго определенного количества символов (букв, цифр, графических элементов и т.д.) или в шифрограмме они отделяются друг от друга специальными символами (пробелом, точкой, запятой и т.д.). В нерегулярных шифрах шифрозамены состоят из разного количества символов и записываются в шифрограмме в подряд (без выделения друг от друга), что значительно затрудняет криптоанализ.

Совмещенный шифр (совмещенная таблица). Данный шифр применялся еще семейством Ардженти - криптологами, разрабатывавшими шифры для Папы Римского в XVI в. В XX столетии этим способом пользовались коммунисты в ходе гражданской войны в Испании. В начале войны противники фашизма в Испании контролировали большинство крупных городов и защищали свою связь, включая радиопередачи, с помощью различных методов шифрования, в том числе совмещенных шифров.

Вариант коммунистов получил название «совмещенный» из-за необычного использования одно- и двухцифровых шифрозамен, благодаря чему сообщение приобретало дополнительную защиту от потенциального дешифровальщика. Некоторые буквы шифровались одной цифрой, другие же - парой цифр. При этом криптоаналитик противника совершенно не представлял, где в перехваченных сообщениях находятся одноцифровые, а где двухцифровые шифрозамены.

Таблица шифрозамен состоит из 10 столбцов с нумерацией 0, 9, 8, 7, 6, 5, 4, 3, 2 и 1. В начальную строку вписывается ключевое слово без повторяющихся букв. В последующие строки вписываются по десять не вошедших в него букв по порядку следования в алфавите. Строки, за исключением начальной, нумеруются по порядку, начиная с 1.

	0	9	8	7	6	5	4	3	2	1
	Д	Я	И	Н	А					
1	Б	В	Г	Е	Ё	Ж	З	Й	К	Л
2	М	О	П	Р	С	Т	У	Ф	Х	Ц
3	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	-	-

Рис.4.23. Пример таблицы шифрозамен совмещенного шифра с ключевым словом «ДЯДИНА»

При шифровании буквы исходного сообщения, входящие в ключевое слово, заменяются на одну цифру (номер столбца), остальные – двумя (номера строки и столбца). Например, для приведенной выше таблицы шифрозамен исходное сообщение «АБРАМОВ» будет зашифровано как «610276202919».

При получении шифрограммы адресат знает, что когда появляются цифры 1, 2 или 3, с ними обязательно связана еще одна цифра, поскольку они представляют собой цифровую пару. Так что 35 - это, несомненно, пара, а 53 - нет, ведь в таблице нет строки с номером 5. Перехват такого сообщения третьей стороной даст ей всего лишь ряд цифр, потому что криптоаналитик противника не имеет ни малейшего представления, какие цифры одиночные, а какие входят в состав пар.

Вопросы для самопроверки

- 1. В чем заключается основная идея криптографических преобразований шифров замены?
- 2. Перечислите основные разновидности шифров замены.
- 3. Дайте характеристику разновидностям шифров замены.
- 4. Назовите основной недостаток шифра однозначной замены.

5. ШИФРЫ ПЕРЕСТАНОВКИ

5.1. Основы шифрования

Перестановка представляет собой способ шифрования, при котором для получения шифрограммы буквы исходного сообщения меняют местами. Типичным примером перестановки являются анаграммы, ставшие популярными в XVII в. **Анаграмма** (греч. *ανα* - «снова» и *γράφω* - «запись») - литературный приём, состоящий в перестановке букв или звуков определённого слова (или словосочетания), что в результате даёт другое слово или словосочетание [17]. Например: апельсин - спаниель, полковник - клоповник, горилка - рогалик, лепесток - телескоп.

Прародителем анаграммы однако считают поэта и грамматика Ликофрона, который жил в Древней Греции в III веке до н. э. Как сообщал византийский автор Иоанн Цец, из имени царя Птолемея он составил первую из известных нам анаграмм: Ptolemaios - Apo Melitos, что в переводе означает «из мёда», а из имени царицы Арсинои: Arsinoe - Ion Eras («фиалка Геры»). В XVII—XIX вв. среди естествоиспытателей было принято зашифровывать свои открытия в виде анаграмм, что служило двум нуждам: скрыть гипотезу до её окончательной проверки и утвердить авторство на открытие, когда оно будет подтверждено. Так, в 1610 г. Галилео Галилей для закрепления авторства на открытие спутников Сатурна зашифровал латинскую фразу «Altissimum planetam tergeminum observavi» («Высочайшую планету тройную наблюдал») следующим образом: «Smaismrmilmepoetaleumibunenugttauiras» (буквы «v» и «u» в латинских текстах часто считались взаимозаменяемыми)¹.

Доподлинно не известно, когда появился шифр перестановки, но вполне возможно, что писцы в древности переставляли буквы в имени своего царя ради того, чтобы скрыть его подлинное имя или в ритуальных целях [43].

Все шифры перестановки делятся на два **подкласса**:

- шифры одинарной (простой) перестановки. При шифровании символы перемещаются с исходных позиций в новые один раз;
- шифры множественной (сложной) перестановки. При шифровании символы перемещаются с исходных позиций в новые несколько раз.

¹В те времена самой дальней из известных («высочайшей») планет был Сатурн. В действительности, в силу несовершенства телескопа, используемого Галилеем, он наблюдал не спутники, а кольца Сатурна, которые выступали по краям планеты. Эти выступы («ушки») и были приняты им за спутники. Свою гипотезу о них в виде анаграммы Галилей отослал Иоганну Кеплеру, который, потратив множество сил, перевел ее как «Salve umbistineum geminatum Martia proles» (лат., «Возрадуйтесь, два протуберанца - сыны Марса»). Кеплер не обратил внимание на то, что в его переводе была лишняя буква, т.к. по его соображениям у Марса должны были быть два спутника, неоткрытые на тот момент. Спутники Марса (Фобос и Деймос) были открыты американским астрономом Асафом Холлом позже - в 1877 г. [54].

5.2. Шифры одинарной перестановки

В общем случае для данного класса шифров при шифровании и дешифровании используется таблица перестановок.

1	2	3	...	n
I ₁	I ₂	I ₃	...	I _n

Рис.5.1. Таблица перестановок

В первой строке данной таблицы указывается позиция символа в исходном сообщении, а во второй – его позиция в шифрограмме. Таким образом, максимальное количество ключей для шифров перестановки равно $n!$, где n – длина сообщения.

Шифр простой одинарной перестановки. Для шифрования и дешифрования используется таблица перестановок, аналогичная показанной на рис.5.2.

1	2	3	4	5	6	7
2	4	1	7	6	5	3

Рис.5.2. Таблица перестановок

Например, если для шифрования исходного сообщения «АБРАМОВ» использовать таблицу, представленную на рис.5.2, то шифрограммой будет «РАВБОМА». Для использования на практике такой шифр не удобен, так как при больших значениях n приходится работать с длинными таблицами и для сообщений разной длины необходимо иметь свою таблицу перестановок.

Шифр блочной одинарной перестановки. При использовании этого шифра задается таблица перестановки блока символов, которая последовательно применяется до тех пор, пока исходное сообщение не закончится. Если исходное сообщение не кратно размеру блока, тогда оно при шифровании дополняется произвольными символами.

1	2	3
2	3	1

Рис.5.3. Таблица перестановок

Для примера выберем размер блока, равный 3, и примем таблицу перестановок, показанную на рис.5.3. Дополним исходное сообщение «АБРАМОВ» буквами **Б** и **Э**, чтобы его длина была кратна 3. В результате шифрования получим «РАБОАМЭВБ».

Количество ключей для данного шифра при фиксированном размере блока равно $m!$, где m – размер блока.

Шифры маршрутной перестановки. Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру (плоскую или объемную). Преобразования состоят в том, что в фигуру исходный текст вписывается по ходу одного маршрута, а выписывается по другому. Один из таких шифров – шифр «Считала» - упоминался ранее. Некоторые из них приводятся ниже.

Шифр табличной маршрутной перестановки. Наибольшее распространение получили шифры маршрутной перестановки, основанные на таблицах. При шифровании в такую таблицу вписывают исходное сообщение по определённому маршруту, а выписывают (получают шифрограмму) - по другому. Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом.

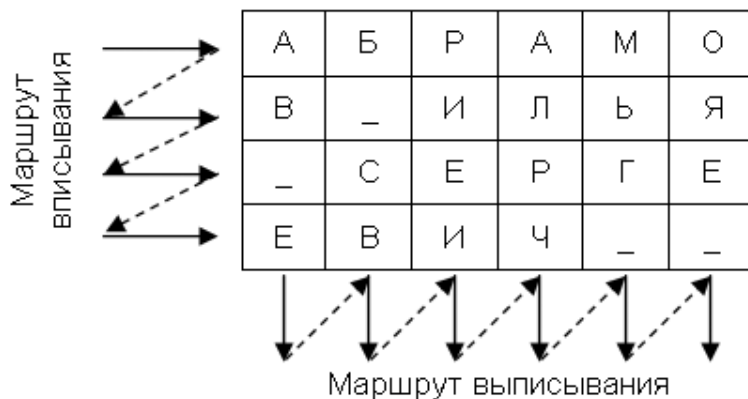


Рис.5.4. Пример использования шифра маршрутной перестановки

Например, исходное сообщения «АБРАМОВ ИЛЬЯ СЕРГЕЕВИЧ» вписывается в прямоугольную таблицу

размерами 4x6, маршрут вписывания – слева-направо сверху-вниз, маршрут выписывания – сверху-вниз слева-направо. Шифрограмма в этом случае выглядит «АВ_ЕБ_СВРИЕИАЛР ЧМЬГ_ОЯЕ_».

Шифр вертикальной перестановки. Является разновидностью предыдущего шифра. К особенностям шифра можно отнести следующие:

- количество столбцов в таблице фиксируется и определяется длиной ключа;
- маршрут вписывания - строго слева-направо сверху-вниз;
- шифрограмма выписывается по столбцам в соответствии с их нумерацией (ключом).

Ключ	Д	Я	Д	И	Н	А
	2	6	3	4	5	1
Текст	А	Б	Р	А	М	О
	В	_	И	Л	Ь	Я
	_	С	Е	Р	Г	Е
	Е	В	И	Ч	_	_

Рис.5.5. Пример использования шифра вертикальной перестановки

В качестве ключа можно использовать слово или фразу. Тогда порядок выписывания столбцов соответствует алфавитному порядку букв в ключе. Например, если ключевым словом будет «ДЯДИНА», то присутствующая в нем буква **А** получает номер 1, **Д** – 2 и т.д. Если какая-то буква входит в слово несколько раз, то ее появления нумеруются последовательно слева направо. В примере первая буква **Д** получает номер 2, вторая **Д** – 3.

При шифровании сообщения «АБРАМОВ ИЛЬЯ СЕРГЕЕВИЧ» результат будет «ОЯЕ_АВ_ЕРИЕИАЛРЧМЬГ_Б_СВ».

Шифр «Перекресток» [43]. Для перемешивания букв могут использоваться фигуры специального вида. Один из таких способов носит название «перекресток». В приведенном ниже примере рисуют крестообразные фигуры в количестве, достаточном, чтобы разместить в них все буквы сообщения. Открытый текст записывают вокруг этих фигур заранее оговоренным способом - в нашем случае по часовой стрелке. Таким образом, сообщение «АБРАМОВ ИЛЬЯ СЕРГЕЕВИЧ» может выглядеть следующим образом:

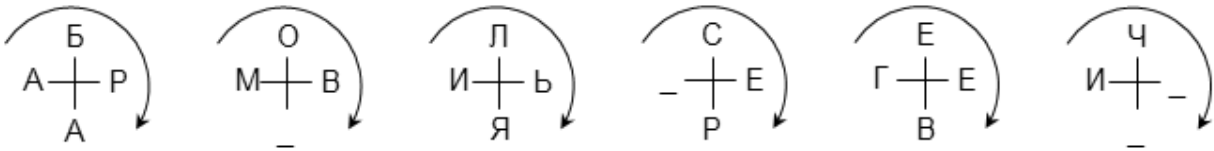
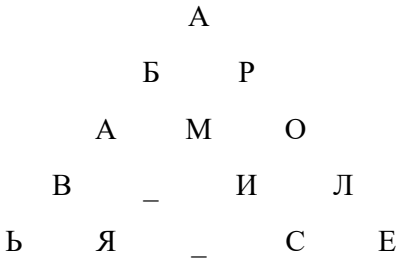


Рис.5.6. Пример размещения открытого текста в шифре «Перекресток»

Буквы берутся построчно. Вначале берется оговоренное количество букв (N) из первой строки, затем удвоенное количество букв (2N) из второй и снова N букв из третьей строки. Например, при N = 3 шифрограмма будет выглядеть «БОЛАРМВИЬА_ЯСЕЧ_ЕГЕИ_РВ_».

Шифры с использованием треугольников и трапеций [43]. Помочь выполнить перестановки могут как треугольники, так и трапеции. Открытый текст вписывается в эти фигуры в соответствии с количеством слов и формой выбранной фигуры, которая может быть растянута или сжата, чтобы в ней поместилось сообщение. Для первой фигуры, треугольника, открытый текст записывается построчно от вершины до основания.



Р	Г	Е	Е	В	И
Д	Я	Д	И	Н	А
Д	Я	Д	И	Н	
2	10	3	6	8	1
4	11	5	7	9	

Рис.5.7. Пример использования шифра перестановки при вписывании в треугольник

Ниже записывается ключевое слово. Поскольку основание широкое, ключевое слово повторяется. Буквы строки с ключевым словом нумеруются последовательно согласно их алфавитному порядку. Зашифрованное сообщение выписывается по столбцам согласно выполненной нумерации. Таким образом, для открытого текста «АБРАМОВ ИЛЬЯ СЕРГЕЕВИ» и ключевого слова «ДЯДИНА» шифрограмма будет выглядеть «АМ_РВГРИЕЛВАЯЕБ_ЕИЬРС».

Шифр «Поворотная решетка» [14, 17, 43]. В 1550 г. итальянский математик Джероламо Кардано², состоящий на службе у папы Римского, в книге «О тонкостях» предложил новую технику шифрования - **решётку Кардано**.

Изначально решетка Кардано представляла собой трафарет с прорезанными в нем отверстиями. В этих отверстиях на листе бумаги, который клали под решетку, записывались буквы, слоги и слова сообщения. Далее трафарет снимался, и свободное пространство заполнялось более или менее осмысленным текстом для маскировки секретного послания. Такой метод сокрытия информации относится к стеганографии.

Позднее был предложен шифр «поворотная решетка» или, как его еще называют, «решетка для выющихся растений», поскольку она напоминала отверстия в деревянных решетках садовых строений. Этот шифр считают первым **транспозиционным** (геометрическим) шифром.

Несмотря на то, что между изначальным предложением Кардано и шифром «поворотная решетка» большая разница, методы сокрытия информации, основанные на использовании трафаретов, принято называть «решетками Кардано».

Для шифрования и дешифрования с помощью данного шифра изготавливается прямоугольный трафарет с четным количеством строк и столбцов. В трафарете вырезаются клетки таким образом, чтобы при наложении его на таблицу того же размера четырьмя возможными способами, его вырезы полностью покрывали все ячейки таблицы ровно по одному разу.

При шифровании трафарет накладывается на таблицу. В видимые ячейки таблицы выписываются буквы исходного текста слева-направо сверху-вниз. Далее трафарет поворачивается и вписывается следующая часть букв. Эта операция повторяется еще два раза. Шифрограмму выписывают из итоговой таблицы по определенному маршруту.

Таким образом, ключом при шифровании является трафарет, порядок его поворотов и маршрут выписывания.

Пример шифрования сообщения «АБРАМОВ+ДЯДИНА» показан на рис.5.8. Результат шифрования – «АДВ_МНРДБЯ+_ОААИ».

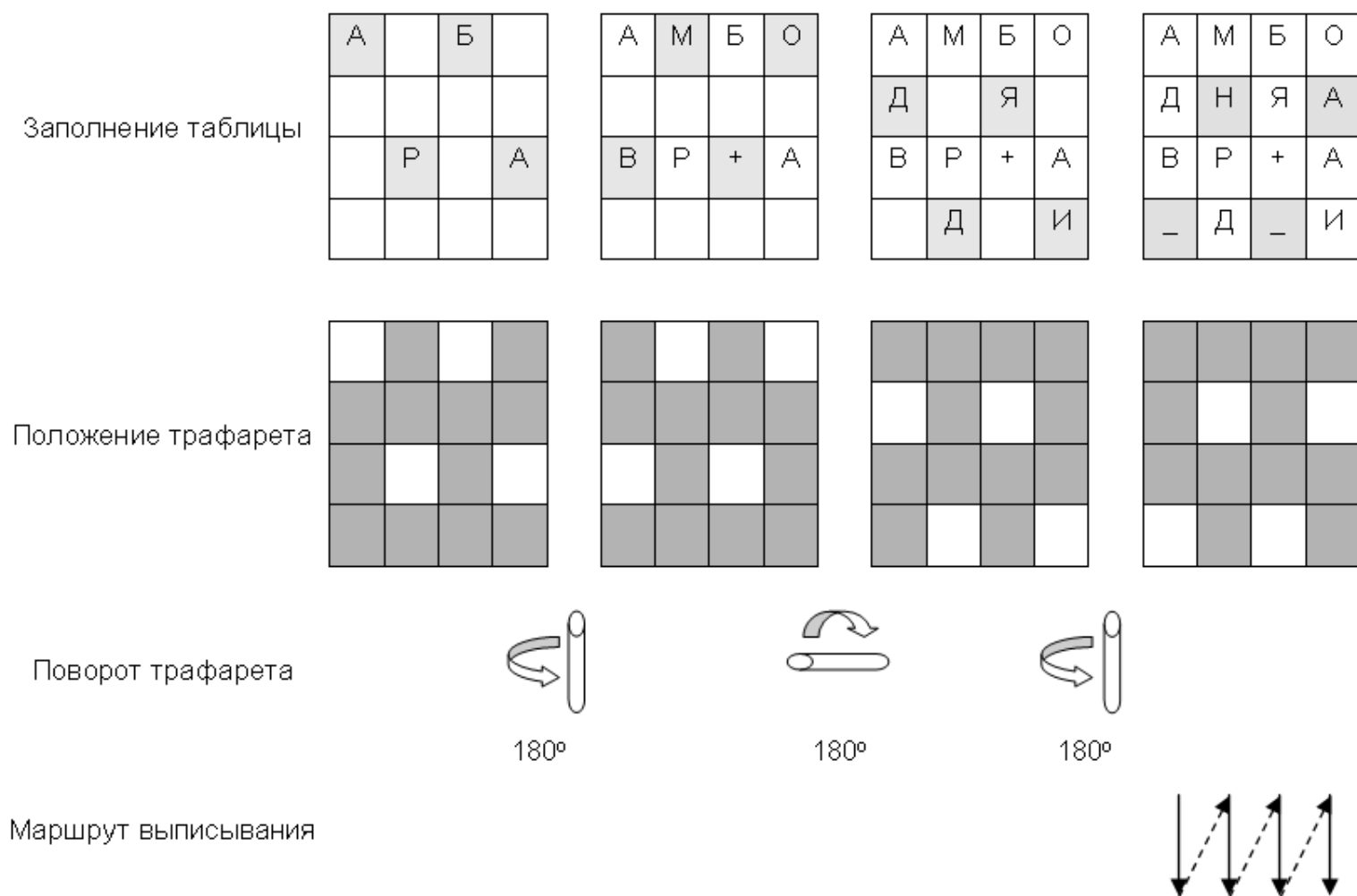


Рис.5.8. Пример использования шифра «поворотная решетка»

Данный метод шифрования применялся нидерландскими правителями для секретных посланий в 1740-х гг. Он также использовался в армии кайзера Вильгельма в Первую мировую войну. Для шифрования немцы использовали решетки разных размеров, которым французские криптоаналитики дали собственные кодовые имена: Анна (25 букв), Берта (36 букв), Дора (64 буквы) и Эмиль (81 буква). Однако использовались решетки очень недолго (всего четыре месяца) к огромному разочарованию французов, которые только-только начали подбирать к ним ключи.

Магические квадраты. Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами начиная с 1, которые в сумме по каждому столбцу, каждой строке и каждой диагонали дают одно и то же число.

Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила». По преданию, описанному в одной из пяти канонических книг Древнего Китая - Шу-Цзин (Книге записанных преданий), в 2200 году до н.э. из реки Ло вышла огромная черепаха (по другой версии - дракон), символ вечности. На ее панцире были видны пятна, образующие удивительный рисунок.

龜 書 圖

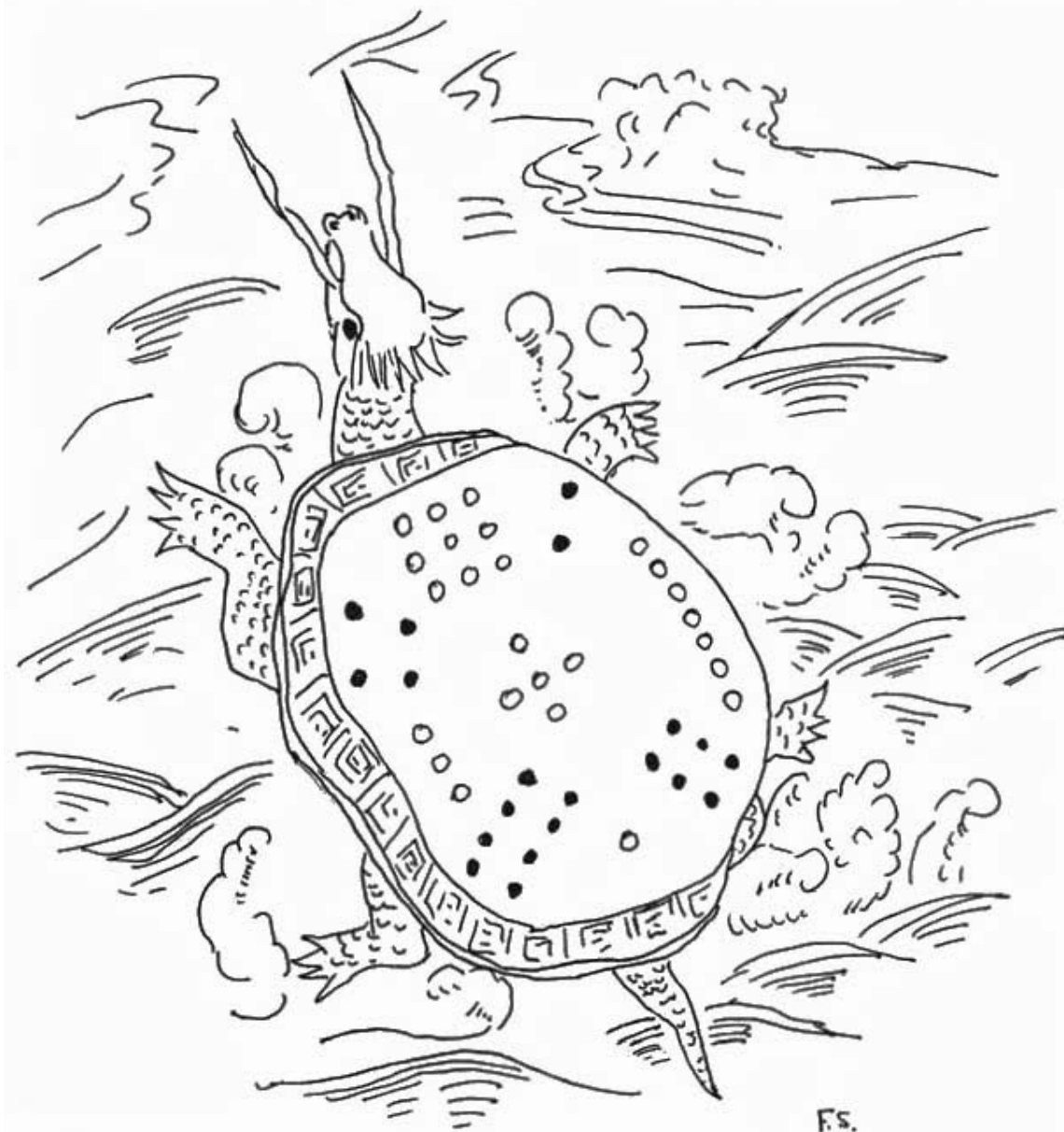


Рис.5.9. Магический квадрат Ло Шу

Когда черепаха вышла из воды, высыхали лужи после недавнего ливня. Великий Юй взял эту черепаху и рассмотрел странный узор на ее панцире. Этот узор вдохновил его на создание трактата под названием «Хун Фань» («Великий план»), в котором говорилось о физике, астрологии, предсказаниях, морали, политике и религии [53].

Магические квадраты широко применялись для передачи секретной информации. При шифровании исходное сообщение вписывалось в квадрат по приведенной в них нумерации, после чего шифрограмма выписывалась по строкам. Количество возможных магических квадратов (ключей) быстро возрастает с увеличением их размера. Так, существует лишь один магический квадрат размером 3x3, если не принимать во внимание его повороты. Магических квадратов 4x4 насчитывается уже 880, а число магических квадратов размером 5x5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был невыносим [17].

Рассмотрим квадрат размером 4x4. В него вписываются числа от 1 до 16. Его магия состоит в том, что сумма чисел по строкам, столбцам и полным диагоналям равняется одному и тому же числу - 34.

16	3	2	13
5	10	11	8

9	6	7	12
4	15	14	1

Рис.5.10. Магический квадрат 4x4

Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: «АБРАМОВДЯДИНА...». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу. В пустые клетки ставится точка или любая буква.

16 .	3 Р	2 Б	13 А
5 М	10 Д	11 И	8 Д
9 Я	6 О	7 В	12 Н
4 А	15 .	14 .	1 А

Рис.5.11. Пример шифрования с помощью магического квадрата

После этого шифрованный текст записывается в строку (считывание производится слева-направо сверху-вниз, построчно) – «.РБАМДИДЯОВНА..А».

²Джелорамо Кардано (1501 – 1576 гг.) - итальянский математик, инженер, философ, медик и астролог. В его честь названы открытые Сципионом дель Ферро формулы решения кубического уравнения (Кардано первым их опубликовал) и карданный вал (известного ещё Леонардо да Винчи). Написал около 240 книг (131 из них была опубликована, 111 остались в виде рукописей) [43].

5.3. Шифры множественной перестановки

В данном подклассе шифров используется идея повторного шифрования уже зашифрованного сообщения или многократной перестановки символов исходного сообщения перед попаданием в итоговую шифрограмму.

Шифр двойной перестановки. В таблицу по определенному маршруту записывается текст сообщения, затем переставляются столбцы, а потом переставляются строки. Шифрограмма выписывается по определенному маршруту.

Пример шифрования сообщения «АБРАМОВ+ДЯДИНА» показан на следующем рисунке. Результат шифрования – «ОАБЯ+_АИВ_РДМНАД».



Рис.5.12. Пример использования шифра двойной перестановки

Ключом к шифру являются размеры таблицы, маршруты вписывания и выписывания, а также порядки

перестановки столбцов и строк. Если маршруты являются фиксированными величинами, то количество ключей равно $n! \cdot m!$, n и m – количество столбцов и строк в таблице.

Несмотря на многоступенчатую процедуру шифрования, включая двойную перестановку, данный шифр может быть эквивалентно заменен шифром простой одинарной перестановки. На следующем рисунке приведена таблица эквивалентных одинарных перестановок для примера шифрования, приведенного на рис. 5.12.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
А	Б	Р	А	М	О	В	+	Д	Я	Д	И	Н	А	_	_
15	3	11	7	13	1	9	5	16	4	12	8	14	2	10	6
О	А	Б	Я	+	_	А	И	В	_	Р	Д	М	Н	А	Д

Рис.5.13. Таблица эквивалентных одинарных перестановок

Аналогичную замену на шифр блочной одинарной перестановки можно выполнить и для других шифров: табличная маршрутная перестановка, «поворотная решетка», «магический квадрат» и др.

Вопросы для самопроверки

- 1. В чем заключается основная идея криптографических преобразований шифров перестановки?
- 2. Перечислите основные разновидности шифров перестановки.
- 3. Дайте характеристику разновидностям шифров перестановки.

Шифры гаммирования (аддитивные шифры) являются самыми эффективными с точки зрения стойкости и скорости преобразований (процедур зашифрования и дешифрования). По стойкости данные шифры относятся к классу совершенных. Для зашифрования и дешифрования используются элементарные арифметические операции – открытое/зашифрованное сообщение и гамма, представленные в числовом виде, складываются друг с другом по модулю (**mod**). Напомним, что результатом сложения двух целых чисел по модулю является остаток от деления (например, $5+10 \bmod 4 = 15 \bmod 4 = 3$).

В литературе шифры этого класса часто называют потоковыми, хотя к потоковым относятся и другие разновидности шифров. В шифрах гаммирования может использоваться сложение по модулю N (общий случай) и по модулю 2 (частный случай, ориентированный на программно-аппаратную реализацию).

Сложение по модулю N. В 1888 г. француз маркиз де Виари в одной из своих научных статей, посвященных криптографии, доказал, что при замене букв исходного сообщения и ключа на числа справедливы формулы:

$$C_i = (P_i + K_i) \bmod N, \tag{6.1}$$

$$P_i = (C_i + N - K_i) \bmod N, \tag{6.2}$$

где P_i, C_i - i-ый символ открытого и зашифрованного сообщения;
N - количество символов в алфавите;
K_i - i-ый символ гаммы (ключа).

Данные формулы позволяют выполнить зашифрование / расшифрование по Вижнеру при замене букв алфавита числами согласно следующей таблице (применительно к русскому алфавиту):

Таблица 6.1. Таблица кодирования символов

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Например, для шифрования используется русский алфавит (N = 33), открытое сообщение – «АБРАМОВ», гамма – «ЖУРИХИИ». При замене символов на числа буква **А** будет представлена как 0, **Б** – 1, ..., **Я** – 32. Результат шифрования показан в следующей таблице.

Таблица 6.2. Пример аддитивного шифрования по модулю N = 33

С и м в о л	открытого сообщения, P _i	А	Б	Р	А	М	О	В
		0	1	17	0	13	15	2
	гаммы, K _i	Ж	У	Р	И	Х	И	И
		7	20	17	9	22	9	14
	шифрограммы, C _i	Ж	Ф	Б	И	В	Ч	П
		7	21	1	9	2	24	16

Сложение по модулю 2 (шифр Вернама). Значительный успех в криптографии связан с именем американца Гильберто Вернама [15]. В 1917 г. он, будучи сотрудником телеграфной компании AT&T, совместно с Мейджором Джоозефом Моборном предложил идею автоматического шифрования телеграфных сообщений. Речь шла о своеобразном наложении гаммы на знаки алфавита, представленные в соответствии с телеграфным кодом Бодо пятизначными «импульсными комбинациями». Например, буква **А** представлялась комбинацией («—» + «+»), а комбинация («+ + — + +») означала перехода от букв к цифрам. На бумажной ленте, используемой при работе телеайпа, знаку «+» соответствовало наличие отверстия, а знаку «—» - его отсутствие. При считывании с ленты металлические щупы проходили через отверстия, замыкали электрическую цепь и, тем самым, посылали в линию импульс тока.

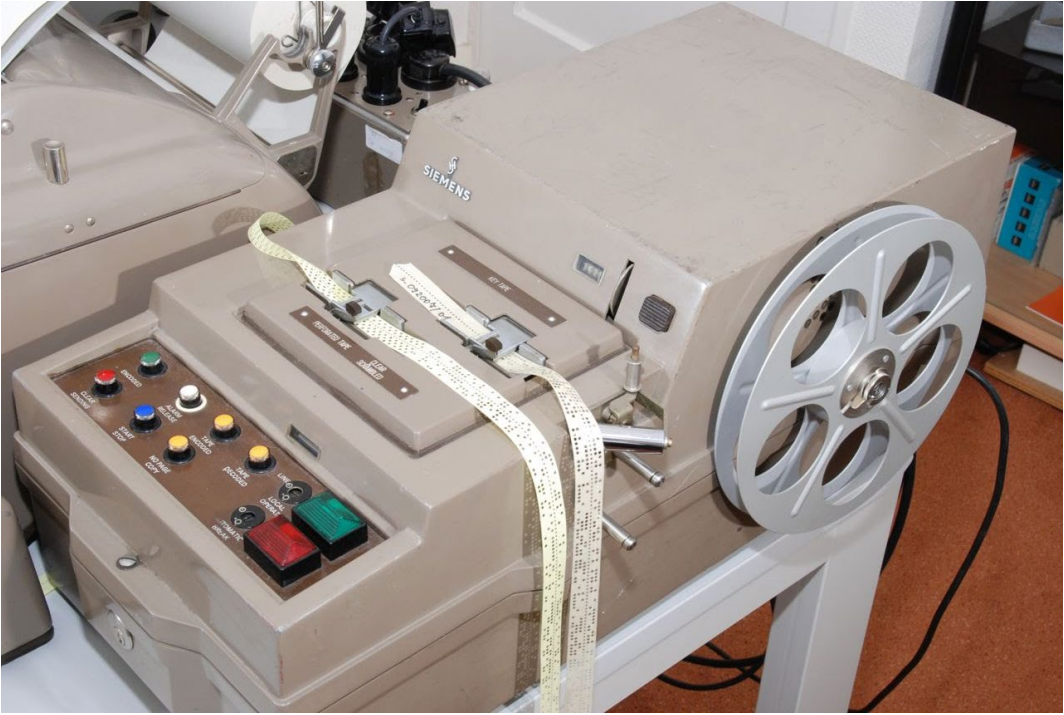


Рис.6.1. Шифровальная машина Siemens M-190 [www.cryptomuseum.com]

Вернам предложил электромеханически покомбинатно складывать «импульсы» знаков открытого текста с «импульсами» гаммы, предварительно нанесенными на ленту. Сложение проводилось «по модулю 2» (⊕, для булевых величин аналог этой операции – XOR, «Исключающее ИЛИ»). Имеется в виду, что если «+» отождествить с 1, а «—» с 0, то сложение определяется двойной арифметикой:

⊕	0	1
0	0	1
1	1	0

Таким образом, при данном способе шифрования символы текста и гаммы представляются в двоичном виде, а затем каждая пара двоичных разрядов складывается по модулю 2. Процедуры шифрования и дешифрования выполняются по следующим формулам:

$$C_i = P_i \oplus K_i, \tag{6.3}$$

$$P_i = C_i \oplus K_i. \tag{6.4}$$

Вернам сконструировал и устройство для такого сложения. Замечательно то, что процесс шифрования оказался полностью автоматизированным. Кроме того, оказались слитыми воедино процессы зашифрования / расшифрования и передачи по каналу связи.

В 1918 г. два комплекта соответствующей аппаратуры были изготовлены и испытаны. Испытания дали положительные результаты. Единственное неудовлетворение специалистов - криптографов было связано с гаммой. Дело в том, что первоначально гамма была нанесена на ленту, склеенную в кольцо. Несмотря на то, что знаки гаммы на ленте выбирались случайно, при зашифровании длинных сообщений гамма регулярно повторялась. Этот недостаток так же отчетливо осознавался, как и для шифра Вижнера. Уже тогда хорошо понимали, что повторное использование гаммы недопустимо даже в пределах одного сообщения. Попытки удлинить гамму приводили к неудобствам в работе с большим кольцом. Тогда был предложен вариант с двумя лентами, одна из которых шифровала другую, в результате чего получалась гамма, равную длине периода, равную произведению длин исходных периодов.

Шифры гаммирования стали использоваться немцами в своих дипломатических представительствах в начале 1920-х гг., англичанами и американцами – во время Второй мировой войны. Разведчики-нелегалы ряда государств использовали **шифр-блокноты**¹. Шифр Вернама применялся на правительственной «горячей линии» между Вашингтоном и Москвой, где ключевые материалы представляли собой перфорированные бумажные ленты, производившиеся в двух экземплярах [23].



Рис 6.2. Одноразовый шифровальный блокнот (СССР, ГДР, 1960-е гг.) [www.cryptomuseum.com]

Перед иллюстрацией использования шифра приведем таблицу кодов символов Windows 1251 и их двоичное представление.

Таблица 6.3. Коды символов Windows 1251 и их двоичное представление

Буква	Дес-код	Вин-код	Буква	Дес-код	Вин-код	Буква	Дес-код	Вин-код
А	192	1100 0000	Л	203	1100 1011	Ц	214	1101 0110
Б	193	1100 0001	М	204	1100 1100	Ч	215	1101 0111
В	194	1100 0010	Н	205	1100 1101	Ш	216	1101 1000
Г	195	1100 0011	О	206	1100 1110	Щ	217	1101 1001
Д	196	1100 0100	П	207	1100 1111	Ъ	218	1101 1010
Е	197	1100 0101	Р	208	1101 0000	Ы	219	1101 1011
Ж	198	1100 0110	С	209	1101 0001	Ь	220	1101 1100
З	199	1100 0111	Т	210	1101 0010	Э	221	1101 1101
И	200	1100 1000	У	211	1101 0011	Ю	222	1101 1110
Й	201	1100 1001	Ф	212	1101 0100	Я	223	1101 1111
К	202	1100 1010	Х	213	1101 0101			

Примечание. Дес-код – десятичный код символа, Вин-код – двоичный код символа.

Пример шифрования сообщения «ВОВА» с помощью ключа «ЮЛЯ» показан в следующей таблице. Так как длина ключа меньше длины открытого сообщения, то для генерации гаммы он циклически повторяется.

Таблица 6.4. Пример аддитивного шифрования по модулю 2

Открытое сообщение, P_i	Буква	В	О	В	А
	Дес-код	194	206	194	192
	Вин-код	1100 0010	1100 1110	1100 0010	1100 0000
Гамма, K_i	Буква	Ю	Л	Я	Ю
	Дес-код	222	203	223	222
	Вин-код	1101 1110	1100 1011	1101 1111	1101 1110
Шифрограмма, C_i	Дес-код	28	5	29	30
	Вин-код	0001 1100	0000 0101	0001 1101	0001 1110

Шифрование по модулю 2 обладает замечательным свойством - вместо истинной гаммы противнику можно сообщить ложную гамму, которая при наложении на шифрограмму даст осмысленное выражение.

Таблица 6.5. Пример использования ложной гаммы

Шифрограмма, C_i	Дес-код	28	5	29	30
	Вин-код	0001 1100	0000 0101	0001 1101	0001 1110
Ложная гамма, K'_i	Буква	Ю	Е	М	Б
	Дес-код	222	197	204	193
	Вин-код	1101 1110	1100 0101	1100 1100	1100 0001
Ложное открытое сообщение, P'_i	Дес-код	194	192	209	223
	Вин-код	1100 0010	1100 0000	1101 0001	1101 1111
	Буква	В	А	С	Я

Пример, представленный в таблице, иллюстрирует совершенность шифров гаммирования. Для перехваченной шифрограммы противник может подобрать большое количество гамм, дающих при расшифровании осмысленные сообщения и не имеющих ничего общего с истинным открытым сообщением. Более того, под любое ложное открытое сообщение найдется ложная гамма.

Стойкость аддитивных шифров определяется, главным образом, качеством гаммы, которое зависит от длины периода и случайности распределения по периоду [8].

Длиной периода гаммы называется минимальное количество символов, после которого последовательность начинает повторяться. **Случайность распределения символов по периоду** означает отсутствие закономерностей между появлением различных символов в пределах периода.

Для обеспечения абсолютной стойкости необходимо, чтобы последовательность символов в пределах периода гаммы обладала следующими свойствами:

- была случайной (должна отсутствовать закономерность в появлении символов гаммы);
- символы алфавита гаммы были распределены нормально (равновероятно);
- совпадала по размеру или была больше исходного открытого текста;
- применялась только один раз.

Первые два свойства (требования) проверяются с помощью различных тестов. Наиболее популярный и авторитетный из них «Набор статистических тестов для генераторов случайных и псевдослучайных чисел для криптографических приложений» (англ. NIST SP 800-22 «A statistical test suite for random and pseudorandom number generators for cryptographic applications»), включающий в себя 15 тестов.

Классический одноразовый шифровальный блокнот - большой неповторяющийся случайный набор символов ключа, написанный на листах бумаги, склеенных в блокнот. Шифровальщик при личной встрече снабжался блокнотом, каждая страница которого содержала ключ. Такой же блокнот имелся и у принимающей стороны. Использованные страницы после однократного использования уничтожались.

Несмотря на все достоинства шифров гаммирования, одной из ключевых проблем их применения на практике является получение качественных гамм. Для процедур зашифрования/дешифрования можно использовать истинно случайные или псевдослучайные гаммы (последовательности). **Псевдослучайная последовательность** – последовательность чисел, которая была вычислена по определённой процедуре, но имеет все свойства случайной последовательности чисел в рамках решаемой задачи. Отличие истинно случайных последовательностей от псевдослучайных заключается в невозможности предсказания (расчета, определения) символов в ней. Таким образом, любой алгоритмически устроенный программно-аппаратный комплекс не может генерировать истинно случайные последовательности, т.к. он работает по строго определенным правилам, а значит результат (гамма) предсказуем. Как сказал Джон фон Нейман, «всякий, кто питает слабость к арифметическим методам получения случайных чисел, грешен вне всяких сомнений» [63].

Истинно случайные гаммы могут быть получены путем оцифровки случайных физических или антропогенных процессов.

Псевдослучайные гаммы получают путем применения рекуррентных формул² или полноценных алгоритмов. При этом отсутствие истинной случайности не мешает получать криптографически стойкие последовательности, в т.ч. и с бесконечным периодом.

²**Рекуррентная формула** - формула вида $a_n = f(n, a_{n-1}, a_{n-2}, \dots, a_{n-p})$, определяющая каждый член последовательности a_n как функцию от p предыдущих членов и возможно номера члена последовательности n .

6.2.1. Генерация истинно случайных последовательностей

Как было отмечено выше, генерация истинно случайных последовательностей возможна путем оцифровки случайных физических или антропогенных процессов.

Среди **физических процессов**, которые рассматривались в качестве источника случайных последовательностей, можно выделить следующие [17, 64]:

- **дробовый шум** – беспорядочные изменения (флуктуации) принимаемого или передаваемого сигнала относительно его среднего значения, вызванные дискретностью потоков фотонов и электронов в оптических и радиоэлектронных устройствах;
- **тепловой шум** – равновесный шум, обусловленный тепловым движением носителей заряда в проводнике, в результате чего на концах проводника возникает флуктуирующая разность потенциалов. В микропроцессорах Intel с архитектурой Ivy Bridge для аппаратной генерации случайных последовательностей используется тепловой шум в кристаллах кремния [65]. Для усиления энтропии³ поток битов проходит дополнительную фильтрацию и шифрование AES в режимах CBC и CRT;



Рис.6.3. Микропроцессор Core i7-3770 с архитектурой Ivy Bridge и инструкцией генерации случайных чисел RdRand

- движение жидкостей в лавовых лампах. Компания CloudFlare, через сеть которой проходит до 10% трафика Интернета, в качестве одного из источников случайных последовательностей использует стену с сотней лавовых ламп;



Рис.6.4. «Стена энтропии» в компании CloudFlare

- движение ленточек в потоке воздуха вентилятора;



Рис.6.5. Хаотичное движение ленточек в потоке воздуха

- **радиоактивный распад** – спонтанное изменение состава или внутреннего строения нестабильных атомных ядер путём испускания элементарных частиц, гамма-квантов и/или ядерных фрагментов. Компания CloudFlare в качестве одного из источников случайных последовательностей использует радиоактивный элемент;



Рис.6.6. Счетчик Гейгера

- **электромагнитное излучение** – электромагнитные волны, возникающие при возмущении магнитного или электрического поля. Генераторы случайных последовательностей на базе квантовых явлений предлагает большое количество компаний (ID Quantique, QuintessenceLabs, ComScire и др.);



Рис.6.7. Квантовый генератор случайных чисел [www.idquantique.com/random-number-generation/overview]

- **лавинный пробой в полупроводниках** – электрический пробой p-n-перехода, вызванный лавинным размножением носителей заряда под действием сильного электрического поля;

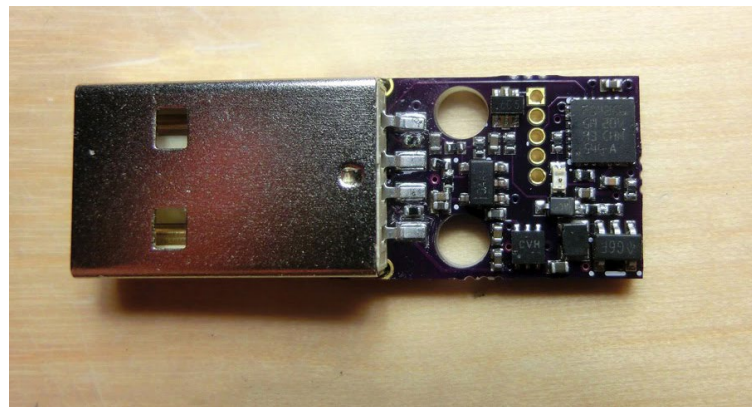


Рис.6.8. Устройство ChaosKey [altusmetrum.org/ChaosKey]

- нестабильная частота свободно работающего осциллятора. Компания RAND использовала это явление для публикации в 1955 г. книги «Миллион случайных цифр со стандартным отклонением 100 000», а компания AT&T в 1986 г. представила коммерческую микросхему-генератор [66].

К **антропогенным процессам**, используемых в качестве источника случайных последовательностей, можно отнести следующие:

- время между нажатиями клавиш;
- движения компьютерной мыши;
- изменение скорости вращения жесткого диска, вызванного турбулентностью воздуха [8];
- время между принятыми пакетами в сети (например, пинг сайта Google).

Для большинства рассмотренных выше генераторов на базе физических и антропогенных процессов характерны определенные **недостатки**:

- необходимость передачи гамм всем участникам обмена данными. Так как гамма генерируется в одном месте и она случайна, то принимающая данные сторона для расшифровки предварительно должна получить эту гамму (проблема обмена ключами);
- медленная скорость генерации числовых последовательностей;
- антропогенные процессы могут иметь скрытые зависимости – каждый пользователь обладает своим «подчерком» работы с компьютером.

В заключение обзора генераторов истинно случайных последовательностей рассматривается оригинальный метод, предложенный в 2013 г. учеными Корнельского университета [42]. Кратко принцип нового метода шифрования заключается в том, что отправитель и получатель (Алиса и Боб) во время встречи формируют общий ключ, облучая кусочки стекла изображением-паттерном с ID, (внешне он напоминает QR-код). В результате отражения и преломления, характер которого индивидуален для каждого куска стекла, у Алисы и Боба получаются собственные случайные изображения, которые затем оцифровываются (получаются ключи key_A и key_B). Из этих изображений и составляется общий ключ ($key_{AB} = key_A \oplus key_B$).

Схема генерации одного общего ключа показана на следующем рисунке.

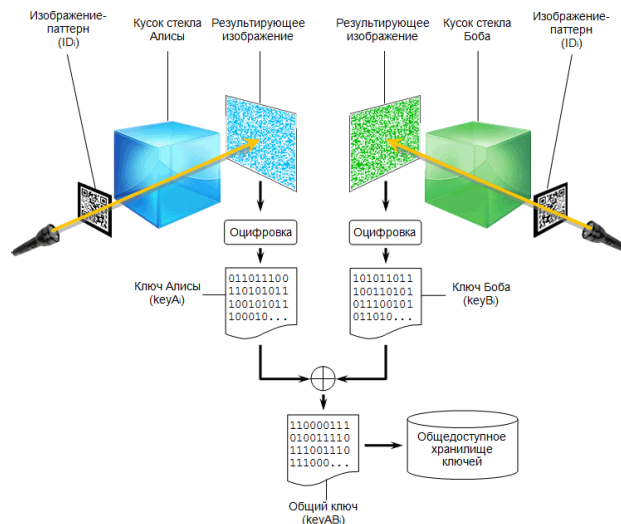


Рис.6.9. Схема генерации одного общего ключа

Как и в классической системе Вернама, каждый случайный паттерн (ключи $keyA_i$, $keyB_i$ и $keyAB_i$) можно использовать лишь однажды. В связи с этим Алиса и Боб должны сформировать достаточное количество ключей, облучая свои куски стекла разными паттернами. После генерации общие ключи $keyAB_i$ помещаются в общедоступное хранилище.

Процедура обмена шифрограммами выглядит следующим образом.

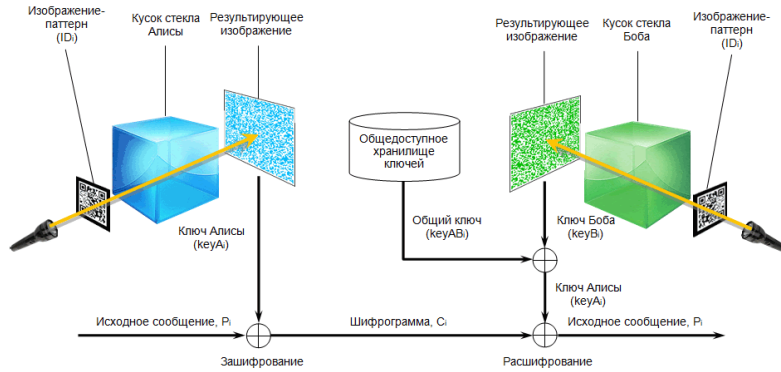


Рис.6.10. Схема зашифрования и дешифрования сообщения

- 1) Алиса выбирает паттерн с ID_1 , облучает свой кусочек стекла и оцифровывает полученное изображение, получая ключ $keyA_1$.
- 2) Исходное сообщение P_1 Алиса складывает по модулю 2 с ключом $keyA_1$ ($C_1 = P_1 \oplus keyA_1$) и отправляет шифрограмму C_1 с идентификатором паттерна ID_1 Бобу.
- 3) Боб по полученному идентификатору ID_1 из общедоступного хранилища считывает общий ключ $keyAB_1$ и, облучая паттерн с ID_1 и свой кусочек стекла, генерирует собственный ключ $keyB_1$.
- 4) Складывая по модулю 2 ключи $keyAB_1$ и $keyB_1$, Боб получает ключ $keyA_1$ ($keyA_1 = keyAB_1 \oplus keyB_1$).
- 5) Для прочтения исходного сообщения P_1 Боб складывает по модулю 2 шифрограмму C_1 и ключ $keyA_1$ ($P_1 = C_1 \oplus keyA_1$).

По утверждению авторов схемы, взломать шифр Вернама можно только украв сами кусочки полупрозрачного стекла. Однако даже в этом случае у Алисы и Боба будет около 24 часов на определение факта кражи, поскольку злоумышленнику потребуется определить структуру стеклянного образца. Другие возможные проблемы при использовании данной схемы:

- потеря кусочка стекла;
- появление сколов и царапин на стекле;
- необходимость точного взаимного расположения и ориентации источника света, изображения-паттерна, кусочка стекла и полотна с результирующим изображением при оцифровке гаммы.

³**Информационная энтропия** – мера неопределённости или непредсказуемости информации, неопределённость появления какого-либо символа первичного алфавита.

6.2.2. Генерация псевдослучайных последовательностей

Генераторы псевдослучайных последовательностей получили наибольшее распространение. По схеме использования они делятся на синхронные и самосинхронизирующиеся [8, 23].

Схема шифрования с использованием **синхронных генераторов** представлена на следующем рисунке.

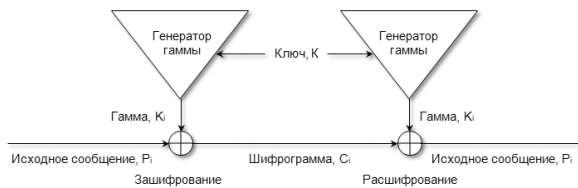


Рис.6.11. Схема шифрования с использованием синхронных генераторов

При этом генератор гаммы, как правило, состоит из трех основных блоков.

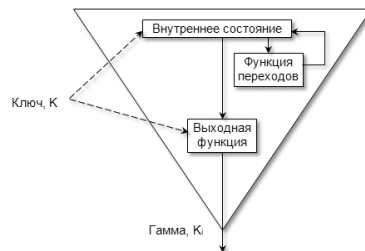


Рис.6.12. Устройство генератора гаммы с внутренней обратной связью

Внутреннее состояние описывает текущее состояние генератора гаммы. **Начальное внутреннее состояние**, как правило, определяется ключом K . Два генератора, с одинаковым ключом и одинаковым внутренним состоянием, создают одинаковые гаммы. **Функция переходов** считывает текущее внутреннее состояние и генерирует новое внутреннее состояние. **Выходная функция** считывает внутреннее состояние и генерирует бит (биты) гаммы K_i .

В другой разновидности, так называемых **генераторах типа счетчик**, отсутствует блок с функцией переходов. В отличие от генераторов с обратной связью, они позволяют вычислить i -й бит гаммы, не вычисляя всех предыдущих битов. Для этого генератор устанавливается в i -е внутреннее состояние, после чего вычисляется соответствующий ему i -й бит гаммы. Это свойство полезно использовать для обеспечения произвольного доступа к файлам данных, что позволяет расшифровывать отдельный фрагмент данных, не расшифровывая файл полностью.

В синхронном генераторе гамма генерируется независимо от потока сообщения. На шифрующей стороне генератор гаммы последовательно выдает биты гаммы K_i . На расшифровывающей стороне другой генератор гаммы один за другим выдает идентичные биты гаммы. Эта схема работает нормально, если оба генератора синхронизированы.

Недостаток синхронного генератора. Если один из генераторов пропускает один из циклов или бит шифрограммы теряется при передаче, то все символы шифрограммы, следующие за ошибкой, расшифровываются некорректно. В этом случае отправитель и получатель должны синхронизировать генераторы и заново передать некорректно расшифрованную часть сообщения.

Достоинство синхронного генератора. Отсутствие распространения ошибок. Если во время передачи бит C_i изменит свое значение, что намного вероятнее его потери, то некорректно расшифровывается только один измененный бит.

В **самосинхронизирующихся генераторе** каждый бит гаммы представляет собой функцию фиксированного числа предыдущих битов шифрограммы. Используемые при таком шифровании генераторы гаммы называют **генераторами с обратной связью по шифрограмме (шифртексту)**.

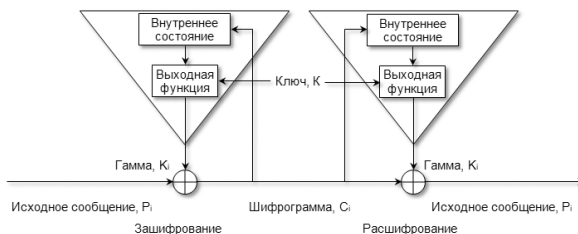


Рис.6.13. Схема шифрования с использованием самосинхронизирующихся генераторов гаммы

Внутреннее состояние зависит от **n** предыдущих битов шифрограммы. Каждое сообщение начинается случайным заголовком (**вектор инициализации, синхропосылка**) длиной **n** бит, после прохождения которого оба генератора гаммы синхронизируются.

Недостатки самосинхронизирующегося генератора.

1. Распространение ошибки. Для каждого бита шифрограммы, искаженного при передаче, расшифровывающий генератор выдает **n** некорректных битов гаммы. Следовательно, измененный бит влияет на внутреннее состояние, каждой ошибке шифрограммы будет соответствовать **n** ошибок открытого текста.
2. При потере бита C_i необходимо заново передать часть сообщения, но в отличие от синхронных генераторов, синхронизация намного проще.

Для генерации псевдослучайных последовательностей используют рекуррентные формулы или полноценные алгоритмы. В первом случае члены числовой последовательности не только рассчитываются рекуррентно, но и впоследствии становятся частью гаммы. Во втором случае для генерации гаммы используются более сложные правила, в т.ч. для повышения энтропии гаммы могут применять хеш-функции и шифрование.

В качестве иллюстрации ниже приведены некоторые из них.

А) Рекуррентные формулы:

- линейный конгруэнтный генератор;
- инверсный конгруэнтный генератор;
- аддитивный генератор;
- регистр сдвига с линейной обратной связью.

А.1) Линейный конгруэнтный генератор – генератор псевдослучайных чисел, в котором новый член последовательности рассчитывается на базе предыдущего через линейную зависимость. В общем случае линейный конгруэнтный генератор задается выражением:

$$X_{i+1} = (a \cdot X_i + b) \bmod m,$$
 (6.5)

где a, b и m – некоторые коэффициенты.

Алгоритм RANDU - один из вариантов линейного конгруэнтного генератора псевдослучайных чисел, десятилетиями использовавшийся на мейнфреймах. Он определяется рекуррентным соотношением:

$$X_{i+1} = (65539 \cdot X_i) \bmod 2^{31},$$
 (6.6)

где X_0 - нечётное.

Пример псевдослучайной последовательности, порождаемой алгоритмом RANDU при начальном значении $X_0 = 1$:

1
65 539
393 225
1 769 499
7 077 969
26 542 323
...
388 843 697
238 606 867
79 531 577
477 211 307
1 (повтор для элемента № 536 870 913)

К сожалению, линейные конгруэнтные генераторы нельзя использовать в криптографии, т.к. они предсказуемы. Впервые линейные конгруэнтные генераторы были взломаны Джимом Ридсом, а затем Джоан Бояр [8]. Ей удалось также вскрыть **квадратичные генераторы**

$$X_{i+1} = (a \cdot X_i^2 + b \cdot X_i + c) \bmod m$$
 (6.7)

и кубические генераторы

$$X_{i+1} = (a \cdot X_i^3 + b \cdot X_i^2 + c \cdot X_i + d) \bmod m.$$
 (6.8)

А.2) Инверсный конгруэнтный генератор (генератор Эйхенауэра – Лена) – генератор псевдослучайных чисел, в котором новый член последовательности рассчитывается как обратное число к предыдущему по модулю. Общая формула генератора выглядит следующим образом:

$$X_{i+1} = (a \cdot X_i^{-1} + b) \bmod m,$$
 (6.9)

где a, b и m – некоторые коэффициенты, $0 \leq a < m, 0 \leq b < m$.

Как и в случае с линейным конгруэнтным генератором получаемая последовательность периодична с максимальным периодом m. Данные генераторы считаются более стойкими, но требует значительных вычислений.

А.3) Аддитивный генератор (запаздывающий генератор Фибоначчи) – генератор псевдослучайных чисел, в котором новый член последовательности зависит более чем от одного из предшествующих. Одна из ранних реализаций генератора последовательности Фибоначчи с запаздыванием была предложена 1958 г. Дж. Ж. Митчелом и Д. Ф. Муром:

$$X_{i+1} = (X_{i-a} + X_{i-b}) \bmod m,$$
 (6.10)

где a = 24, b = 55 – запаздывание, b > a ≥ 1;
 $X_0 \dots X_{54}$ – произвольные целые числа;
m – чётное число.

Более сложные реализации аддитивных генераторов применяются в алгоритмах Fish, Pike, Mush и др.

А.4) Регистр сдвига с линейной обратной связью (РСЛОС) – упорядоченный набор битов, у которого значение входного (вдвигаемого слева, старшего) бита равно линейной булевой функции от значений остальных битов регистра до сдвига. Теорию последовательности регистров сдвига разработал в 1965 г. главный криптограф норвежского правительства Эрнст Селмер [8].

Длиной регистра называется количества битов в нем. В качестве булевой функции для РСЛОС чаще всего используют сложение по модулю 2. Такие РСЛОС обычно записывают в виде многочлена (полинома) или упорядоченной последовательности. Запись $x^8 + x^4 + x^3 + x^2 + 1$ или (8, 4, 3, 2, 0) означает, что длина регистра 8 битов, а входной бит рассчитывается по формуле $b_7 = b_4 \oplus b_3 \oplus b_2 \oplus b_0$ (для битов нумерация начинается справа и с нулевой позиции). Выходной (выдвигаемый справа, младший) бит будет являться частью генерируемой гаммы. Расчет требуемой гаммы осуществляется в цикле, на каждой итерации которого выполняются следующие операции.

1. Добавление выходного бита b_0 к гамме.
2. Расчет входного бита b_{n-1} по формуле.
3. Сдвиг битов регистра вправо на одну позицию.
4. Занесение рассчитанного входного бита b_{n-1} в позицию n-1.

В следующей таблице приведен пример генерации гаммы для регистра, инициализированного значением 10001100₂.

Таблица 6.6. Пример генерации гаммы для РСЛОС $x^8 + x^4 + x^3 + x^2 + 1$

№ п/п	Исходное состояние регистра	Бит гаммы, b_0	Входной бит, $b_7 = b_4 \oplus b_3 \oplus b_2 \oplus b_0$	Сдвиг регистра вправо на одну позицию	Занесение входного бита b_7 в регистр
0	10001100	0	$0 \oplus 1 \oplus 1 \oplus 0 = 0$	1000110	01000110
1	01000110	0	$0 \oplus 0 \oplus 1 \oplus 0 = 1$	0100011	10100011
2	10100011	1	$0 \oplus 0 \oplus 0 \oplus 1 = 1$	1010001	11010001
3	11010001	1	$1 \oplus 0 \oplus 0 \oplus 1 = 0$	1101000	01101000
4	01101000	0	$0 \oplus 1 \oplus 0 \oplus 0 = 1$	0110100	10110100
...	...	...	...	...	...
Гамма		00110...			

Для регистра длиной n максимальное количество состояний (период гаммы) составляет $2^n - 1$ (Это число равно $2^n - 1$, а не 2^n , поскольку заполнение РСЛОС нулями влечет вывод регистром бесконечной последовательности нулей, что совершенно бесполезно). Для получения такого максимального периода многочлен должен быть примитивным по модулю 2. **Примитивный многочлен степени n** – неприводимый многочлен, который является делителем $x^{2^n-1} + 1$, но не является делителем $x^d + 1$ для всех d, являющихся делителями $2^n - 1$. Чем больше битов регистра используются для расчета входного бита, тем лучше (повышается стойкость). Многочлены с большим количеством членов называют **плотными**, с малым – **разреженными**.

РСЛОС обладают высокой скоростью генерации чисел, хорошими статистическими свойствами, а также возможностью простой реализации на аппаратном уровне. Исследователями предложено несколько десятков различных вариантов реализации генераторов на базе РСЛОС, в т.ч. с применением комбинации нескольких РСЛОС одновременно и разных функций расчета входного или выходного бита (регистры сдвига с нелинейной обратной связью, обобщенной обратной связью, обратной связью по переносу и т.д.).

Б) Алгоритмы:

- алгоритм Блюм - Блюм - Шуба;
- RC4;
- Trivium;
- генератор на базе иррациональных чисел.

Б.1) Алгоритм Блюм - Блюм - Шуба (англ. Algorithm Blum - Blum - Shub, BBS) предложен в 1986 г. Ленор Блюм, Мануэлем Блюмом и Майклом Шубом.

Рекуррентная формула BBS выглядит следующим образом:

$$X_{i+1} = X_i^2 \bmod m, \tag{6.11}$$

где $m = p * q$ – является произведением двух больших простых p и q , сравнимых с 3 по модулю 4.

На каждом шаге алгоритма гамма получаются из X_i путём взятия либо паритетного бита, либо одного или более младших битов X_i . Начальное значение X_0 должно быть **взаимно простым**⁴ с m – в противном случае у генерируемой последовательности быстро появляется период.

Пример с использованием двух малых простых чисел.

$p = 7 \ (7 \bmod 4 = 3)$ и $q = 19 \ (19 \bmod 4 = 3)$.
 $m = 7 * 19 = 133$.
 $X_0 = 53$.

Таблица 6.7. Пример генерации гаммы по алгоритму BBS

№ п/п	X		Четный паритетный бит	Младший бит	2 младших бита
	Дес-код	Bin-код			
0	53	110101	0	1	01
1	16	10000	1	0	00
2	123	1111011	0	1	11
3	100	1100100	1	0	00
4	25	11001	1	1	01
...	...	...	...	...	...
Гамма			01011...	10101...	0100110001...

Как было отмечено выше, X_0 должно быть взаимно простым с m . Если для генерации последовательности с параметрами $p = 7$, $q = 19$ и $m = 133$ выбрать $X_0 = 57 = 3 * 19$, то она будет состоять из одних $X_i = 57 \ (57^2 \bmod 133 = 57)$. Таким образом период последовательности будет равным 1, что не лучшим образом сказывается на качестве гаммы. Слишком малый период может возникать и в случае, когда X_0 и m взаимно просты. Например, если при тех же параметрах выбрать $X_0 = 130$, то последовательность будет выглядеть: 130, 9, 81, 44, 74, 23, 130, ...

Особенностью этого алгоритма является то, что для получения X_n обязательно вычислять все $n - 1$ предыдущих чисел, если известно начальное состояние генератора X_0 и числа p и q , то n -ное значение может быть вычислено по формуле:

$$X_n = X_0^{2^n \bmod ((p-1)(q-1))} \bmod m. \tag{6.12}$$

Б.2) RC4 (от англ. Rivest cipher или Ron's code) был создан сотрудником компании «RSA Security» Рональдом Ривестом в 1987 г. В течение семи лет шифр являлся коммерческой тайной, и точное описание алгоритма предоставлялось только после подписания соглашения о неразглашении, но в сентябре 1994 г. его описание было анонимно отправлено в список рассылки «Cyrpherpunks» [17].

Этап 1. Инициализация S-блока.

Перед генерацией гаммы выполняется инициализация **S-блока** длиной **L_s**. Обычно **L_s** выбирается кратно 8 битов ($2^8 = 256$, $2^{16} = 65536$ и т.п.). Для инициализации используется ключ **K** длиной **L_K** от 40 до 2048 битов по следующему алгоритму.

```
1. Цикл А. Для i := 0 до Ls - 1
    1.1. S[i] := i
2. j := 0
3. Цикл В. Для i := 0 до Ls - 1
    3.1. j := (j + S[i] + K[i mod LK]) mod Ls
    3.2. Поменять местами S[i] и S[j]
```

Этап 2. Генерация гаммы.

Непосредственная генерация гаммы выполняется циклически блоками по **L_s** битов до достижения необходимой длины псевдослучайной последовательности **L_g**. Алгоритм генерации следующий.

```
1. i := 0
2. j := 0
3. L := 0
4. Цикл. Пока L < Lg
    4.1. i := (i + 1) mod Ls
    4.2. j := (j + S[i]) mod Ls
    4.3. Поменять местами S[i] и S[j]
    4.4. t := (S[i] + S[j]) mod Ls
    4.5. Блок гаммы := S[t]
    4.6. L := L + Ls
```

RC4 получил широкое распространение в криптосистемах и протоколах, в частности [17]:

- WEP (англ. Wired Equivalent Privacy) — алгоритм для обеспечения безопасности сетей Wi-Fi;
- WPA (англ. Wi-Fi Protected Access) — обновленный алгоритм сертификации устройств сетей Wi-Fi;
- BitTorrent protocol encryption — протоколы пиринговых файлообменных сетей;
- SSL (англ. Secure Sockets Layer) — криптографический протокол передачи данных в сети;
- Kerberos — сервер аутентификации Kerberos;
- PDF (англ. Portable Document Format) — межплатформенный формат электронных документов, разработанный фирмой Adobe Systems;
- Skype — программное обеспечение IP-телефонии;
- и др.

Обнаруженные уязвимости в стандартной реализации RC4 привели к отказу от его использования в некоторых криптосистемах и протоколах, а также появлению различных его модификаций: RC4A, RC4+, VMPC, Spritz.

Б.3) Trivium был представлен в 2008 г. как часть европейского проекта eSTREAM по профилю 2 (аппаратно ориентированные шифры) и в настоящий момент имеет статус международного стандарта «ISO/IEC 29192-3:2012. Информационные технологии - Методы безопасности - Легкая криптография - Часть 3: Поточные шифры» (англ. «ISO/IEC 29192-3:2012. Information technology - Security techniques - Lightweight cryptography - Part 3: Stream ciphers»). Авторами генератора (шифра) являются Кристоф Де Канньер и Барт Пренел [17].

По аналогии с RC4 процедура выработки гаммы состоит из двух этапов: инициализации S-блока и непосредственно генерации гаммы.

Этап 1. Инициализация S-блока.

Длина **S-блока** составляет 288 битов. При этом он условно делится на 3 части длинами 93, 84 и 111 битов. В первую часть **S₁** заносится 80-битовый ключ **K** с добавлением 13 нулевых битов, во вторую часть **S₂** заносится 80-битовый вектор инициализации **IV** с добавлением 4 нулевых битов и в последнюю часть **S₃** заносятся нулевые биты за исключением трех последних единичных битов. После первоначальной инициализации в цикле осуществляется связывание битов из разных частей со сдвигами битов вправо в каждой из них. Весь алгоритм инициализации выглядит следующим образом.

```
1. S1 = (s1, s2, ..., s93) := (K1, K2, ..., K80, 0, ..., 0)
2. S2 = (s94, s95, ..., s177) := (IV1, IV2, ..., IV80, 0, ..., 0)
3. S3 = (s178, s179, ..., s288) := (0, ..., 0, 1, 1, 1)
4. Цикл. Для i := 1 до 288
    4.1. t1 := s66 ⊕ (s91 ∧ s92) ⊕ s93 ⊕ s171
    4.2. t2 := s162 ⊕ (s175 ∧ s176) ⊕ s177 ⊕ s264
    4.3. t3 := s243 ⊕ (s286 ∧ s287) ⊕ s288 ⊕ s69
    4.4. Сдвиг первой части на один бит вправо S1 := (_, s1, s2, ..., s92)
    4.5. Занесение t3 в первую позицию первой части S1 := (t3, s1, s2, ..., s92)
    4.6. Сдвиг второй части на один бит вправо S2 := (_, s94, s95, ..., s176)
    4.7. Занесение t1 в первую позицию второй части S2 := (t1, s94, s95, ..., s176)
    4.8. Сдвиг третьей части на один бит вправо S3 := (_, s178, s179, ..., s287)
```


4.9. Занесение t_2 в первую позицию третьей части $S_3 := (t_2, s_{178}, s_{179}, \dots, s_{287})$

Этап 2. Генерация гаммы.

Для генерации гаммы длиной L_g в каждой итерации цикла на основе 15 битов **S-блока** вычисляется один бит гаммы и выполняются операции, идентичные рассмотренным в инициализации **S-блока**. Алгоритм генерации следующий.

```
1. L := 0
2. Цикл. Пока L < Lg
    2.1. Бит гаммы :=  $s_{66} \oplus s_{93} \oplus s_{162} \oplus s_{177} \oplus s_{243} \oplus s_{288}$ 
    2.2.  $t_1 := s_{66} \oplus (s_{91} \wedge s_{92}) \oplus s_{93} \oplus s_{171}$ 
    2.3.  $t_2 := s_{162} \oplus (s_{175} \wedge s_{176}) \oplus s_{177} \oplus s_{264}$ 
    2.4.  $t_3 := s_{243} \oplus (s_{286} \wedge s_{287}) \oplus s_{288} \oplus s_{69}$ 
    2.5. Сдвиг первой части на один бит вправо  $S_1 := (_, s_1, s_2, \dots, s_{92})$ 
    2.6. Занесение  $t_3$  в первую позицию первой части  $S_1 := (t_3, s_1, s_2, \dots, s_{92})$ 
    2.7. Сдвиг второй части на один бит вправо  $S_2 := (_, s_{94}, s_{95}, \dots, s_{176})$ 
    2.8. Занесение  $t_1$  в первую позицию второй части  $S_2 := (t_1, s_{94}, s_{95}, \dots, s_{176})$ 
    2.9. Сдвиг третьей части на один бит вправо  $S_3 := (_, s_{178}, s_{179}, \dots, s_{287})$ 
    2.10. Занесение  $t_2$  в первую позицию третьей части  $S_3 := (t_2, s_{178}, s_{179}, \dots, s_{287})$ 
    2.11. L := L + 1
```

Существуют упрощенные модификации генератора гаммы Univium, Bivium, Trivium-toy и Bivium-toy.

Б.4) Иррациональное число – вещественное число, которое не является рациональным, т.е. не может быть представлено в виде обыкновенной дроби $\pm \frac{m}{n}$, где m, n – натуральные числа. К наиболее известным иррациональным числам относятся $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\ln 2$, e и π [17].

Иррациональное число может быть представлено в виде бесконечной непериодической десятичной дроби. Другими словами в дробной части такого числа бесконечное количество цифр и в их записи отсутствует период. Это говорит о том, что любая конечная случайная числовая последовательность рано или поздно обязательно будет являться частью иррационального числа. Данные обстоятельства могут сделать иррациональные числа ценным источником псевдослучайных последовательностей. Для генерации гаммы можно будет указать номер позиции в дробной части, с которой следует начать выбирать последовательность цифр для гаммы. Очевидно, что данный номер должен быть очень большим, чтобы потенциальный противник не смог за приемлемое время его определить методом перебора.

К **проблемам** использования иррациональных чисел в качестве псевдослучайных числовых последовательностей относятся:

- отсутствие доказательства нормальности чисел;
- относительно сложный алгоритм расчета, подразумевающий, как правило, использование рекуррентных процедур;
- наличие в своем составе «плохих» последовательностей (например, последовательностей требуемой для гаммы длины, но состоящих из одних нулей или имеющих легко определяемый период).

В качестве примера рассмотрим число π .

Равновероятность появления цифр в записи ($\approx$ нормальность) числа π не доказана, хотя анализ первых 200 млрд. десятичных цифр говорит в пользу этого.

Таблица 6.8. Количество появлений десятичных цифр в первых 200 млрд. знаках числа π

Цифра	Количество появлений
0	20 000 030 841
1	19 999 914 711
2	20 000 136 978
3	20 000 069 393
4	19 999 921 691
5	19 999 917 053
6	19 999 881 515
7	19 999 967 594
8	20 000 291 044
9	19 999 869 180

Для расчета цифр числа π можно использовать приближенные формулы, ряды, пределы, интегралы и т.п. В первом случае получается неточное значение и, как правило, с периодом («теряется» иррациональность), в других требуется сложная процедура расчета с получением всех предшествующих цифр, начиная с первой.

Важным достижением в области расчетов числа π стала формула Бэйли – Боруэйна – Плаффа, открытая в 1997 г. Саймоном Плаффом и названная в честь авторов статьи, в которой она впервые была опубликована [67].

$$\pi = \sum_{k=0}^{\infty} \frac{1}{16^k} \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6} \right). \quad (6.13)$$

Эта формула примечательна тем, что она позволяет извлечь любую конкретную шестнадцатеричную или двоичную цифру числа π без вычисления предыдущих. К сожалению, расчеты по этой формуле достаточно медлительны, но это уже значительный шаг вперед для использования иррациональных чисел в практической криптографии.

⁴**Взаимно простые числа** – числа, не имеющие общих делителей, кроме 1, т.е. наибольший общий делитель которых равен 1.

6.3. Отличие ключа от гаммы

Очень часто понятия «ключ» и «гамма» отождествляют, но между ними есть принципиальные отличия. Напомним, **ключ** – минимально необходимая информация (за исключением сообщения, алфавитов и алгоритма), необходимая для шифрования и дешифрования сообщений. **Гаммой** является вся числовая последовательность, используемая для шифрования или дешифрования сообщения с длиной не менее этого сообщения.

Для иллюстрации отличий приведена следующая таблица.

Таблица 6.9. Отличия ключа от гаммы

Метод генерации гаммы	Ключ	Гамма
На базе случайных физических или антропогенных процессов	Ключ соответствует гамме	
На базе слова или фразы (см. табл. 6.2 и 6.4)	Слово или фраза	Циклически повторяющееся слово или фраза
Линейный или инверсный конгруэнтный генератор	Начальное число и коэффициенты формул	Генерируемая числовая последовательность
Регистр сдвига с линейной обратной связью	Вид полинома и исходное состояние регистра	Генерируемая числовая последовательность
RC4	Ключ К	Числовая последовательность из частей S-блока
На базе числа π	Номер начальной позиции в дробной части, с которой выбираются цифры числа π	Последовательность цифр числа π , начиная с заданной позиции

6.4. Стандарты и спецификации США

Развитая система стандартов и спецификаций по генерации и тестированию псевдослучайных последовательностей существует в США. ANSI (Американский национальный институт стандартов – англ. American national standards institute) и NIST (Американский национальный институт стандартизации – англ. National Institute of Standards and Technology) разработали следующие документы:

- стандарты ANSI серии X9.82:
 - ANSI X9.82 «Random Number Generation. Part 1: Overview and Basic Principles» (рус. «Генерация случайных чисел. Часть 1: Обзор и основные принципы»);
 - ANSI X9.82 «Financial Services - Random Number Generation. Part 2: Entropy Sources» (рус. «Финансовые услуги – Генерация случайных чисел. Часть 2: Источники энтропии»);
 - ANSI X9.82 «Random Number Generation. Part 3: Deterministic Random Bit Generators» (рус. «Генерация случайных чисел. Часть 3: Детерминированные генераторы случайных битов»);
 - ANSI X9.82 «Random Number Generation. Part 4: Random Bit Generator Constructions» (рус. «Генерация случайных чисел. Часть 4: Конструкции генератора случайных битов»);
- специальные публикации NIST серии 800:
 - NIST SP 800-22 Rev.1a «A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications» (рус. «Набор статистических тестов для генераторов случайных и псевдослучайных чисел для криптографического приложений»);
 - NIST SP 800-90A «Recommendation for Random Number Generation Using Deterministic Random Bit Generators» (рус. «Рекомендации для генерации случайных чисел с использованием детерминированных генераторов случайных битов»).

1. В чем заключается основная идея криптографических преобразований аддитивных шифров?
2. Назовите основные характеристики гаммы.
3. При каких условиях применения гаммы аддитивный шифр можно считать совершенным.
4. Опишите схемы шифрования с использованием синхронных и самосинхронизирующихся потоковых шифров.

7. КВАНТОВОЕ ШИФРОВАНИЕ

7.1. Основы квантовой физики

Квант (от лат. quantum - «сколько») - неделимая порция какой-либо величины в физике. В основе понятия лежит представление о том, что некоторые физические величины могут принимать только определенные (дискретные) значения, величина которых кратна некоторому минимальному значению (постоянной Планка). **Постоянная Планка** (квант действия) - коэффициент, связывающий величину энергии электромагнитного излучения с его частотой (или некоторую другую пару физических величин)

$$h = \frac{E}{\nu} = 6.62606957(29) * 10^{-34}, \text{ Дж*с} \quad (7.1)$$

где E - энергия электромагнитного излучения, Дж;
 ν - частота электромагнитного излучения, 1/с.

На текущий момент большинство ученых считает, что на макроскопическом уровне (звезд, людей, молекул) действуют законы классической физики, а на микроскопическом (элементарных частиц – кварков, фотонов, электронов) – иные, в т.ч. и квантовой. В рамках квантовой физики любая элементарная частица рассматривается как квант возбуждения поля, характерной для этой частицы. Квантовые поля могут взаимодействовать между собой, в результате чего кванты (частицы) могут превращаться друг в друга.

Одной из элементарных частиц является фотон. **Фотон** (от др.-греч. φῶς - «свет») - квант электромагнитного излучения (электромагнитная волна) с нулевыми массой покоя и зарядом. Согласно современным представлениям фотону свойственен **корпускулярно-волновой дуализм**. С одной стороны, фотон демонстрирует свойства волны в явлениях дифракции¹ и интерференции² в том случае, если размеры препятствий сравнимы с длиной волны фотона. С другой стороны, процессы взаимодействия фотонов с веществом (излучение и поглощение) можно успешно истолковать только на основе представлений о нем, как о дискретной частице.

Излучение светящегося тела можно представить как потоки фотонов, направленных от него во все стороны.



Рис.7.1. Излучение светящегося тела

Эти потоки распространяются, как правило, вдоль прямолинейного луча, за исключением прохода малых препятствий (см. дифракцию) или вблизи массивных тел (планет, звезд). Т.о. поток фотонов можно представить как набор электромагнитных волн, каждая из которых колеблется (поляризована) в одной

ПЛОСКОСТИ.

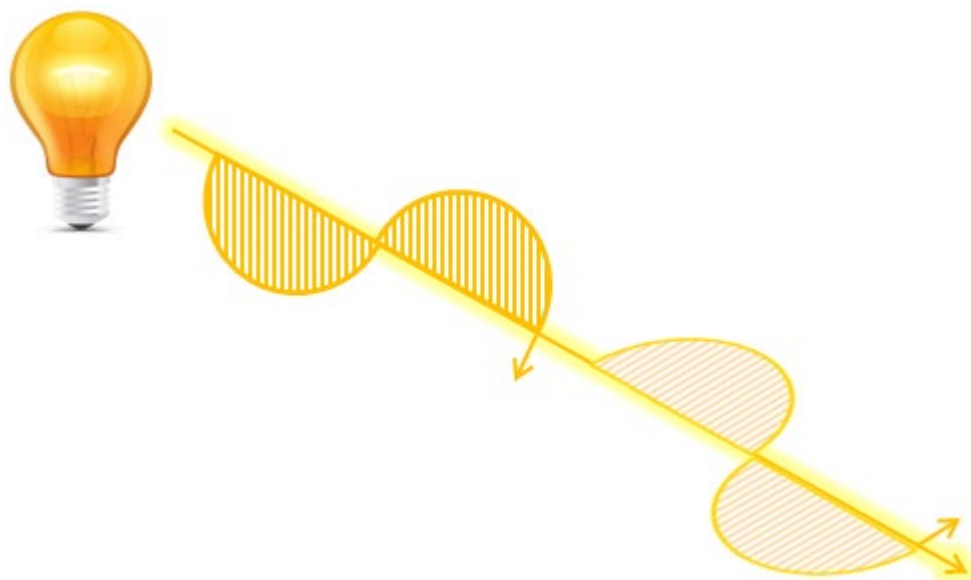


Рис.7.2. Поток из двух фотонов (электромагнитных волн)

При пропускании оптического излучения через **линейный поляризатор** (например, призму Глана) на выходе можно получить поток фотонов с требуемой поляризацией. Образно этот процесс можно представить, как прохождение фотонов через фильтр с плоским отверстием, который проходит только часть фотонов – те, плоскость поляризации которых совпадает с ориентацией отверстия фильтра.

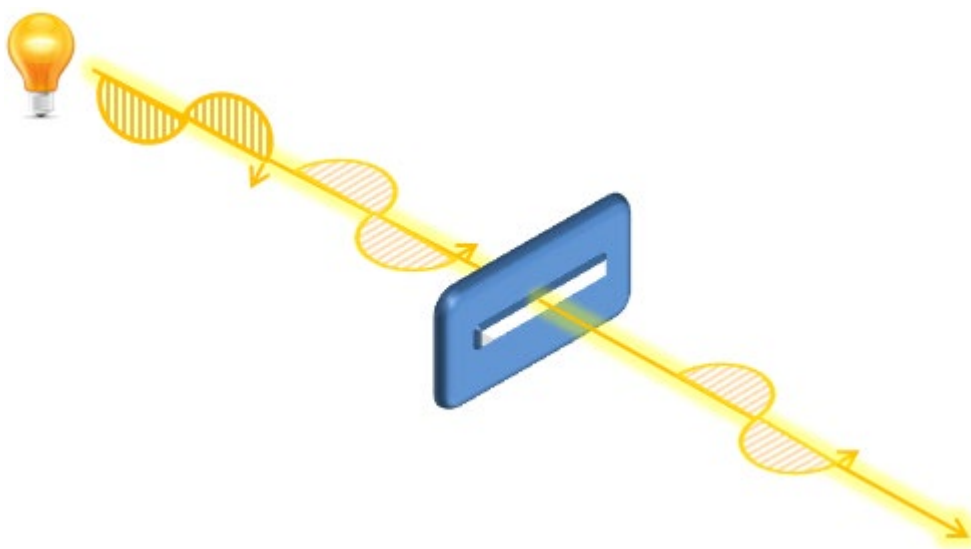


Рис.7.3. Прохождение потока фотонов сквозь фильтр

Если сгенерировать поток фотонов с требуемой поляризацией можно, то точно определить поляризацию произвольно перехваченных фотонов современные измерительные устройства не позволяют. Это обстоятельство и позволило использовать квантовую механику для шифрования информации.

Для кодирования информации, представленной в битовом виде, достаточно двух линейных поляризаторов с разными плоскостями поляризации. Фотоны, ориентированные в одной плоскости будут соответствовать «1», в другой – «0». На этом принципе основана работа передающего устройства (генератора фотонов).

Принимающее устройство может быть построено на базе линейного поляризатора или **поляризационной разделительной призмы**.

В первом случае, если принятый фотон проходит сквозь поляризатор и регистрируется стоящим за ним фотодетектором, то он идентифицируется как «1», в противном случае – как «0».

Во втором случае, при прохождении фотона через призму он перенаправляется на один из двух фотодетекторов, соответствующих двум взаимно перпендикулярным плоскостям поляризации (**базису**). Перенаправление выполняется на тот фотодетектор, чья плоскость поляризации наиболее близка к плоскости поляризации принятого фотона. Если передающая и принимающая стороны используют одинаковый базис поляризации (например, горизонтально-вертикальный), то принимающая сторона будет однозначно идентифицировать поступающие фотоны (например, с горизонтальной поляризацией как «1», с вертикальной - как «0»). Если принимающая сторона будет использовать другой базис поляризации, то вероятность правильной идентификации снижается. В частности, если у принимающей стороны базис будет повернут на 45° относительно передающей, то вероятность правильной идентификации будет примерно 50%.

¹**Дифракция** (лат. diffractus - буквально разломанный, переломанный) – отклонение света (световых волн, фотонов) от прямолинейного распространения при прохождении сквозь малые отверстия или огибании малых препятствий.

²**Интерференция света** – перераспределение интенсивности света в результате наложения (суперпозиции) нескольких световых волн.

7.2. Основы квантового шифрования

7.2.1. Шифрования с использованием линейных поляризаторов на принимающей стороне

Для отправки и приема фотонов стороны могут использовать четыре фильтра (поляризатора).

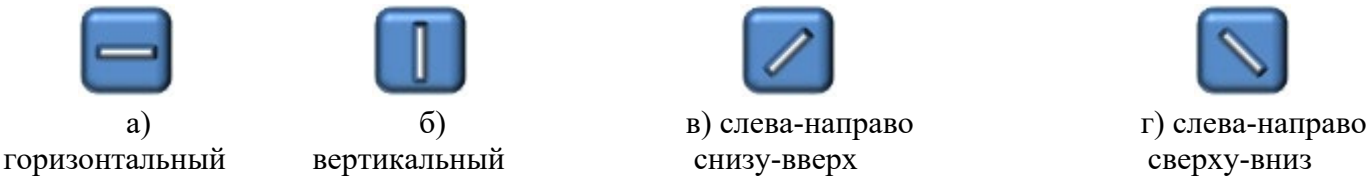


Рис.7.4. Фильтры для отправки и приема фотонов

Если передающая и принимающая стороны для одного фотона (бита информации) будут использовать одинаковые фильтры, то он будет регистрироваться фотодетектором на принимающей стороне и идентифицироваться как «1», в противном случае – как «0».

Для обмена секретной информацией сторонам достаточно использовать два фильтра. При этом они заранее оговаривают порядок их использования на принимающей стороне, но он должен быть случайным для потенциального противника. Этот порядок будет являться ключом шифрования/дешифрования. Отправитель, зная последовательность применения фильтров получателем (ключ), для отправки сообщения должен применить соответствующий фильтр, чтобы получатель правильно идентифицировал принятый фотон.

В следующей таблице приведен пример отправки сообщения «00110101₂» при использовании получателем горизонтального и вертикального фильтров.

Таблица 7.1. Пример отправки и приема сообщения

Посылаемое сообщение, бит	0	0	1	1	0	1	0	1
Фильтры, применяемые получателем (ключ)								
Фильтры, выбираемые отправителем								
Принятое сообщение, бит	0	0	1	1	0	1	0	1

Т.к. противник не знает порядок использования фильтров, то он не может правильно интерпретировать перехваченные фотоны.

В целях обеспечения стойкости данной схемы шифрования ключ, как и в шифрах гаммирования, должен быть истинно случайным и одноразовым. Для генерации таких ключей можно использовать генераторы гамм. Например, если в гамме очередной бит равен «1», то получатель должен использовать горизонтальный фильтр, иначе – вертикальный. Для генерации ключа (гаммы) можно использовать квантовые протоколы обмена ключами (например, протокол BB84).

Для повышения стойкости шифра рекомендуется менять пары фильтров на стороне получателя. Это позволит также определить факт прослушивания канала связи. При перехвате фотона противник вынужден создать его копию (клон) и послать ее законному получателю. Если противник будет использовать не ту пару фильтров или разделительную призму, то поляризацию части фотонов он не сможет правильно определить, а значит и создать требуемые копии. Для проверки перехвата сообщения отправитель и получатель могут вычислить хеш-образы (контрольные суммы), соответственно, посланного и принятого сообщений. Сравнив хеш-образы, которые можно передавать по открытому каналу не защищая, они могут сделать вывод о прослушивания канала связи или о корректности передачи (целостности) данных.

7.2.2. Шифрования с использованием поляризационной разделительной призмы на принимающей стороне

Для передачи секретной информации передающая и принимающая стороны используют два базиса поляризации: прямолинейный и диагональный. При этом порядок чередования базисов для отдельных фотонов (битов информации), как и в предыдущей схеме, должен быть известен сторонам и случайным для потенциального противника. Этот порядок представляет собой ключ шифрования/дешифрования, для формирования которого можно использовать генераторы гамм или протокол BB84. При этом, если в гамме очередной бит равен «1», то стороны должны использовать прямолинейный базис, иначе – диагональный.

Для отправки фотонов передающая сторона применяет четыре фильтра

Таблица 7.2. Фильтры для отправки фотонов

Базис	Тип фильтра	Значение бита
	горизонтальный 	0
	вертикальный	1

		
диагональный 	слева-направо снизу-вверх 	0
	слева-направо сверху-вниз 	1

Тип фильтра для передачи отдельного фотона выбирается в зависимости от определенного сторонами порядка использования базисов. Аналогичным образом поступает и принимающая сторона – применяет базис поляризации в зависимости от ключа.

Таблица 7.3. Пример отправки и приема сообщения

Посылаемое сообщение, бит	0	0	1	1	0	1	0	1
Базисы, применяемые получателем (ключ)								
Фильтры, выбираемые отправителем								
Принятое сообщение, бит	0	0	1	1	0	1	0	1

Противник, перехватив фотон, не может со стопроцентной уверенностью определить его поляризацию: действительно он угадал применяемый базис ($\approx$ идентифицировал отправленный бит) или это был базис, расположенный под углом 45° к применяемому? В последнем случае вероятность правильной идентификации бита равна 50%.

Это обстоятельство позволяет также определить факт прослушивания канала связи. При перехвате фотона противник вынужден создать его копию (клон) и послать ее законному получателю. Определив значение бита для перехваченного фотона, у него будет два равновероятных варианта поляризации для копии, соответствующие двум разным базисам. Для проверки перехвата сообщения передающая и принимающая стороны могут вычислить хеш-образы (контрольные суммы), соответственно, посланного и принятого сообщений и сравнить их.

Вопросы для самопроверки

1. Дайте определение понятиям «квант» и «фотон».
2. В чем заключается природа корпускулярно-волнового дуализма фотона?
3. В чем суть шифрования с помощью фотонов?

8. КОМБИНИРОВАННЫЕ ШИФРЫ

8.1. Шифры ADFGX и ADFGVX

Комбинированные (составные) шифры предполагают использование для шифрования сообщения сразу нескольких методов (например, сначала замена символов, а затем их перестановка).

Два самых известных полевых шифра в истории криптографии - ADFGX и ADFGVX. Шифр ADFGX впервые был использован во время решающих этапов Первой мировой войны, когда в марте 1918 г. кайзеровские генералы начали крупное наступление. Шифр ADFG(V)X был разработан полковником Фрицем Небелем, офицером связи, служившим в штабе германской армии [43]. Оба шифра предполагают вначале применение к буквам исходного сообщения замену, после чего для получения окончательной шифрограммы выполняется перестановка.

Таблица шифрозамен ADFGX представляет собой матрицу 5 x 5, а для ADFGVX – 6 x 6. Строки и столбцы обозначаются буквами, входящими в название шифра. Пример таблицы шифрозамен для шифра ADFGVX применительно к русскому алфавиту показан на следующем рисунке.

	A	D	F	G	V	X
A	Ю	У	И	Ч	К	Б
D	В	Г	Е	Ф	Ж	З
F	Й	А	Л	М	О	П
G	Р	Щ	Т	Я	Ё	Х
V	Ц	Н	Ш	С	Ъ	Ы
X	Ь	Э	Д	-	-	-

Рис.8.1. Пример таблицы шифрозамен для шифра ADFGVX

Шифрозамена для буквы исходного текста состоит из букв, обозначающих строку и столбец, на пересечении которых она находится (см. шифр «Полибианский квадрат»). Например, для сообщения «АБРАМОВ» набор шифрозамен будет «FD AX GA FD FG FV DA».

На втором этапе для выполнения перестановки полученный набор шифрозамен вписывается построчно сверху-вниз в таблицу, количество столбцов в которой строго определено (ADFGX) или соответствует количеству букв в ключевом слове (ADFGVX). Нумерация столбцов либо оговаривается сторонами (ADFGX) либо соответствует положению букв ключевого слова в алфавите, как в шифре вертикальной перестановки (ADFGVX). Например, для полученного выше набора шифрозамен перестановочная таблица с ключевым словом «ДЯДИНА» показана на следующем рисунке.

Д	Я	Д	И	Н	А
2	6	3	4	5	1
F	D	A	X	G	A
F	D	F	G	F	V
D	A				

Рис.8.2. Перестановочная таблица шифра ADFGVX с ключевым словом «ДЯДИНА»

На третьем этапе буквы выписываются из столбцов в соответствии с их нумерацией, при этом считывание происходит по столбцам, а буквы объединяются в пятибуквенные группы. Таким образом, окончательная шифрограмма для рассматриваемого примера будет выглядеть «AVFFD AFXGG FDDA».

8.2. Основы блочного комбинированного шифрования

Среди комбинированных методов шифрования наиболее распространенными являются методы блочного шифрования. **Блочное шифрование** предполагает разбиение исходного открытого текста на равные блоки, к которым применяется однотипная процедура шифрования. В настоящее время блочные шифры широко используются на практике. Российский и бывший американский стандарты шифрования (DES) относятся именно к этому классу шифров. В основе шифров лежат так называемые «**сети Фейстеля**» [17]. В 1971 г. Хорст Фейстель (Horst Feistel) запатентовал два устройства с различными алгоритмами шифрования, названные затем общим именем

«Люцифер» (Lucifer). Одно из устройств использовало конструкцию, впоследствии названную «сетью Фейстеля» («Feistel cipher», «Feistel network»). Работа над созданием новых криптосистем велась им в стенах IBM вместе с Доном Копперсмитом (Don Coppersmith). Проект «Люцифер» был скорее экспериментальным, но стал базисом для алгоритма Data Encryption Standard (DES). В 1977 г. DES стал стандартом в США на шифрование данных вплоть до 2001 г. и до последнего времени широко использовался в криптографических системах.

Сеть Фейстеля состоит из нескольких **ячеек**.

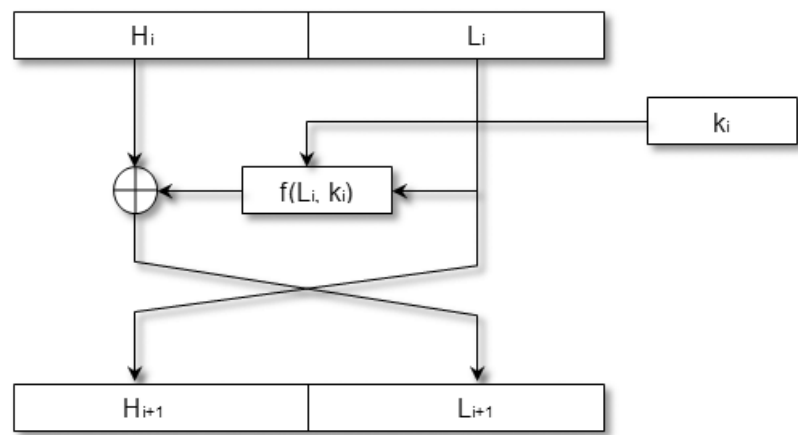


Рис.8.3. Ячейка Фейстеля

На определенном раунде шифрования шифруемый блок разбивается на две равные половинки - H_i (высший, high) и L_i (низкий, low). К правой половинке применяется функция шифрования f с использованием ключевого элемента k_i (части ключа или модификации части ключа). После этого выполняется сложение по модулю два левой половинки и результата модификации правой половинки. В результате шифруемым блоком для следующего раунда будет объединение половинок, полученных по формулам

$$H_{i+1} = L_i, \quad (8.1)$$

$$L_{i+1} = H_i \oplus f(L_i, k_i). \quad (8.2)$$

В общем виде, центральная часть блочных шифров, основанных на сетях Фейстеля, выглядит следующим образом.

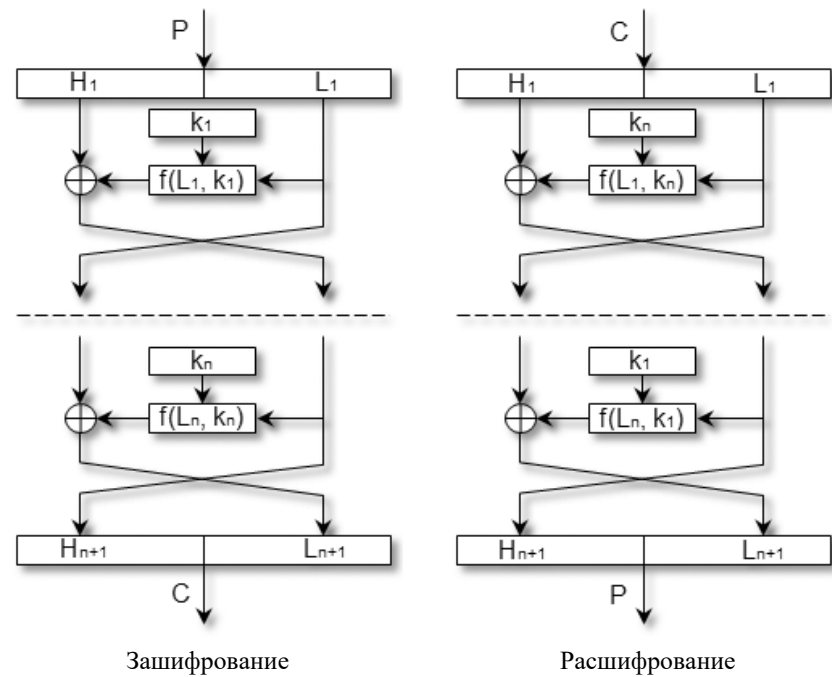


Рис.8.4. Сеть Фейстеля

Как видно, процедуры зашифрования и расшифрования полностью идентичны, за исключением порядка использования ключевых элементов k_i . При этом функция шифрования f может быть сколь угодно сложной и не обязательно обратимой. Обратимость гарантирует сама конструкция сети.

Шифрование при помощи данной конструкции легко реализуется как на программном уровне, так и на аппаратном, что обеспечивает широкие возможности применения. На основе сетей Фейстеля разработано большое количество шифров, среди которых: DES, ГОСТ 28147-89, Blowfish, CAST, FEAL, IDEA, Khufu, Twofish и многие другие.

8.3. DES

DES (Data Encryption Standard, стандарт шифрования данных) - федеральный стандарт шифрования США в 1977-2001 гг. **для использования во всех несекретных правительственных каналах связи** (FIPS PUB 46 «Data Encryption Standard») [8, 16]. Несмотря на то, что в настоящий момент федеральным стандартом шифрования США является Rijndael (AES), рассмотрение DES позволяет понять основные принципы блочного шифрования.

В алгоритме, лежащем в основе DES, используются методы замены, перестановки и гаммирования (сложение по модулю 2).

Открытое сообщение разбивается на блоки длиной 64 бита. Если длина сообщения не кратна 64, оно дополняется справа недостающим количеством битов.

Данные шифруются ключом длиной 56 битов. На самом деле ключ имеет размер 64 бита, однако реально для выработки ключевых элементов используются только 56 из них. Самые младшие биты каждого байта ключа (8-ой, 16-ый, ..., 64-ый) не попадают в ключевые элементы и служат исключительно для контроля четности. Требуется, чтобы сумма битов каждого байта ключа, включая контрольный, была четной (четный паритетный бит).

Для решения разнообразных криптографических задач, разработаны **четыре рабочих режима**, реализующих DES:

- электронная кодовая книга ECB (Electronic Code Book);
- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

Режим ECB (электронная кодовая книга - Electronic Code Book).

Открытое сообщение разбивают на 64-битовые блоки. Каждый из них шифруют независимо с использованием одного и того же ключа шифрования.

Общая схема шифрования блока изображена на рис.8.5 [24].

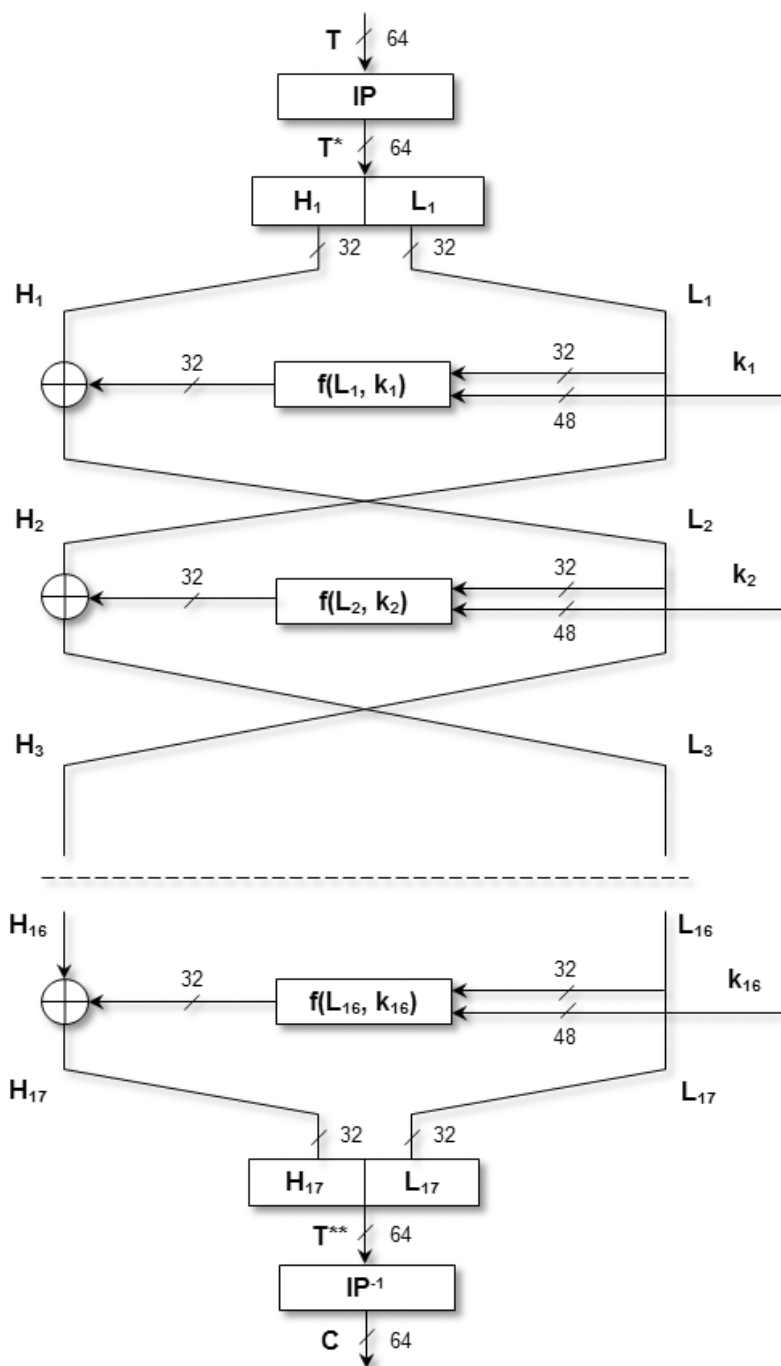


Рис.8.5. Схема шифрования блока

1. Шифрование 64-битового блока данных T начинается с начальной перестановки битов IP .

Таблица 8.1. Начальная перестановка IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

В таблице указывается новое положение соответствующего бита. Таким образом, при выполнении начальной перестановки 58-ый бит станет 1-ым, 50-ый – 2-ым, 42-ой – 3-им и т.д.

2. Результат перестановки T^* разделяется на две 32-битовые части H_1 и L_1 , с которыми выполняются 16 раундов преобразования.

3. В каждом раунде i старшая половина H_i блока модифицируется путем побитового прибавления к ней по модулю 2 ($\oplus$) результата вычисления функции шифрования f , зависящей от младшей половины блока L_i и 48-битового ключевого элемента k_i . Ключевой элемент k_i вырабатывается из ключа шифрования. Между раундами старшая и младшая половины блока меняются местами. В последнем раунде происходит то же самое, за исключением обмена значениями половинок блока.

4. Полублоки H_{17} и L_{17} объединяются в полный блок T^{**} , в котором выполняется конечная битовая перестановка IP^{-1} , обратная начальной.

Таблица 8.2. Конечная перестановка IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Результат последней операции и является выходным значением цикла шифрования – зашифрованным блоком C .

Все перестановки в таблицах IP и IP^{-1} подобраны разработчиками таким образом, чтобы максимально затруднить процесс расшифровки путём подбора ключа.

Схема функции шифрования f приведена на рис.8.6.

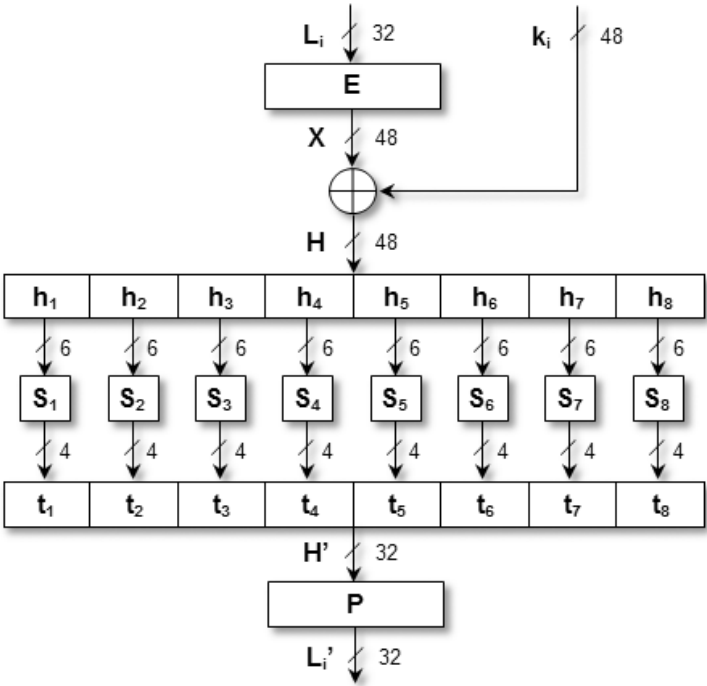


Рис.8.6. Схема функции шифрования

1. На вход поступает 32-битовая половина шифруемого блока L_i и 48-битовый ключевой элемент k_i .
2. L_i разбивается на 8 тетрад по 4 бита. Каждая тетрада по циклическому закону дополняется крайними битами из соседних тетрад до 6-битного слова (функция расширения E). Цикличность означает, что первый бит L_i добавляется последним в последнее слово, а последний бит L_i добавляется первым в первое слово. Далее выполняется объединение тетрад в 48-битный блок X . Например, $L_i = 011101101...01101_2$, тогда $X = 101110101101...011010_2$.
3. X побитово суммируется по модулю 2 ($\oplus$) с ключевым элементом k_i .
4. 48-битовый блок данных H разделяется на восемь 6-битовых элементов, обозначенных $h_1, h_2, ..., h_8$.
5. Каждое из значений h_j преобразуется в новое 4-битовое значение t_j с помощью соответствующего узла замены S_j .

Таблица 8.3. Значения t_j

Узел замены	Номер строки	Номер столбца															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Если на вход S_j поступает блок $h_j = b_1b_2b_3b_4b_5b_6$, то двухбитовое число b_1b_6 указывает номер строки матрицы, а четырёхбитовое число $b_2b_3b_4b_5$ - номер столбца в таблице узлов замен. В результате применения узла замены S_j к блоку h_j получается число (от 0 до 15), которое преобразуется в t_j . Например, в узел замены S_3 поступает $h_3 = 101011_2$. Тогда, номер строки равен 3_{10} ($b_1b_6 = 11_2$), номер столбца – 5_{10} ($b_2b_3b_4b_5 = 0101_2$), $t_3 = 9_{10}$ (1001_2).

6. Полученные восемь элементов t_j вновь объединяются в 32-битовый блок H' .

7. В H' выполняется перестановка битов P .

Таблица 8.4. Перестановка P

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9

19	13	30	6	22	11	4	25
----	----	----	---	----	----	---	----

Результат последней операции и является выходным значением функции шифрования L_i .

Ключевые элементы вырабатываются из ключа с использованием сдвигов и битовых выборок-перестановок. Таким образом, ключевые элементы состоят исключительно из битов исходного ключа, «перетасованных» в различном порядке. Схема выработки ключевых элементов показана на следующем рисунке.

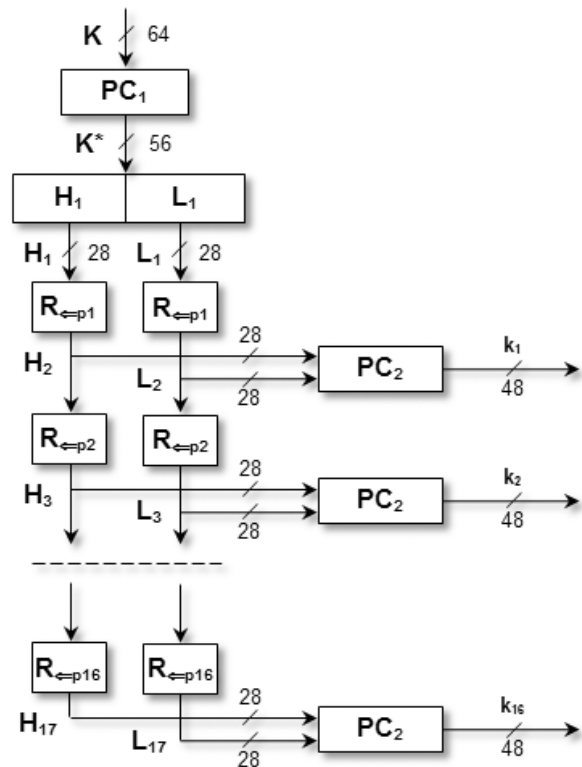


Рис.8.7. Схема выработки ключевых элементов

1. Выработка ключевых элементов из ключа **K** начинается со входной выборки-перестановки битов **PC₁**, которая отбирает 56 из 64 битов ключа и располагает их в другом порядке.

Таблица 8.5. Перестановка **PC₁**

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

- 2. Результат выборки-перестановки **K*** разделяется на две 28-битовые части: старшую **H₁** и младшую **L₁**.
- 3. 16 раз выполняется процедура.
- 3а. В зависимости от номера итерации обе части циклически сдвигаются на 1 или 2 бита влево.

Таблица 8.6. Циклический сдвиг

Номер итерации	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Сдвиг (бит)	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

3б. После сдвига части объединяются и из них с помощью выборки-перестановки **PC₂** отбираются 48 битов, которые и формируют очередной ключевой элемент.

Таблица 8.7. Перестановка **PC₂**

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Алгоритмы шифрования и расшифрования DES-ECB в общем виде выражаются следующими схемами

$$C = \text{DES}(T) = \text{IP}(T) \rightarrow H_1 \oplus f(L_1, k_1), L_1 \rightarrow \dots \rightarrow H_{16} \oplus f(L_{16}, k_{16}), L_{16} \rightarrow \text{IP}^{-1}(2^{32} * L_{17} + H_{17}), \quad (8.3)$$

$$T = \text{DES}^{-1}(C) = \text{IP}(C) \rightarrow H_1 \oplus f(L_1, k_{16}), L_1 \rightarrow \dots \rightarrow H_{16} \oplus f(L_{16}, k_1), L_{16} \rightarrow \text{IP}^{-1}(2^{32} * L_{17} + H_{17}). \quad (8.4)$$

Как видно схема алгоритма остается неизменной, меняется лишь порядок использования ключевых элементов. Таким образом, для расшифрования необходимо «прогнать» DES с тем же ключом, но использовать ключевые элементы в обратном порядке.

Использование различных методов шифрования:

- замена - функция расширения E , узлы замены S ;
- перестановка – перестановки IP , IP^{-1} , P , PC_1 , PC_2 , чередование L_i и H_i , циклический сдвиг;
- гаммирование – $\oplus$.

Из-за небольшого числа возможных ключей (всего 256), появляется возможность их полного перебора на быстродействующей вычислительной технике за реальное время. В 1998 г. Electronic Frontier Foundation используя специальный компьютер DES-Cracker, удалось взломать DES за 3 дня. По неподтвержденным данным, Агентство национальной безопасности США уже в 1996 г. могло вскрывать ключ DES за 3-15 мин. с помощью устройства стоимостью 50000 долларов.

Режим CBC (сцепление блоков шифра - Cipher Block Chaining).

Схемы алгоритмов представлены на следующем рисунке. По каждой из стрелок передается 64 бита информации.

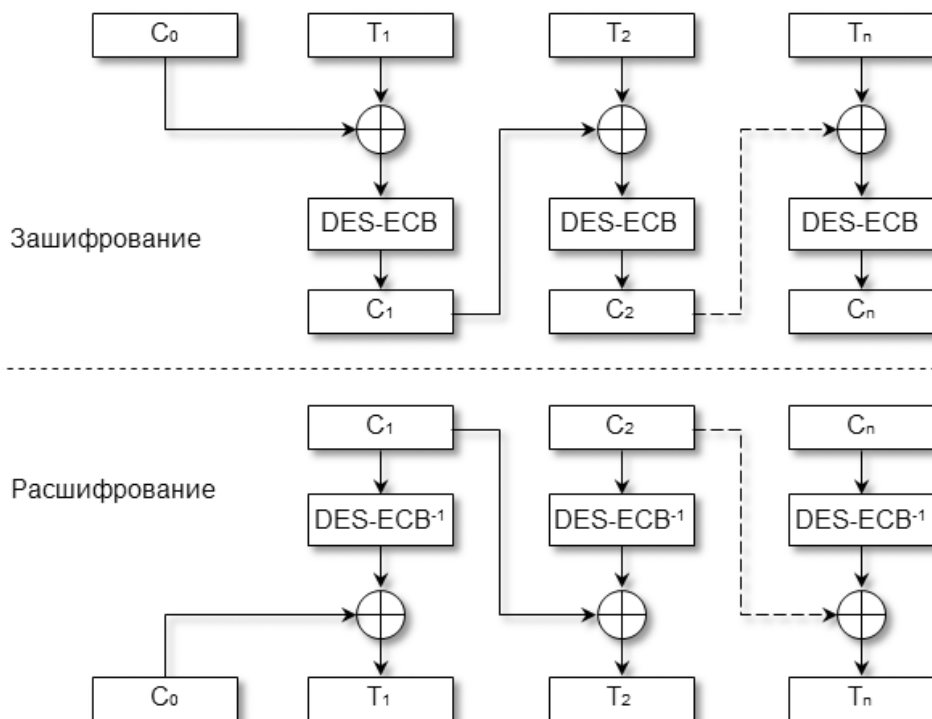


Рис.8.8. Схемы алгоритмов DES в режиме сцепления блоков шифра (CBC)

1. Исходное сообщение разбивается на 64-битовые блоки: $T_1, T_2, \dots, T_n$.
2. Первый блок T_1 складывается по модулю 2 с 64-битовым начальным вектором C_0 , который меняется и держится в секрете (C_0 -

синхропосылка, по сути, второй ключ).

3. Полученная сумма затем шифруется с использованием ключа DES.

4. 64-битовый шифр C_1 складывается по модулю 2 со вторым блоком текста, результат шифруется и получается второй 64-битовый шифр C_2 , и т.д.

5. Процедура повторяется до тех пор, пока не будут обработаны все блоки текста. Т.о., для всех $i = 1 \dots n$ (n - число блоков) результат шифрования C_i определяется следующим образом: $C_i = \text{DES}(T_i \oplus C_{i-1})$.

Очевидно, что последний 64-битовый блок шифртекста является функцией секретного ключа, начального вектора и каждого бита открытого текста независимо от его длины. Этот блок шифртекста называют **кодом аутентификации сообщения (КАС)**. Код КАС может быть легко проверен получателем, владеющим секретным ключом и начальным вектором, путем повторения процедуры, выполненной отправителем. Достоинство данного режима в том, что он не позволяет накапливаться ошибкам при передаче. Блок T_i является функцией только C_{i-1} и C_i . Поэтому ошибка при передаче приведет к потере только двух блоков исходного текста.

Режимы CFB и OFB (обратная связь по шифртексту - Cipher Feed Back; обратная связь по выходу - Output Feed Back).

В алгоритмах CFB и OFB используется такой же подход, что и в алгоритме CBC, когда результат шифрования (расшифрования) блока на предыдущем шаге используется для шифровки (расшифровки) очередного блока. В этих режимах размер входного блока может быть меньше 64 бит.

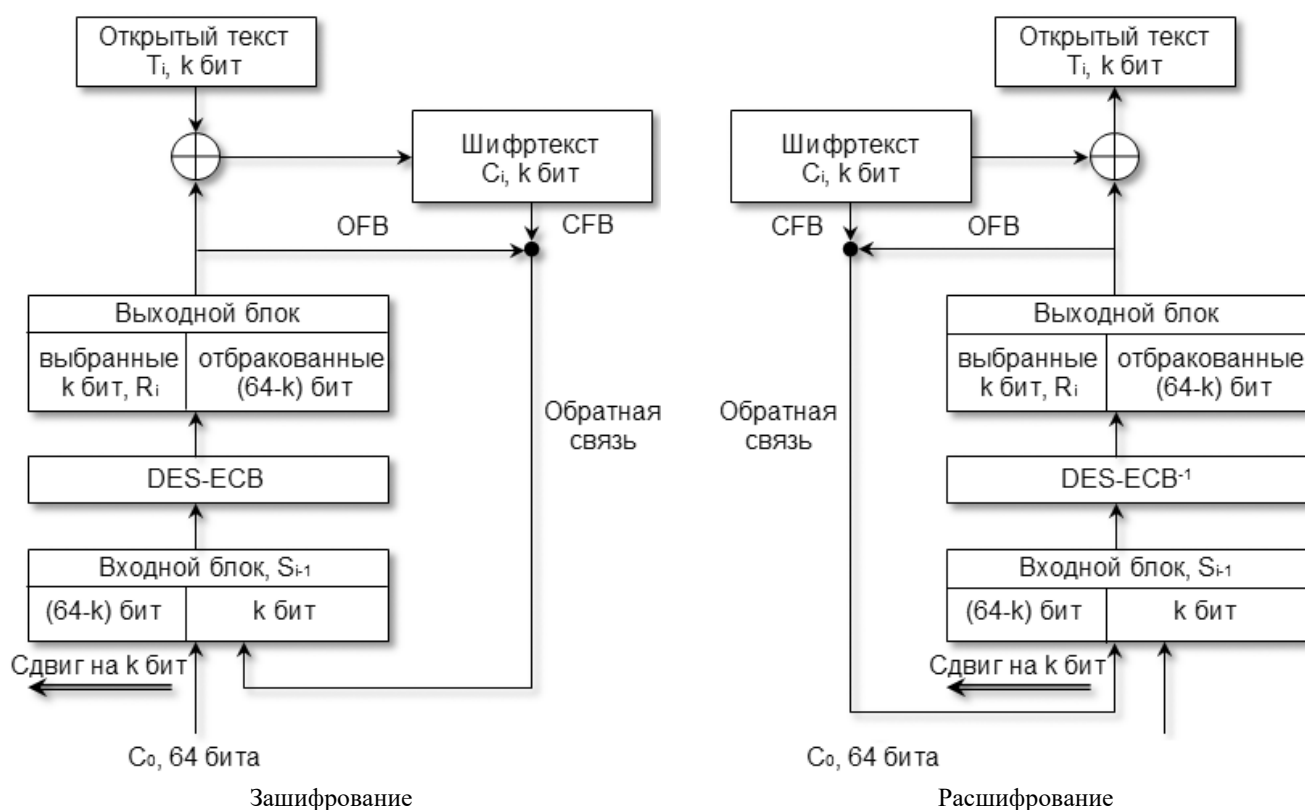


Рис.8.9. Схемы алгоритмов DES в режимах CFB и OFB

Алгоритм шифрования.

1. Исходное сообщение разбивается на блоки, длиной k бит: $T_1, T_2, \dots, T_n$.

2. Синхропосылка шифруется с использованием ключа DES.

3. Из полученного результата выбираются старшие k бит, которые складываются с блоком открытого текста T_i по модулю 2 для получения шифртекста C_i .

4. Процедура повторяется до тех пор, пока не будут обработаны все блоки текста. При этом, содержимое входного блока сдвигается на k бит влево (причем сдвиг не циклический) и младшие k бит заполняются либо шифртекстом (CFB), либо старшими k бит выходного блока (OFB).

Алгоритм расшифрования аналогичен алгоритму шифрования и отличается только входом и выходом стрелок в блок сложения по модулю 2.

Тройной DES.

При тройном DES текст шифруется 3 раза DES. Таким образом, длина ключа возрастает до 168-бит (56×3). Однако, применение тройного DES не всегда означает увеличение уровня безопасности сообщения.

Типы тройного шифрования DES:

- DES-EEE3: Шифруется 3 раза с 3 различными ключами.
- DES-EDE3: 3 DES операции шифровка-расшифровка-шифровка с 3 различными ключами.
- DES-EEE2 и DES-EDE2: Как и предыдущие, за исключением того, что первая и третья операции используют одинаковый ключ.

Сферы применения разных режимов DES.

Электронная кодовая книга ECB рекомендуется использовать для шифрования сообщений длиной в один блок (как правило, ключей). Недостаток ECB, в сравнении с другими режимами шифрования - сохранение статистических особенностей открытого текста [17].

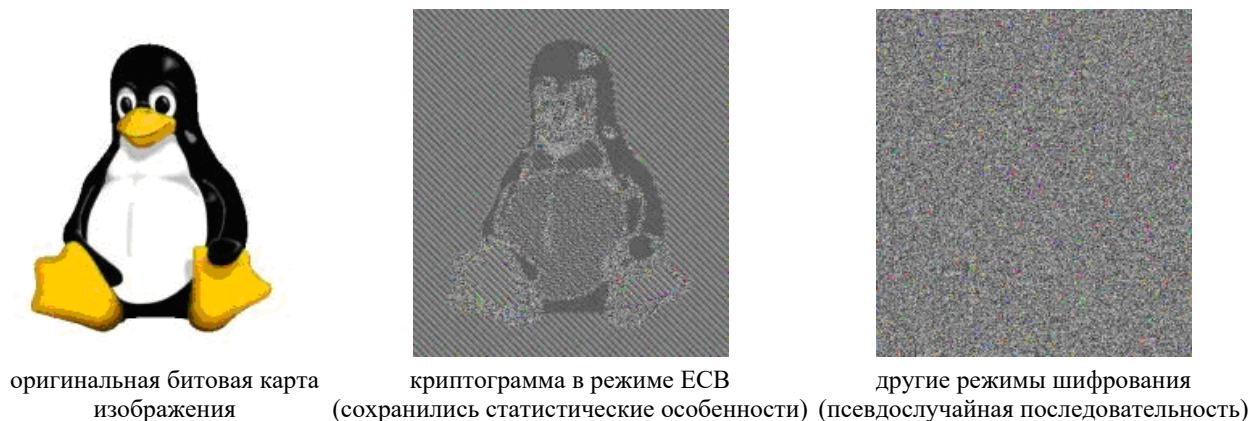


Рис.8.10. Сохранение статистических особенностей открытого текста

Сцепление блоков шифра CBC и тройной DES могут использоваться для шифрование больших объемов данных (в частности тройной DES используется для эмиссии и обработки кредитных карт VISA, EuroPay и других платежных систем).

Обратная связь по шифртексту CFB и обратная связь по выходу OFB рекомендуется для шифрования отдельных символов или небольших сообщений.

8.4. ГОСТ 28147-89

ГОСТ 28147-89 - бывший советский и российский стандарт симметричного шифрования, введенный в 1990 г. («ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»). С момента опубликования ГОСТа на нём стоял ограничительный гриф «Для служебного пользования», и формально шифр был объявлен «полностью открытым» только в мае 1994 г. [17].

В алгоритме, лежащем в основе ГОСТ, используются методы замены, перестановки и гаммирования (сложение по модулю 2 и 2^{32}).

Открытое сообщение разбивается на блоки длиной 64 бита. Если длина сообщения не кратна 64, оно дополняется справа недостающим количеством битов.

Длина ключа – 256 битов.

Рабочие режимы:

- простой замены;
- гаммирования;
- гаммирования с обратной связью;
- имитовставки.

Режим простой замены.

Открытое сообщение разбивают на 64-битовые блоки. Каждый из них шифруют независимо с использованием одного и того же

ключа шифрования. Перед шифрованием 256-битный ключ разбивается на восемь 32-битных ключевых элементов (блоков) $k_1, k_2, \dots, k_8$.

Общая схема шифрования блока изображена на следующем рисунке.

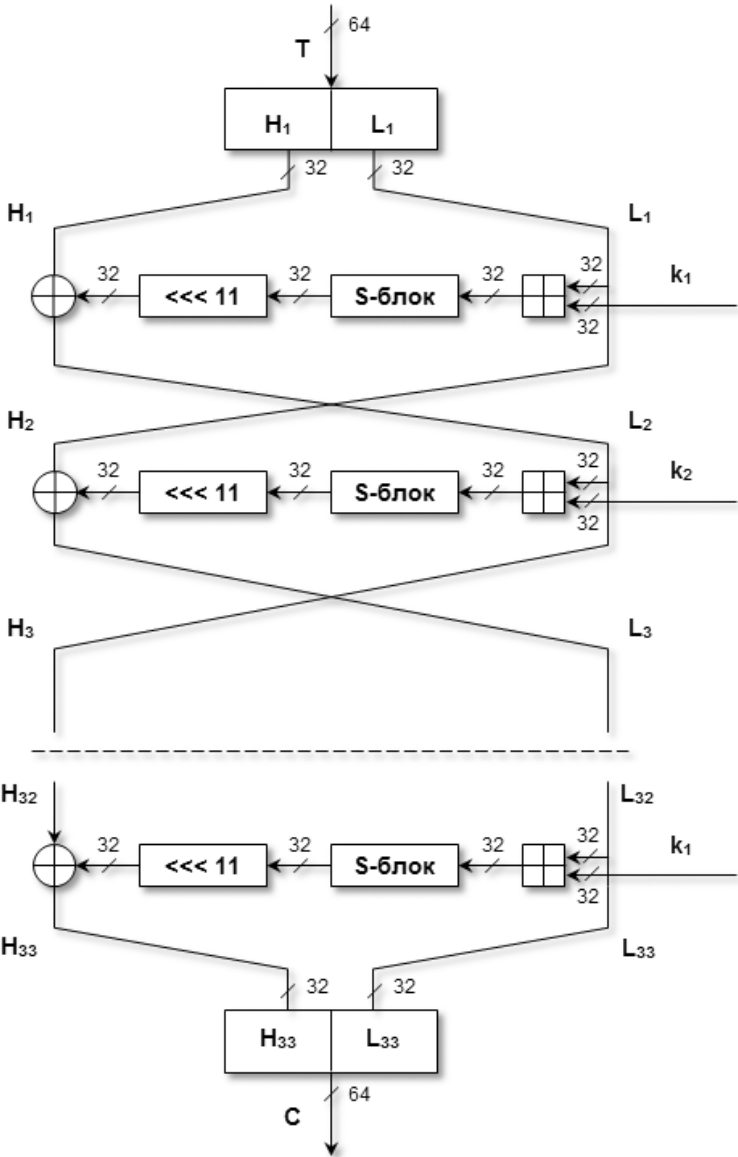


Рис.8.11. Схема шифрования блока

1. Шифрование 64-битового блока данных T начинается с его разбиения на две 32-битовые части H_1 и L_1 , с которыми выполняются 32 раунда преобразования.

2. В каждом раунде i :

2.1. Младшая половина L_i складывается с ключевым элементом k_i по модулю 2^{32} ($\boxplus$).

$$X_i = (L_i + k_i) \bmod 2^{32}. \tag{8.5}$$

Порядок использования ключевых элементов указан в следующей таблице.

Таблица 8.8. Порядок использования ключевых элементов

Раунд	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Ключевой элемент	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Раунд	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Ключевой элемент	1	2	3	4	5	6	7	8	8	7	6	5	4	3	2	1

2.2. Результат сложения X_i разбивается на восемь 4-битных фрагментов x_{ij} ($j = 1..8$), каждый из которых поступает на вход своего S -блока (узла замены) и заменяется на другой 4-битовый фрагмент y_{ij} ($j = 1..8$). В самом ГОСТ S -блоки не приведены. Указывается

только, что они должны быть откуда-то взяты. В ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования» в приложении А приведены «проверочные» S-блоки, которые использовал ЦБ РФ в своих приложениях.

Таблица 8.9. Значения y_{ij}

S-блок (S_j)	Значение x_{ij}															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3
S_2	14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9
S_3	5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11
S_4	7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3
S_5	6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2
S_6	4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
S_7	13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
S_8	1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

- Так, если третий фрагмент $x_{i3} = 6_{10} (0110_2)$, то он заменяется на $y_{i3} = 4_{10} (0100_2)$.
- 2.3. Замененные фрагменты y_{ij} объединяются обратно в 32-битовый блок Y_i . После чего выполняется циклический сдвиг влево на 11 бит – $Z_i = Y_i \lll 11$.
- 2.4. Старшая половина H_i блока модифицируется путем побитового прибавления к ней по модулю 2 ($\oplus$) результата сдвига Z_i .
- 2.5. Между раундами старшая и младшая половины блока меняются местами.
3. Полублоки H_{33} и L_{33} объединяются в зашифрованный блок C .

Расшифрование отличается зашифрования обратным порядком использования ключевых элементов, представленного в табл.8.8.

Использование различных методов шифрования:

- замена - узлы замены (S-блоки);
- перестановка – чередование H_i и L_i , циклический сдвиг на 11 бит;
- гаммирование – по модулю 2^{32} ($\boxplus$) и 2 ($\oplus$).

Основные различия между DES и ГОСТ [8]:

- DES использует сложную процедуру для генерации подключей из ключей. В ГОСТ эта процедура очень проста;
- в DES 56-битовый ключ, а в ГОСТ - 256-битовый;
- у S-блоков DES 6-битовые входы и 4-битовые выходы, а у S-блоков ГОСТ 4-битовые входы и выходы. В обоих алгоритмах используется по восемь S-блоков;
- в DES используются перестановка, названная P-блоком, а в ГОСТ используется 11-битовый циклический сдвиг влево;
- в DES 16 этапов, а в ГОСТ - 32.

По мнению одного из авторитетных специалистов в области криптографии Брюса Шнайера увеличенная длина ключа и использование в вдвое больше раундов шифрования делает ГОСТ

... более устойчивым к дифференциальному и линейному криптоанализу, чем DES. ... Разработчики ГОСТ пытались достигнуть равновесия между безопасностью и эффективностью. Они изменили идеологию DES так, чтобы создать алгоритм, который больше подходит для программной реализации. Они, по видимому, менее уверены в безопасности своего алгоритма и попытались скомпенсировать это очень большой длиной ключа, сохранением в секрете S-блоков и удвоением количества итераций. Вопрос, увенчались ли их усилия созданием более безопасного, чем DES, алгоритма, остается открытым.

Брюс Шнайер. «Прикладная криптография»

AES (Advanced Encryption Standard, расширенный стандарт шифрования) - американский стандарт симметричного блочного шифрования, введенный в действие с 26 мая 2002 г. (FIPS PUB 197 «Announcing the ADVANCED ENCRYPTION STANDARD (AES)»). Является упрощенной версией алгоритма Rijndael (авторы Винсент Рэймен и Йоан Даймен), поддерживающего более широкий набор длин блоков (от 128 до 256 битов с шагом в 32 бита).

По типу относится к подстановочно-перестановочным сетям (англ. Substitution-Permutation network, SP-сеть). В алгоритме используются методы замены, перестановки и гаммирования (сложение по модулю 2).

Основные параметры AES приведены в следующей таблицы.

Таблица 8.10. Основные параметры AES

Тип шифра	Длина ключа N_k , битов (слов ¹)	Размер блока зашифрования / расшифрования N_b , битов (слов)	Количество раундов N_r	Количество ключевых элементов ² $N_w = N_b (N_r + 1)$
AES-128	128 (4)	128 (4)	10	44
AES-192	192 (6)		12	52
AES-256	256 (8)		14	60

Примечания.

¹Слово (англ. word) – последовательность из 4 байтов (32 битов).

²Ключевой элемент – 4-байтовое слово, формируемое из ключа.

Схемы зашифрования и расшифрования одного блока изображены на следующем рисунке.

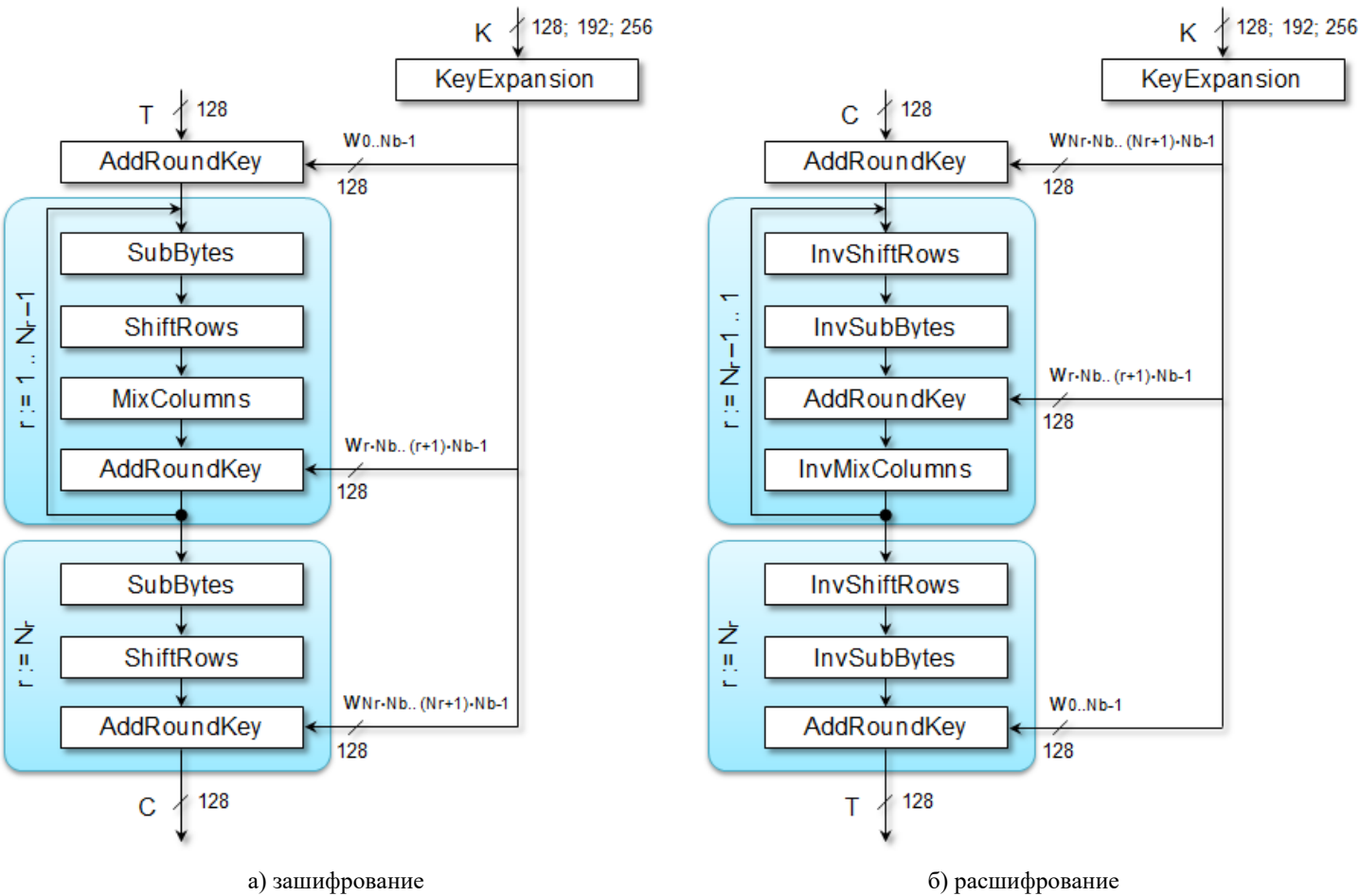


Рис.8.12

А. Формирование ключевых элементов – KeyExpansion.

Перед процедурой зашифрования или расшифрования из ключа **К** формируются набор ключевых элементов w_i . На следующем рисунке отображена схема формирования ключевых элементов при длине ключа $N_k = 128$ битов. При большей длине ключа (192 и 256 битов) имеются особенности получения w_i (см. спецификацию [57]).

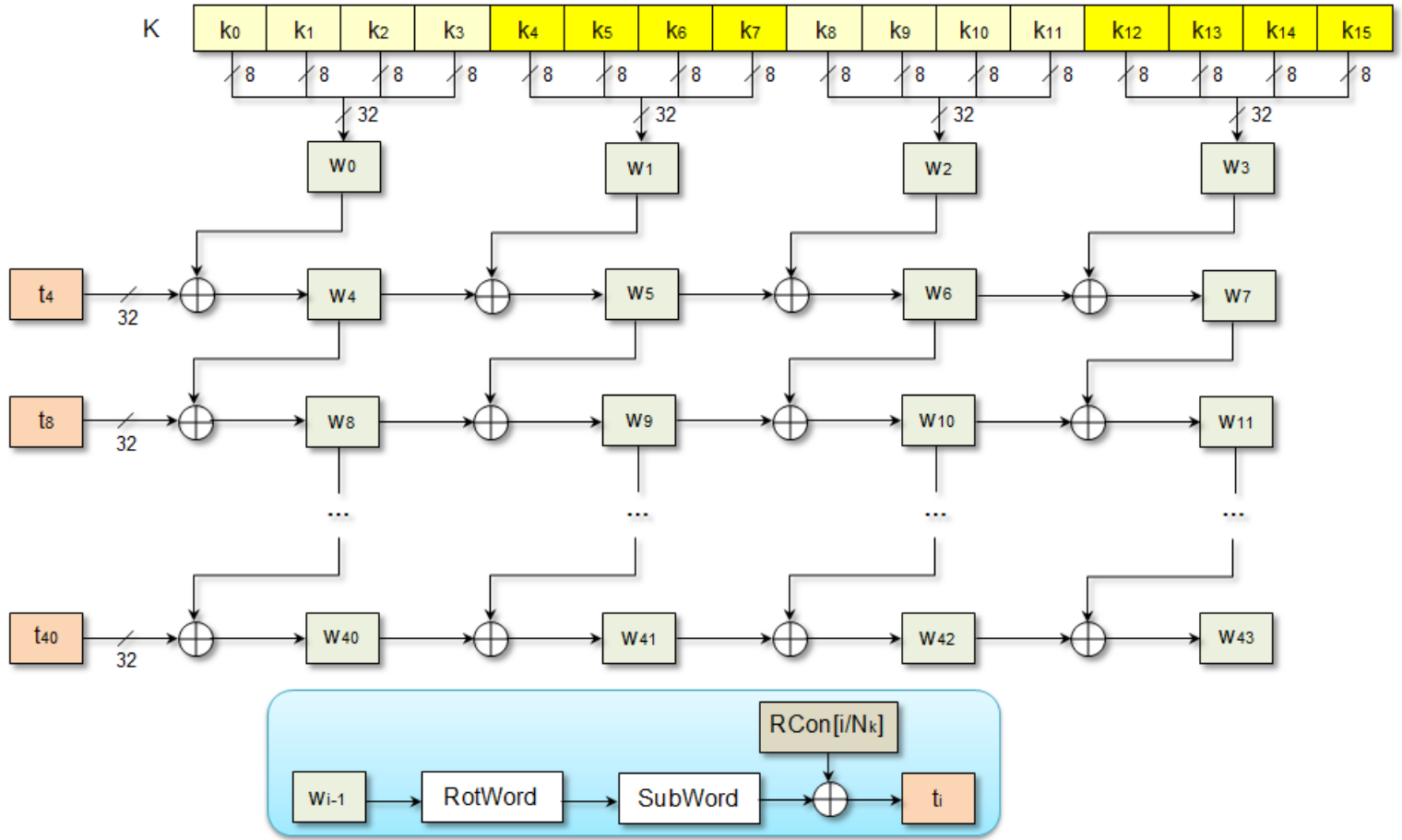
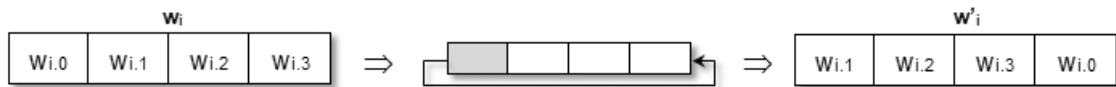


Рис.8.13. Схема формирования ключевых элементов (AES-128)

А.1. RotWord.

Циклический сдвиг в слове w_i на один байт влево.



А.2. SubWord.

Замена каждого байта слова w_i на байт **S-box** в соответствии со следующей таблицей.

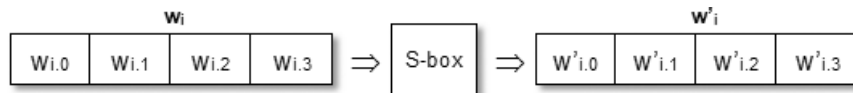


Таблица 8.11. S-box
(16-теричное представление)

	_0	_1	_2	_3	_4	_5	_6	_7	_8	_9	_A	_B	_C	_D	_E	_F
0_	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1_	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2_	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3_	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4_	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84

5_	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6_	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7_	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8_	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9_	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A_	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B_	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C_	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D_	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E_	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F_	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

При этом байт в 16-теричном представлении состоит из двух символов, первый из которых указывает на номер строки **S-box**, а второй – на номер столбца. Например, если один из байтов $w_i = C5_{16}$, то он заменяется на $w'_i = A6_{16}$.

Иначе, таблицу **S-box** можно представить в виде одномерного массива. Тогда w_i – это индекс элемента массива, который служит заменой – $w'_i = \text{S-box}[w_i]$.

A.3. RCon.

4-байтовая константа.

Rcon			
$2^{i/Nk-1}$	0	0	0

B. Зашифрование.

Изначально шифруемый блок **T** представляется массивом байтов **state** размером 4x4. При этом согласно спецификации AES [57] байты выписываются в массив по столбцам.

T = state ₀ =			
S0.0	S0.1	S0.2	S0.3
S1.0	S1.1	S1.2	S1.3
S2.0	S2.1	S2.2	S2.3
S3.0	S3.1	S3.2	S3.3

Далее над массивом **state** выполняются последовательные преобразования.

B.1. AddRoundKey.

Сложение **state** по модулю 2 с четырьмя 4-байтовыми ключевыми элементами.

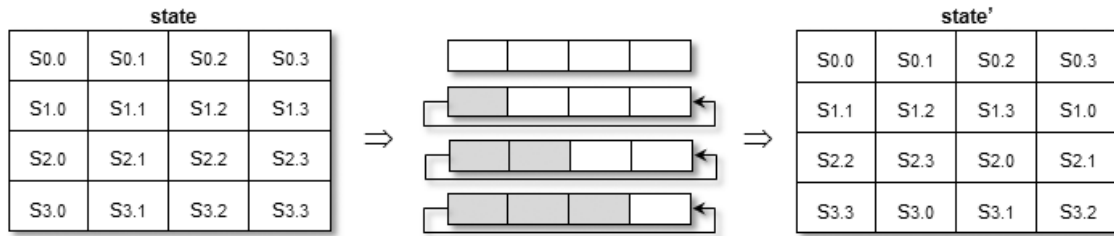
state					$j = r \cdot Nb$					state'			
S0.0	S0.1	S0.2	S0.3	$\oplus$	Wj.0	Wj.1	Wj.2	Wj.3	=	S'0.0	S'0.1	S'0.2	S'0.3
S1.0	S1.1	S1.2	S1.3		Wj+1.0	Wj+1.1	Wj+1.2	Wj+1.3		S'1.0	S'1.1	S'1.2	S'1.3
S2.0	S2.1	S2.2	S2.3		Wj+2.0	Wj+2.1	Wj+2.2	Wj+2.3		S'2.0	S'2.1	S'2.2	S'2.3
S3.0	S3.1	S3.2	S3.3		Wj+3.0	Wj+3.1	Wj+3.2	Wj+3.3		S'3.0	S'3.1	S'3.2	S'3.3

B.2. SubBytes.

Замена байтов **state** по аналогии с **SubWord** в соответствии с табл.8.11.

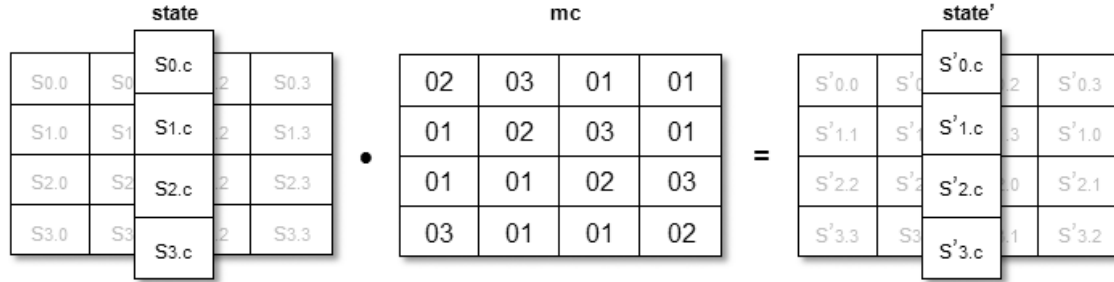
B.3. ShiftRows.

Построчный циклический сдвиг байтов **state** влево на 0, 1, 2 и 3 байта.



B.4. MixColumns.

Смешивание байтов в столбцах **state**. Достигается за счет умножения вектора-столбца **state** на квадратную матрицу **mc**. Умножение выполняется в поле Галуа $GF(2^8)$ по модулю $x^8 + x^4 + x^3 + x + 1$ – обозначается жирной точкой ($\bullet$).



В результате выполняется замена байтов по формулам:

$$s'_{0,c} = (02 \bullet s_{0,c}) \oplus (03 \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus (02 \bullet s_{1,c}) \oplus (03 \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (02 \bullet s_{2,c}) \oplus (03 \bullet s_{3,c})$$

$$s'_{3,c} = (03 \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (02 \bullet s_{3,c})$$

Операция $s \bullet mc$ выполняется по правилам полиномиальной арифметики. Для этого элементы вектора и матрицы представляются в двоичном виде. Например, $[s_{0,0}, s_{1,0}, s_{2,0}, s_{3,0}] = [D4, BF, 5D, 30]_{16} = [11010100, 10111111, 1011101, 110000]_2$ и $[mc_{0,0}, mc_{0,1}, mc_{0,2}, mc_{0,3}] = [02, 03, 01, 01]_{16} = [10, 11, 01, 01]_2$.

Дальнейшие преобразования иллюстрируются на примере умножения и деления в столбик. Умножение выполняется классически, но со сложением единиц в столбцах по модулю 2.

$$\begin{array}{r} * \quad \begin{array}{r} 11010100 \\ \underline{10} \\ 00000000 \\ \oplus \quad \underline{11010100} \\ 110101000 \end{array} \quad \begin{array}{r} * \quad \begin{array}{r} 10111111 \\ \underline{11} \\ 10111111 \\ \oplus \quad \underline{10111111} \\ 111000001 \end{array} \end{array}$$

Взятие остатка от произведения по модулю $x^8 + x^4 + x^3 + x + 1 (= 100011011_2)$ в поле Галуа $GF(2^8)$ выполняется делением в столбик до тех пор, пока остаток превышает 8 битов. При этом вместо вычитания делителя из делимого также используется сложение по модулю 2.

$$\begin{array}{r} \oplus \quad \begin{array}{r} 110101000 \\ \underline{100011011} \\ 10110011 \end{array} \quad \oplus \quad \begin{array}{r} 111000001 \\ \underline{100011011} \\ 11011010 \end{array} \end{array}$$

Для $s_{2,0} = 1 \bullet s_{2,0} = 1011101_2$ и $s_{3,0} = 1 \bullet s_{3,0} = 110000_2$ умножение и взятие остатка не требуется, так как их длина не превышает 8 битов. Более сложный пример деления числа $C543_{16} = 1100010101000011_2$ по модулю $x^8 + x^4 + x^3 + x + 1$ в поле Галуа $GF(2^8)$ показан ниже.

$$\begin{array}{r} \oplus \quad \begin{array}{r} 1100010101000011 \\ \underline{100011011} \\ 100100011 \\ \oplus \quad \underline{100011011} \\ 111000000 \\ \oplus \quad \underline{100011011} \\ 110110110 \\ \oplus \quad \underline{100011011} \\ 101011011 \end{array} \end{array}$$

$$\begin{array}{r} 100011011 \\ 10000001 \\ \hline \end{array} = 81_{16}$$

Окончательное значение элемента $s'_{0,0}$ вектора **state'** получается сложением по модулю 2 полученных остатков.

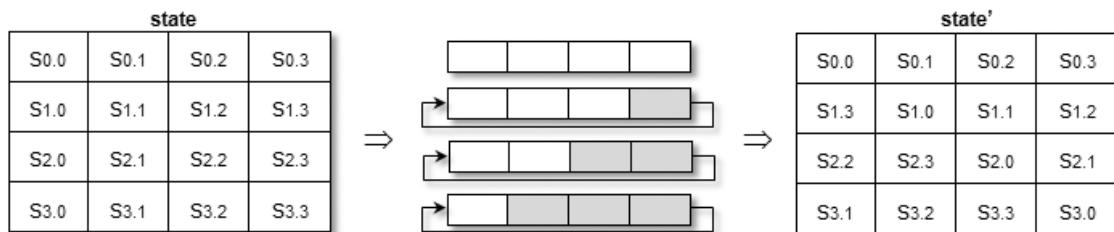
$$\oplus \begin{array}{r} 10110011 \\ 11011010 \\ 1011101 \\ 110000 \\ \hline 00000100 = 04_{16} = s'_{0,0} \end{array}$$

С. Расшифрование.

При расшифровании меняется не только порядок использования ключевых элементов (как в DES и ГОСТ 28147-89), но и выполняется инверсия всех операций.

С.1. InvShiftRows.

Построчный циклический сдвиг байтов **state** вправо на 0, 1, 2 и 3 байта.



С.2. InvSubBytes.

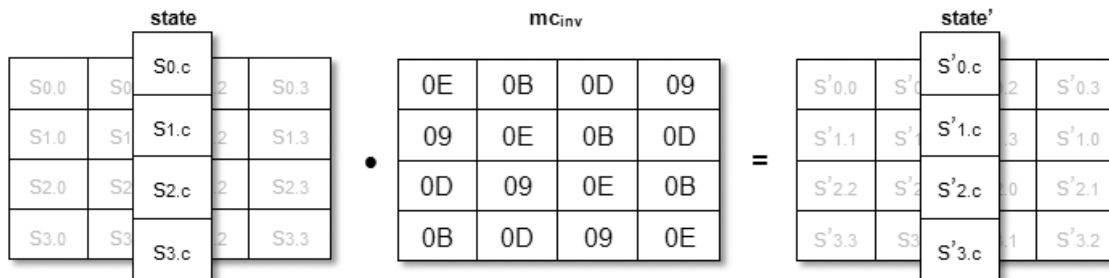
Замена байтов **state** в соответствии со следующей таблицей.

Таблица 8.12. Inverse S-box
(16-теричное представление)

	_0	_1	_2	_3	_4	_5	_6	_7	_8	_9	_A	_B	_C	_D	_E	_F
0_	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1_	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2_	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3_	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4_	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5_	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6_	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7_	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8_	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9_	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A_	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B_	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C_	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D_	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E_	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F_	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

С.3. InvMixColumns.

Смешивание байтов в столбцах – умножение вектора-столбца **state** на квадратную матрицу $\mathbf{mc}_{inv}$ с взятием остатков по модулю $x^8 + x^4 + x^3 + x + 1$ в поле Галуа $GF(2^8)$.



Замена байтов выполняется по формулам:

$$s'_{0,c} = (0E \cdot s_{0,c}) \oplus (0B \cdot s_{1,c}) \oplus (0D \cdot s_{2,c}) \oplus (09 \cdot s_{3,c})$$

$$s'_{1,c} = (09 \cdot s_{0,c}) \oplus (0E \cdot s_{1,c}) \oplus (0B \cdot s_{2,c}) \oplus (0D \cdot s_{3,c})$$

$$s'_{2,c} = (0D \cdot s_{0,c}) \oplus (09 \cdot s_{1,c}) \oplus (0E \cdot s_{2,c}) \oplus (0B \cdot s_{3,c})$$

$$s'_{3,c} = (0B \cdot s_{0,c}) \oplus (0D \cdot s_{1,c}) \oplus (09 \cdot s_{2,c}) \oplus (0E \cdot s_{3,c})$$

В заключение несколько слов о стойкости шифра. В отличие от большинства других шифров, AES имеет простое математическое описание. Это обстоятельство беспокоит многих криптографов. Вот что по этому поводу написали известные популяризаторы криптографии Нильс Фергюсон и Брюс Шнайер.

У нас есть одно критическое замечание к AES: мы не совсем доверяем его безопасности. Что беспокоит нас больше всего в AES, так это его простая алгебраическая структура... Ни один другой блочный шифр не имеет столь простого алгебраического представления. Мы понятия не имеем, ведёт это к атаке или нет, но незнание этого является достаточной причиной, чтобы скептически относиться к использованию AES.

Нильс Фергюсон, Брюс Шнайер. «Практическая криптография»

8.6. ГОСТ 34.12-2015 [58]

ГОСТ 34.12-2015 – российский стандарт симметричного блочного шифрования, введённый в действие 19 июня 2015 г. («ГОСТ 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры»).

Содержит описание двух блочных шифров:

- «**Магма**» («Magma») – с длиной блока $n = 64$ бит;
- «**Кузнечик**» («Kuznyechik») – с длиной блока $n = 128$ бит.

Длина ключа для обоих шифров – $K = 256$ бит.

«**Магма**».

Полностью соответствует ГОСТ 28147-89. В отличие от старого ГОСТ в новом явно определены значения **S-блоков** (подстановок π).

Таблица 8.13. Значения y_{ij} (π)

S-блок (S_j)	Значение x_{ij}															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	12	4	6	2	10	5	11	9	14	8	13	7	0	3	15	1
S_2	6	8	2	3	9	10	5	12	1	14	4	7	11	13	0	15
S_3	11	3	5	8	2	15	10	13	14	1	7	4	12	9	6	0
S_4	12	8	2	1	13	4	15	6	7	0	10	5	3	14	9	11
S_5	7	15	5	10	8	1	6	13	0	9	3	14	11	4	2	12
S_6	5	13	15	6	9	2	12	10	11	7	8	1	4	3	14	0

S_7	8	14	2	5	6	9	1	12	15	4	11	0	13	10	3	7
S_8	1	7	14	13	0	5	8	3	4	15	10	6	9	12	11	2

«Кузнечик».

По типу, как и AES, относится к подстановочно-перестановочным сетям. В алгоритме разворачивания ключа (процедуре формирования итерационных ключей – ключевых элементов) используется сеть Фейстеля.

Схема зашифрования / расшифрования одного блока изображена на следующем рисунке.

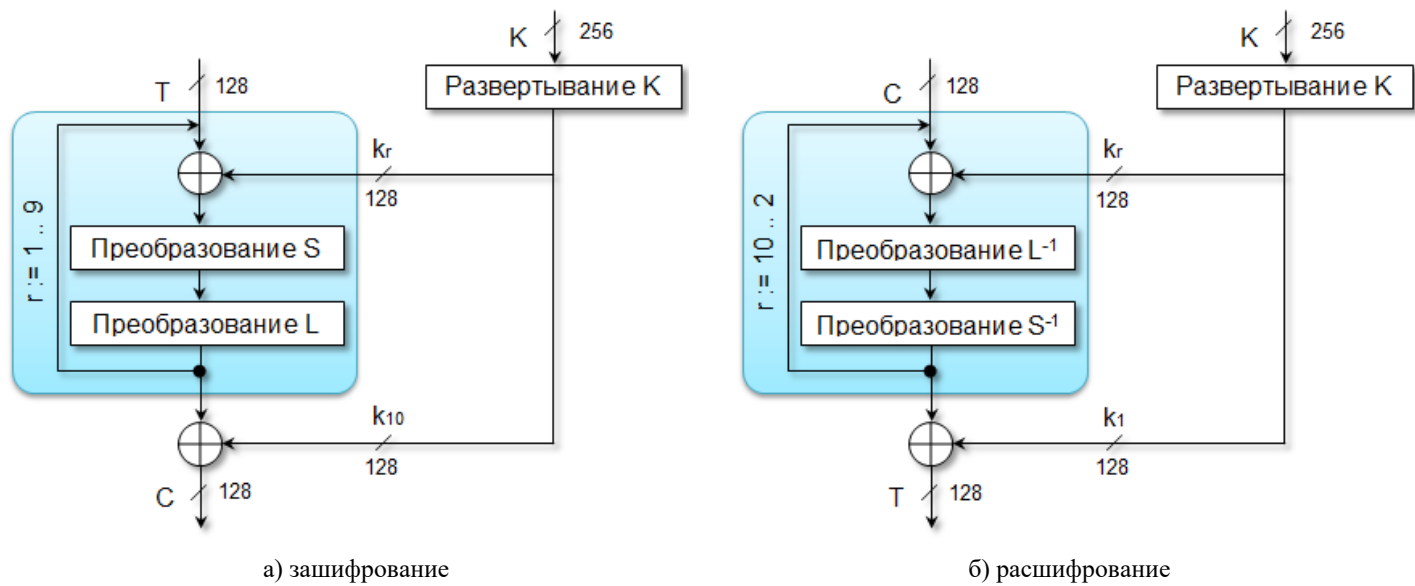


Рис.8.14

А. Развертывание К.

Формирование 10 итерационных ключей (ключевых элементов) выполняется по следующей схеме.

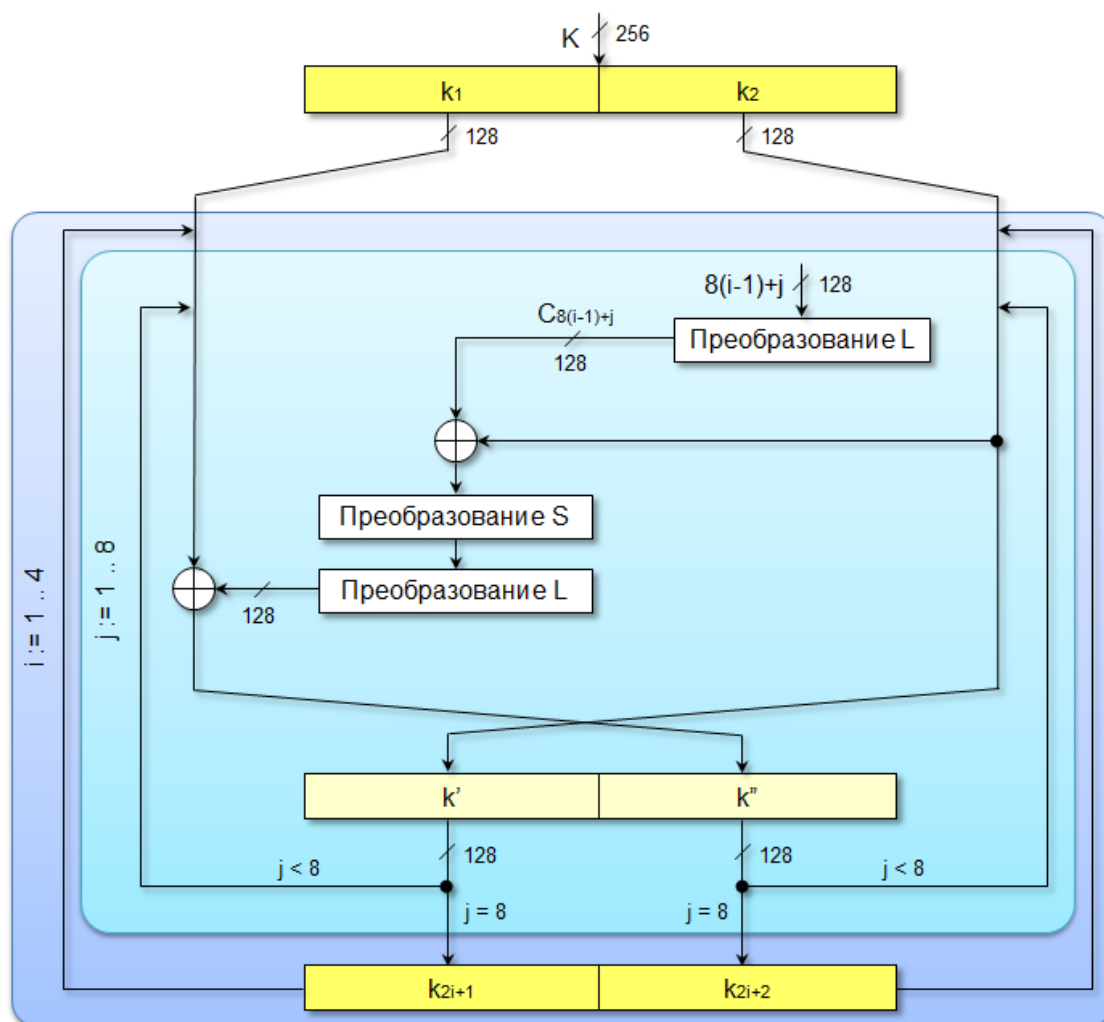


Рис.8.15. Развертывание К

Изначально ключ делится на две половины по 128 битов с получением первых двух итерационных ключей (k_1 и k_2).

Далее, в течение 4 раундов i , формируются остальные 8 итерационных ключей (k_{2i+1} и k_{2i+2}). Каждая последующая пара итерационных ключей получается в результате прогона предыдущей пары через сеть, состоящую из 8 ячеек Фейстеля (в ГОСТ ячейка обозначена F). При этом в начале каждой итерации j (ячейки F) должна быть получена итерационная константа $C_{8(i-1)+j}$ (не путать с обозначением блока шифрограммы C на рис.8.14). Для этого целое число $8(i-1)+j$, представленное в двоичном виде на 128 битов, должно пройти преобразование L .

А.1. Линейное преобразование L.

Преобразование байтов a_i входного 128-битового (16-байтового) массива V в течение 16 раундов по следующей схеме.

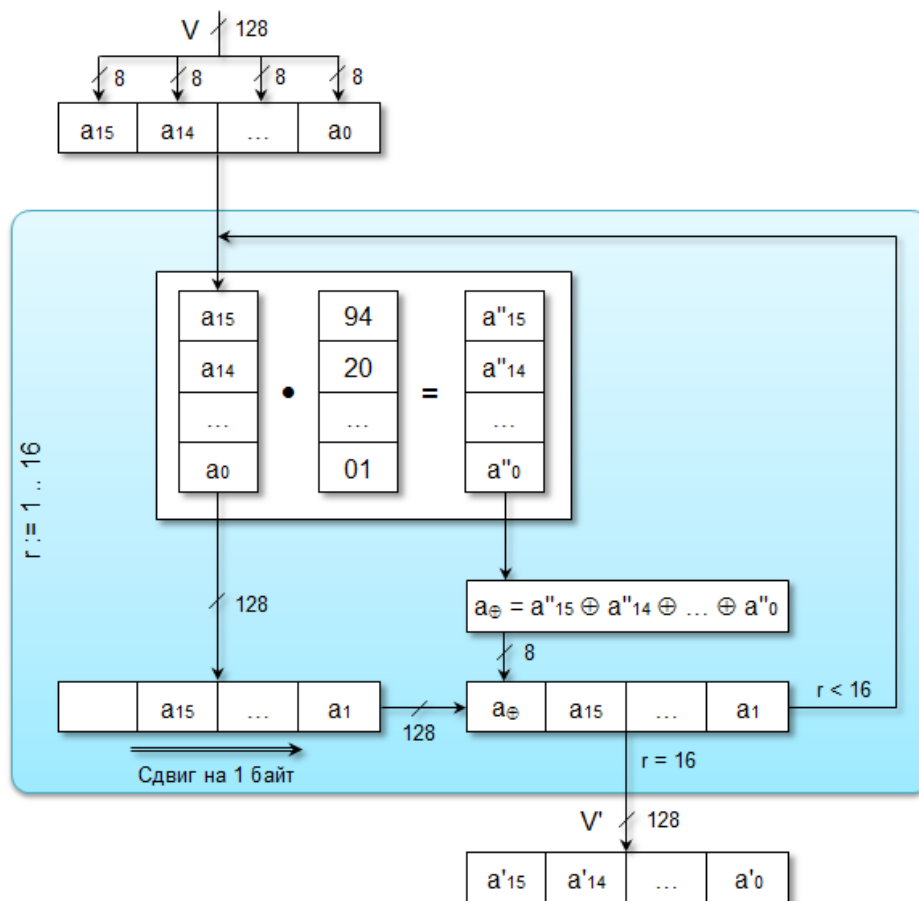


Рис.8.16. Линейное преобразование L

Один раунд состоит из следующей последовательности операций:

- умножение ($\bullet$) каждого байта a_i массива V на соответствующую константу, определенную в ГОСТ;
- сложение по модулю 2 результатов умножения ($a_{\oplus}$);
- сдвиг вправо элементов массива V на 1 байт;
- занесение $a_{\oplus}$ в качестве первого (старшего) байта массива V .

Массив констант по ГОСТ представлен в следующей таблице.

Таблица 8.14. Массив констант

№ п/п	Основание системы счисления		
	16	10	2
1	94	148	10010100
2	20	32	00100000
3	85	133	10000101
4	10	16	00010000
5	C2	194	11000010
6	C0	192	11000000
7	01	1	00000001
8	FB	251	11111011
9	01	1	00000001
10	C0	192	11000000
11	C2	194	11000010
12	10	16	00010000
13	85	133	10000101
14	20	32	00100000

15	84	148	10010100
16	01	1	00000001

Проиллюстрируем выполнение операций на примере 4 раунда определения итерационной константы C_1 (см. п.А.1.4 приложения А к ГОСТ 34.12-2015).

Массив V в начале итерации – $[84, 94, 01, 00, 00, \dots, 00]_{16} = [10000100, 10010100, 00000001, 00000000, 00000000, \dots, 00000000]_2$.

Умножение ($\bullet$) байта на константу выполняется в поле Галуа $GF(2^8)$ по модулю $x^8 + x^7 + x^6 + x + 1$ ($=111000011_2 = 1C3_{16}$) в соответствии с правилами полиномиальной арифметики (см. функцию MixColumns шифра AES):

- полиномиальное умножение:

$$\begin{array}{r}
 \begin{array}{r}
 84 * 94 \\
 * \begin{array}{r} 10000100 \\ 10010100 \end{array} \\
 \hline
 \begin{array}{r}
 00000000 \\
 00000000 \\
 10000100 \\
 00000000 \\
 10000100 \\
 00000000 \\
 00000000 \\
 00000000 \\
 10000100 \\
 \hline
 100100001010000 = 4850_{16}
 \end{array}
 \end{array}
 \quad
 \begin{array}{r}
 \begin{array}{r}
 94 * 20 \\
 * \begin{array}{r} 10010100 \\ 00100000 \end{array} \\
 \hline
 \begin{array}{r}
 00000000 \\
 00000000 \\
 00000000 \\
 00000000 \\
 00000000 \\
 00000000 \\
 10010100 \\
 00000000 \\
 00000000 \\
 \hline
 001001010000000 = 1280_{16}
 \end{array}
 \end{array}
 \quad
 \begin{array}{r}
 \begin{array}{r}
 01 * 85 \\
 * \begin{array}{r} 00000001 \\ 10000101 \end{array} \\
 \hline
 \begin{array}{r}
 00000001 \\
 00000000 \\
 00000000 \\
 00000001 \\
 00000000 \\
 00000000 \\
 00000000 \\
 00000000 \\
 00000000 \\
 00000001 \\
 \hline
 000000010000101 = 85_{16}
 \end{array}
 \end{array}
 \end{array}$$

- полиномиальное деление (для 85_{16} не требуется, т.к. число не превышает 8 битов):

$$\begin{array}{r}
 \begin{array}{r}
 4850 \bmod 1C3 \\
 \oplus \begin{array}{r} 100100001010000 \\ 111000011 \end{array} \\
 \oplus \begin{array}{r} 111000100 \\ 111000011 \end{array} \\
 \hline
 11110000 = F0_{16}
 \end{array}
 \quad
 \begin{array}{r}
 \begin{array}{r}
 1280 \bmod 1C3 \\
 \oplus \begin{array}{r} 1001010000000 \\ 111000011 \end{array} \\
 \oplus \begin{array}{r} 111010110 \\ 111000011 \end{array} \\
 \hline
 10101000 = A8_{16}
 \end{array}
 \end{array}$$

Сложение по модулю 2 результатов умножения - $a_{\oplus}$.

$$\begin{array}{r}
 \begin{array}{r}
 11110000 \\
 10101000 \\
 10000101 \\
 00000000 \\
 \oplus \\
 \hline
 00000000 \\
 11011101 = DD_{16}
 \end{array}
 \end{array}$$

Сдвиг массива V вправо – $[_ , 84, 94, 01, 00, \dots, 00]_{16}$.

Занесение $a_{\oplus}$ в качестве первого (старшего) байта массива V – $[DD, 84, 94, 01, 00, \dots, 00]_{16}$.

А.2. Нелинейное биективное преобразование S.

Замена каждого байта a_i входного 128-битового (16-байтового) массива V на байт подстановки π в соответствии со следующей таблицей.

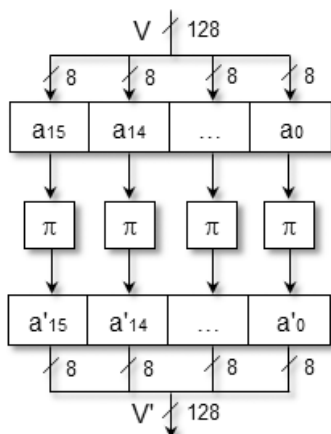


Таблица 8.15. Подстановки π
(16-теричное представление)

	_0	_1	_2	_3	_4	_5	_6	_7	_8	_9	_A	_B	_C	_D	_E	_F
0_	FC	EE	DD	11	CF	6E	31	16	FB	C4	FA	DA	23	C5	04	4D
1_	E9	77	F0	DB	93	2E	99	BA	17	36	F1	BB	14	CD	5F	C1
2_	F9	18	65	5A	E2	5C	EF	21	81	1C	3C	42	8B	01	8E	4F
3_	05	84	02	AE	E3	6A	8F	A0	06	0B	ED	98	7F	D4	D3	1F
4_	EB	34	2C	51	EA	C8	48	AB	F2	2A	68	A2	FD	3A	CE	CC
5_	B5	70	0E	56	08	0C	76	12	BF	72	13	47	9C	B7	5D	87
6_	15	A1	96	29	10	7B	9A	C7	F3	91	78	6F	9D	9E	B2	B1
7_	32	75	19	3D	FF	35	8A	7E	6D	54	C6	80	C3	BD	0D	57
8_	DF	F5	24	A9	3E	A8	43	C9	D7	79	D6	F6	7C	22	B9	03
9_	E0	0F	EC	DE	7A	94	B0	BC	DC	E8	28	50	4E	33	0A	4A
A_	A7	97	60	73	1E	00	62	44	1A	B8	38	82	64	9F	26	41
B_	AD	45	46	92	27	5E	55	2F	8C	A3	A5	7D	69	D5	95	3B
C_	07	58	B3	40	86	AC	1D	F7	30	37	6B	E4	88	D9	E7	89
D_	E1	1B	83	49	4C	3F	F8	FE	8D	53	AA	90	CA	D8	85	61
E_	20	71	67	A4	2D	2B	09	5B	CB	9B	25	D0	BE	E5	6C	52
F_	59	A6	74	D2	E6	F4	B4	C0	D1	66	AF	C2	39	4B	63	B6

При этом байт a_i в 16-теричном представлении состоит из двух символов, первый из которых указывает на номер строки подстановки π , а второй – на номер столбца. Например, если один из байтов $a_i = C5_{16}$, то он заменяется на $a'_i = AC_{16}$.

Иначе, таблицу подстановок π можно представить в виде одномерного массива. Тогда a_i – это индекс элемента массива, который служит заменой – $a'_i = \pi[a_i]$.

В. Зашифрование.

Зашифрование представляется собой последовательное применение к исходному блоку текста T в течение 9 раундов r гаммирования по модулю 2 с итерационными ключами k_r , а также преобразований S и L (см. А.1 и А.2). Для окончательного получения блока шифрограммы C результат раундовых преобразований складывается по модулю 2 с последним итерационным ключом k_{10} .

С. Расшифрование.

При расшифровании меняется не только порядок использования итерационных ключей (как в DES и ГОСТ 28147-89), но и выполняется инверсия всех операций.

С.1. Линейное преобразование L^{-1} .

Преобразование байтов a_i входного 128-битового (16-байтового) массива V в течение 16 раундов по следующей схеме.

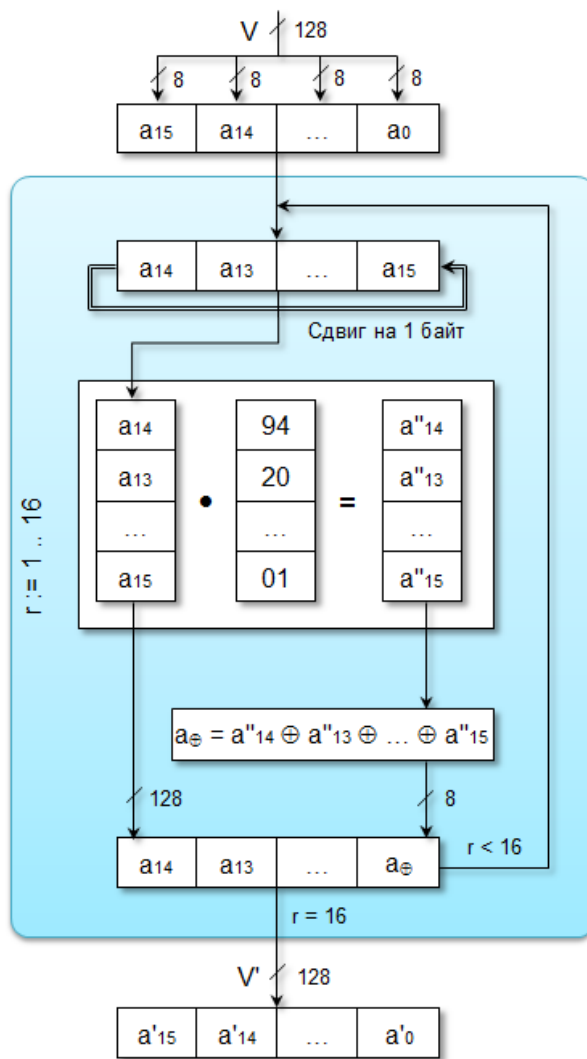


Рис.8.17. Линейное преобразование L^{-1}

Обратное линейное преобразование L^{-1} выполняется по тем же правилам, что и прямое L . К особенностям преобразования L^{-1} следует отнести:

- сдвиг выполняется в начале итерации;
- используется циклический сдвиг влево вместо простого сдвига вправо;
- результат сложения a_0 заносится как последний (младший) байт массива V .

С.2. Нелинейное биективное преобразование S^{-1} .

Замена байтов a_i входного 128-битового массива (16-байтового) V на байт подстановки π^{-1} в соответствии со следующей таблицей.

Таблица 8.16. Подстановки π^{-1}
(16-теричное представление)

	_0	_1	_2	_3	_4	_5	_6	_7	_8	_9	_A	_B	_C	_D	_E	_F
0_	A5	2D	32	8F	0E	30	38	C0	54	E6	9E	39	55	7E	52	91
1_	64	03	57	5A	1C	60	07	18	21	72	A8	D1	29	C6	A4	3F
2_	E0	27	8D	0C	82	EA	AE	B4	9A	63	49	E5	42	E4	15	B7
3_	C8	06	70	9D	41	75	19	C9	AA	FC	4D	BF	2A	73	84	D5
4_	C3	AF	2B	86	A7	B1	B2	5B	46	D3	9F	FD	D4	0F	9C	2F
5_	9B	43	EF	D9	79	B6	53	7F	C1	F0	23	E7	25	5E	B5	1E
6_	A2	DF	A6	FE	AC	22	F9	E2	4A	BC	35	CA	EE	78	05	6B
7_	51	E1	59	A3	F2	71	56	11	6A	89	94	65	8C	BB	77	3C
8_	7B	28	AB	D2	31	DE	C4	5F	CC	CF	76	2C	B8	D8	2E	36

9_	DB	69	B3	14	95	BE	62	A1	3B	16	66	E9	5C	6C	6D	AD
A_	37	61	4B	B9	E3	BA	F1	A0	85	83	DA	47	C5	B0	33	FA
B_	96	6F	6E	C2	F6	50	FF	5D	A9	8E	17	1B	97	7D	EC	58
C_	F7	1F	FB	7C	09	0D	7A	67	45	87	DC	E8	4F	1D	4E	04
D_	EB	F8	F3	3E	3D	BD	8A	88	DD	CD	0B	13	98	02	93	80
E_	90	D0	24	34	CB	ED	F4	CE	99	10	44	40	92	3A	01	26
F_	12	1A	48	68	F5	81	8B	C7	D6	20	0A	08	00	4C	D7	74

8.7. ГОСТ 34.13-2015 [59]

ГОСТ 34.13-2015 – российский стандарт симметричного блочного шифрования, введённый в действие 19 июня 2015 г. («ГОСТ 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»).

Является дополнением к ГОСТ 34.12-2015 и определяет режимы работы блочных шифров:

- простой замены (Electronic Codebook, ECB);
- гаммирования (Counter, CTR);
- гаммирования с обратной связью по выходу (Output Feedback, OFB);
- простой замены с сцеплением (Cipher Block Chaining, CBC);
- гаммирования с обратной связью по шифртексту (Cipher Feedback, CFB);
- выработки имитовставки (Message Authentication Code algorithm).

Для каждого из режимов в стандарте приведены схемы зашифрования / расшифрования, которые в качестве базовых операций используют процедуры зашифрования / расшифрования по ГОСТ 34.12-2015.

Вопросы для самопроверки

1. Дайте описание ячейки Фейстеля.
2. Назовите основные режимы DES.
3. Перечислите методы шифрования, используемые в DES-ECB.
4. Приведите схему алгоритма DES в режиме сцепления блоков шифра.
5. Назовите сферы применения разных режимов DES
6. Какова длина ключа шифра ГОСТ и как генерируются ключевые элементы.
7. Назовите основные различия между DES и ГОСТ.

9.1. Основы шифрования

Главная проблема использования одноключевых (симметричных) криптосистем заключается в распределении ключей. Для того, чтобы был возможен обмен информацией между двумя сторонами, ключ должен быть сгенерирован одной из них, а затем в конфиденциальном порядке передан другой. Особую остроту данная проблема приобрела в наши дни, когда криптография стала общедоступной, вследствие чего количество пользователей больших криптосистем может исчисляться сотнями и тысячами.

Начало асимметричным шифрам было положено в работе «Новые направления в современной криптографии» Уитфилда Диффи и Мартина Хеллмана, опубликованной в 1976 г. Находясь под влиянием работы Ральфа Меркла (Ralph Merkle) о распространении открытого ключа, они предложили метод получения секретных ключей для симметричного шифрования, используя открытый канал. В 2002 г. Хеллман предложил называть данный алгоритм «Диффи – Хеллмана – Меркла», признавая вклад Меркла в изобретение криптографии с открытым ключом [17].

Хотя работа Диффи-Хеллмана создала большой теоретический задел для открытой криптографии, первой реальной криптосистемой с открытым ключом считают алгоритм RSA (названный по имени авторов – Рон Ривест (Ronald Linn Rivest), Ади Шамир (Adi Shamir) и Леонард Адлеман (Leonard Adleman)).

Справедливости ради следует отметить, что в декабре 1997 г. была обнародована информация, согласно которой британский математик Клиффорд Кокс (Clifford Cocks), работавший в центре правительственной связи (GCHQ) Великобритании, описал систему, аналогичную RSA, в 1973 г., а несколькими месяцами позже в 1974 г. Малькольм Вильямсон изобрел математический алгоритм, аналогичный алгоритму Диффи – Хеллмана – Меркла.

Суть шифрования с открытым ключом заключается в том, что для шифрования данных используется один ключ, а для расшифрования другой (поэтому такие системы часто называют **асимметричными**).

Основная предпосылка, которая привела к появлению шифрования с открытым ключом, заключалась в том, что отправитель сообщения (тот, кто зашифровывает сообщение), не обязательно должен быть способен его расшифровывать. Т.е. даже имея исходное сообщение, ключ, с помощью которого оно шифровалось, и зная алгоритм шифрования, он не может расшифровать закрытое сообщение без знания ключа расшифрования.

Первый ключ, которым шифруется исходное сообщение, называется **открытым** и может быть опубликован для использования всеми пользователями системы. Расшифрование с помощью этого ключа невозможно. Второй ключ, с помощью которого дешифруется сообщение, называется **секретным** (закрытым) и должен быть известен только законному получателю закрытого сообщения.

Алгоритмы шифрования с открытым ключом используют так называемые необратимые или односторонние функции. Эти функции обладают следующим свойством: при заданном значении аргумента x относительно просто вычислить значение функции $f(x)$, однако, если известно значение функции $y = f(x)$, то нет простого пути для вычисления значения аргумента x . Например, функция **SIN**. Зная x , легко найти значение **SIN(x)** (например, $x = \pi$, тогда **SIN(π)** = 0). Однако, если **SIN(x)** = 0, однозначно определить x нельзя, т.к. в этом случае x может быть любым числом, определяемым по формуле $i * \pi$, где i – целое число.

Однако не всякая необратимая функция годится для использования в реальных криптосистемах. В их числе и функция **SIN**. Следует также отметить, что в самом определении необратимости функции присутствует неопределенность. Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.

Поэтому чтобы гарантировать надежную защиту информации, к криптосистемам с открытым ключом предъявляются два важных и очевидных **требования**.

1. Преобразование исходного текста должно быть условно необратимым и исключать его восстановление на основе открытого ключа.
2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне.

Все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих **типов односторонних преобразований**.

1. Разложение больших чисел на простые множители (алгоритм RSA).
2. Вычисление дискретного логарифма или дискретное возведение в степень (алгоритм Диффи-Хеллмана-Меркла, схема Эль-Гамала).
3. Задача об укладке рюкзака (ранца) (авторы Хелман и Меркл).
4. Вычисление корней алгебраических уравнений.
5. Использование конечных автоматов (автор Тао Ренжи).
6. Использование кодовых конструкций.
7. Использование свойств эллиптических кривых.

9.2. Алгоритм RSA

Стойкость RSA основывается на большой вычислительной сложности известных алгоритмов разложения числа на простые сомножители (делители). Например, легко найти произведение двух простых чисел 7 и 13 даже в уме – 91. Попробуйте в уме найти два простых числа, произведение которых равно 323 (числа 17 и 19). Конечно, для современной вычислительной техники найти два простых числа, произведение которых равно 323, не проблема. Поэтому для надежного шифрования алгоритмом RSA, как правило, выбираются простые числа, количество двоичных разрядов которых равно нескольким сотням.

[44] В августе 1977 г. знаменитый американский писатель и популяризатор науки Мартин Гарднер озаглавил свою колонку по занимательной математике в журнале Scientific American так: «Новый вид шифра, на расшифровку которого потребуются миллионы лет». После объяснения принципа системы шифрования с открытым ключом он показал само зашифрованное сообщение и открытый ключ N , используемый в этом шифре:

$N = 114\ 381\ 625\ 757\ 888\ 867\ 669\ 235\ 779\ 976\ 146\ 612\ 010\ 218\ 296\ 721\ 242\ 362\ 562\ 561\ 842\ 935\ 706\ 935\ 245\ 733\ 897\ 830\ 597\ 123\ 563\ 958\ 705\ 058\ 989\ 075\ 147\ 599\ 290\ 026\ 879\ 543\ 541$.

Гарднер призвал читателей попробовать расшифровать сообщение, используя предоставленную информацию, и даже дал подсказку: для решения необходимо разложить число N на простые множители p и q . Более того, Гарднер назначил приз в размере \$100 (приличная сумма на тот момент) тому, кто первым получит правильный ответ. Каждый, кто захочет побольше узнать о шифре, писал Гарднер, может обратиться к создателям шифра — Рону Ривесту, Ади Шамиру и Леонарду Адлеману из Лаборатории информации Массачусетского технологического института.

Правильный ответ был получен лишь через 17 лет. Он стал результатом сотрудничества более чем 600 человек. Ключами оказались $p = 32\ 769\ 132\ 993\ 266\ 709\ 549\ 961\ 988\ 190\ 834\ 461\ 413\ 177\ 642\ 967\ 992\ 942\ 539\ 798\ 288\ 533$ и $q = 3\ 490\ 529\ 510\ 847\ 650\ 949\ 147\ 849\ 619\ 903\ 898\ 133\ 417\ 764\ 638\ 493\ 387\ 843\ 990\ 820\ 577$, а зашифрованная фраза звучала так: «Волшебные слова — это брезгливый ягнтяк».

Авторы RSA поддерживали идею её активного распространения. В свою очередь, Агентство национальной безопасности (США), опасаясь использования этого алгоритма в

негосударственных структурах, на протяжении нескольких лет безуспешно требовало прекращения распространения системы. Ситуация порой доходила до абсурда. Например, когда программист Адам Бек (Adam Back) описал на языке Perl алгоритм RSA, состоящий из пяти строк, правительство США запретило распространение этой программы за пределами страны. Люди, недовольные подобным ограничением, в знак протеста напечатали текст этой программы на своих футболках [17].

Первым этапом любого асимметричного алгоритма является создание получателем шифрограмм пары ключей: открытого и секретного. Для алгоритма RSA этап создания ключей состоит из следующих операций.

Таблица 9.1. Процедура создания ключей

№ п/п	Описание операции	Пример
1	Выбираются два простых числа ¹ p и q .	p=7, q=13
2	Вычисляется произведение n = p * q.	n=91
3	Вычисляется функция Эйлера ² φ(n) .	$\varphi(n) = (7-1)(13-1) = 91-7-13+1 = 72$
4	Выбирается открытый ключ e - произвольное число ($0 < e < n$), взаимно простое ³ с результатом функции Эйлера ($e \perp \varphi(n)$).	e=5
5	Вычисляется закрытый ключ d - обратное число ⁴ к e по модулю φ(n) из соотношения $(d * e) \bmod \varphi(n) = 1$.	$(d*5) \bmod 72 = 1, d = 29$
6	Публикуются открытый ключ (e , n) в специальном хранилище, где исключается возможность его подмены (общедоступном сертифицированном справочнике).	

- Примечания.
- 1) **Простое число** — натуральное число, большее единицы и не имеющее других натуральных делителей, кроме самого себя и единицы.
- 2) Результат расчета **функции Эйлера φ(n)** равен количеству положительных чисел, не превосходящих **n** и взаимно простым с **n**. Некоторые случаи и способы расчета функции Эйлера приведены в следующей таблице.

Таблица 9.2. Способы расчета функции Эйлера

Расчетный случай	Формула	Пример (число / расчетная формула / список взаимно простых чисел)
n простое число	$\varphi(n) = n - 1$	$n = 7$ $\varphi(7) = 7 - 1 = 6$ {1, 2, 3, 4, 5, 6}
n = p q произведение двух простых чисел	$\varphi(n) = \varphi(p) \varphi(q) = (p - 1)(q - 1) = n - p - q + 1$ (за исключением случая p = q = 2)	$n = 15 = 3 * 5$ $\varphi(15) = \varphi(3) \varphi(5) = (3 - 1)(5 - 1) = 15 - 3 - 5 + 1 = 8$ {1, 2, 4, 7, 8, 11, 13, 14}
n = p ^q простое число в степени	$\varphi(n) = p^q - p^{q-1}$	$n = 9 = 3^2$ $\varphi(9) = 3^2 - 3^{2-1} = 9 - 3 = 6$ {1, 2, 4, 5, 7, 8}
n = p ₁ ^{q₁} p ₂ ^{q₂} ... p _k ^{q_k} разложение числа согласно основной теореме арифметики (общий случай)	$\varphi(n) = \varphi(p_1^{q_1}) \varphi(p_2^{q_2}) \dots \varphi(p_k^{q_k}) =$ $= p_1^{q_1-1} \left(1 - \frac{1}{p_1}\right) p_2^{q_2-1} \left(1 - \frac{1}{p_2}\right) \dots p_k^{q_k-1} \left(1 - \frac{1}{p_k}\right) =$ $= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$	$n = 84 = 2^2 3^1 7^1$ $\varphi(84) = 84 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{7}\right) = 24$ {1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41, 43, 47, 53, 55, 59, 61, 65, 67, 71, 73, 79, 83}

- 3) **Взаимно простые числа** – числа, не имеющие общих делителей, кроме 1, т.е. наибольший общий делитель которых равен 1.
- 4) **Обратными числами по модулю m** называются такие числа **n** и **n⁻¹**, для которых справедливо выражение **(n * n⁻¹) mod m = 1**. Для вычисления обратных чисел по модулю обычно используется расширенный алгоритм Евклида. В безмодульной математике **обратное число n⁻¹** (обратное значение, обратная величина) - число, на которое надо умножить данное число **n**, чтобы получить единицу (**n * n⁻¹ = 1**). Пара чисел, произведение которых равно единице, называются **взаимно обратными**. Например: 5 и 1/5, -6/7 и -7/6.

Процедуры шифрования и дешифрования выполняются по следующим формулам

C = T^e mod n, (9.1)

T = C^d mod n. (9.2)

где T, C - числовые эквиваленты символов открытого и шифрованного сообщения.

Пример шифрования по алгоритму RSA приведен в следующей таблице. Коды букв соответствуют их положению в русском алфавите (начиная с 1).

Таблица 9.3. Пример шифрования по алгоритму RSA

Открытое сообщение, T	Символ	A	Б	Р	А	М	О	В
	Код	1	2	18	1	14	16	3
Шифрограмма, C = T ⁵ mod 91		1	32	44	1	14	74	61
Открытое сообщение, T = C ²⁹ mod 91		1	2	18	1	14	16	3

Следует отметить, что **p** и **q** выбираются таким образом, чтобы **n** было больше кода любого символа открытого сообщения. В автоматизированных системах исходное сообщение переводится в двоичное представление, после чего шифрование выполняется над блоками бит равной длины. При этом длина блока должна быть меньше, чем длина двоичного представления **n**.

[44] Алгоритм RSA требует много машинного времени и очень мощных процессоров. До 1980-х гг. только правительства, армия и крупные предприятия имели достаточно мощные компьютеры для работы с RSA. В результате у них была фактически монополия на эффективное шифрование. Летом 1991 г. Филипп Циммерман, американский физик и борец за сохранение конфиденциальности, предложил бесплатную систему шифрования PGP (англ. Pretty Good Privacy — «достаточно хорошая степень конфиденциальности»), алгоритм которой мог работать на домашних компьютерах. PGP использует классическое симметричное шифрование, что и обеспечивает ей большую скорость на домашних компьютерах, но она шифрует ключи по асимметричному алгоритму RSA.

Циммерман объяснил причины этой меры в открытом письме, которое заслуживает быть процитированным здесь, по крайней мере, частично из-за пророческого описания

Это личное. Это конфиденциальное. И это только ваше дело и ничье другое. Вы можете планировать политическую кампанию, обсуждать ваши налоги или иметь тайную любовную связь. Или вы можете заниматься тем, что вам не кажется незаконным, хотя таковым является. Что бы то ни было, вы не хотите, чтобы ваши личные электронные письма или конфиденциальные документы были прочитаны кем-то еще. Нет ничего плохого в том, чтобы охранять вашу частную жизнь. Частная жизнь неприкосновенна, как Конституция...

Мы движемся к будущему, где мир будет опутан волоконно-оптическими сетями высокой емкости, связывающими наши повсеместно распространенные персональные компьютеры. Электронная почта станет нормой для всех, а не новинкой, как сегодня. Правительство будет защищать наши электронные сообщения государственными протоколами шифрования. Наверное, большинство людей примет это. Но, возможно, некоторые захотят иметь свои собственные защитные меры... Если конфиденциальность признать вне закона, только люди вне закона будут ею обладать.

Спецслужбы обладают лучшими криптографическими технологиями. Как и торговцы оружием и наркотиками. Как и военные подрядчики, нефтяные компании и другие корпорации-гиганты. Но обычные люди и общественные организации практически не имеют недорогих защитных криптографических технологий с открытым ключом. До сих пор не имели.

PGP дает людям возможность самим защищать свою конфиденциальность. Сегодня существует растущая социальная потребность в этом. Вот почему я написал PGP.

В заключении следует отметить стойкость данного алгоритма. В 2003 г. Ади Шамир и Эран Тромер разработали схему устройства TWIRL, которое при стоимости \$ 10 000 может дешифровать 512-битный ключ за 10 минут, а при стоимости \$ 10 000 000 – 1024-битный ключ меньше, чем за год. В настоящее время Лаборатория RSA рекомендует использовать ключи (параметр **n**) размером 2048 битов.

9.3. Алгоритм на основе задачи об укладке ранца

В 1978 г. Меркл и Хеллман предложили использовать задачу об укладке ранца (рюкзака) для асимметричного шифрования [8]. Она относится к классу NP-полных задач и формулируется следующим образом. Дано множество предметов различного веса. Спрашивается, можно ли положить некоторые из этих предметов в ранец так, чтобы его вес стал равен определенному значению? Более формально задача формулируется так: дан набор значений **M₁, M₂, ..., M_n** и суммарное значение **S**; требуется вычислить значения **b_i** такие что

S = b₁M₁ + b₂M₂ + ... + b_nM_n, (9.3)

где **n** – количество предметов;
b_i - бинарный множитель. Значение **b_i = 1** означает, что предмет **i** кладут в рюкзак, **b_i = 0** - не кладут.

Например, веса предметов имеют значения 1, 5, 6, 11, 14, 20, 32 и 43. При этом можно упаковать рюкзак так, чтобы его вес стал равен 22, использовав предметы весом 5, 6 и 11. Невозможно упаковать рюкзак так, чтобы его вес стал равен 24.

В основе алгоритма, предложенного Мерклом и Хеллманом, лежит идея шифрования сообщения на основе решения серии задач укладки ранца. Предметы из кучи выбираются с помощью блока открытого текста, длина которого (в битах) равна количеству предметов в куче. При этом биты открытого текста соответствуют значениям **b**, а текст является полученным суммарным весом. Пример шифрограммы, полученной с помощью задачи об укладке ранца, показан в следующей таблице.

Таблица 9.4. Пример шифрования на основе задачи об укладке ранца

Открытый текст	1	1	1	0	0	1	0	0	0	1	0	1	1	0	0	1	0	0	0	0	0	0	0	
Рюкзак (ключ)	1	5	6	11	14	20	32	43	1	5	6	11	14	20	32	43	1	5	6	11	14	20	32	43
Шифрограмма	32 (1+5+6+20)								73 (5+11+14+43)								0							

Суть использования данного подхода для шифрования состоит в том, что на самом деле существуют две различные задачи укладки ранца - одна из них решается легко и характеризуется линейным ростом трудоемкости, а другая, как принято считать, нет. Легкий для укладки ранец можно превратить в трудный. Раз так, то можно применить в качестве открытого ключа **трудный** для укладки ранец, который легко использовать для шифрования, но невозможно - для дешифрования. А в качестве закрытого ключа применить **легкий** для укладки ранец, который предоставляет простой способ дешифрования сообщения.

В качестве закрытого ключа (легкого для укладки ранца) используется сверхвозрастающая последовательность. **Сверхвозрастающей** называется **последовательность**, в которой каждый последующий член больше суммы всех предыдущих. Например, последовательность {2, 3, 6, 13, 27, 52, 105, 210} является сверхвозрастающей, а {1, 3, 4, 9, 15, 25, 48, 76} - нет.

Решение для сверхвозрастающего ранца найти легко. В качестве текущего выбирается полный вес, который надо получить, и сравнивается с весом самого тяжелого предмета в ранце. Если текущий вес меньше веса данного предмета, то его в рюкзак не кладут, в противном случае его укладывают в рюкзак. Уменьшают текущий вес на вес положенного предмета и переходят к следующему по весу предмету в последовательности. Шаги повторяются до тех пор, пока процесс не закончится. Если текущий вес уменьшится до нуля, то решение найдено. В противном случае, нет.

Например, пусть полный вес рюкзака равен 270, а последовательность весов предметов равна {2, 3, 6, 13, 27, 52, 105, 210}. Самый большой вес – 210. Он меньше 270, поэтому предмет весом 210 кладут в рюкзак. Вычитают 210 из 270 и получают 60. Следующий наибольший вес последовательности равен 105. Он больше 60, поэтому предмет весом 105 в рюкзак не кладут. Следующий самый тяжелый предмет имеет вес 52. Он меньше 60, поэтому предмет весом 52 также кладут в рюкзак. Аналогично проходят процедуру укладки в рюкзак предметы весом 6 и 2. В результате полный вес уменьшится до 0. Если бы этот рюкзак был бы использован для дешифрования, то открытый текст, полученный из значения шифртекста 270, был бы равен 10100101.

Открытый ключ представляет собой не сверхвозрастающую (нормальную) последовательность. Он формируется на основе закрытого ключа и, как принято считать, не позволяет легко решить задачу об укладке ранца. Для его получения все значения закрытого ключа умножаются на число **n** по модулю **m**. Значение модуля **m** должно быть больше суммы всех чисел последовательности, например, 420 (2+3+6+13+27+52+105+210=418). Множитель **n** должен быть взаимно простым числом с модулем **m**, например, 31. Результат построения нормальной последовательности (открытого ключа) представлен в следующей таблице.

Таблица 9.5. Пример получения открытого ключа

Закрытый ключ, k _i	2	3	6	13	27	52	105	210
Открытый ключ, (k _i *n) mod m = (k _i *31) mod 420	62	93	186	403	417	352	315	210

Для шифрования сообщение сначала разбивается на блоки, по размерам равные числу элементов последовательности в рюкзаке. Затем, считая, что единица указывает на присутствие элемента последовательности в рюкзаке, а ноль — на его отсутствие, вычисляются полные веса рюкзаков – по одному рюкзаку для каждого блока сообщения.

В качестве примера возьмем открытое сообщение «АБРАМОВ», символы которого представим в бинарном виде в соответствии с таблицей кодов символов Windows 1251. Результат шифрования с помощью открытого ключа {62, 93, 186, 403, 417, 352, 315, 210} представлен в следующей таблице.

Таблица 9.6. Пример шифрования

Открытое сообщение		Сумма весов	Шифрограмма (рюкзак), c_i
Символ	Bin-код		
A	1100 0000	62+93	155
Б	1100 0001	62+93+210	365
Р	1101 0000	62+93+403	558
A	1100 0000	62+93	155
М	1100 1100	62+93+417+352	924
О	1100 1110	62+93+417+352+315	1239
В	1100 0010	62+93+315	470

Для расшифрования сообщения получатель должен сначала определить обратное число n^{-1} , такое что $(n * n^{-1}) \bmod m = 1$. После определения обратного числа каждое значение шифрограммы умножается на n^{-1} по модулю m и с помощью закрытого ключа определяются биты открытого текста.

В нашем примере сверхвозрастающая последовательность равна {2, 3, 6, 13, 27, 52, 105, 210}, $m = 420$, $n = 31$. Значение n^{-1} равно 271 ($31 * 271 \bmod 420 = 1$).

Таблица 9.7. Пример расшифрования

Шифрограмма (рюкзак), c_i	$(c_i * n^{-1}) \bmod m = (c_i * 271) \bmod 420$	Сумма весов	Открытое сообщение	
			Символ	Bin-код
155	5	2+3	1100 0000	A
365	215	2+3+210	1100 0001	Б
558	18	2+3+13	1101 0000	Р
155	5	2+3	1100 0000	A
924	84	2+3+27+52	1100 1100	М
1239	189	2+3+27+52+105	1100 1110	О
470	110	2+3+105	1100 0010	В

В своей работе авторы рекомендовали брать длину ключа, равную 100 (количество элементов последовательности). В заключении следует отметить, что задача вскрытия данного способа шифрования успешно решена Шамиром и Циппелом в 1982 г.

9.4. Вероятностное шифрование

Вероятностное шифрование является разновидностью криптосистем с открытым ключом (авторы - Шафи Гольдвассер (Shafi Goldwasser) и Сильвио Микали (Silvio Micali)). Данный вид шифрования относят к допускающим **неоднозначное вскрытие**. Основной целью вероятностного шифрования является устранение утечки информации в криптографии с открытым ключом. Поскольку криптоаналитик всегда может зашифровать случайные сообщения открытым ключом, он может получить некоторую информацию. При условии, что у него есть шифртекст C ($C = E_{k1}(T)$) и он пытается получить открытый текст T , он может выбрать случайное сообщение T' и зашифровать: $C' = E_{k1}(T')$. Если $C' = C$, то он угадал правильный открытый текст. В противном случае он делает следующую попытку.

Вероятностное шифрование такую попытку атаки шифртекста делает бессмысленной. Другими словами, при шифровании с помощью одного и того же открытого ключа можно получить разные шифртексты, которые при расшифровке дают один и тот же открытый текст.

$$C_1 = E_{k1}(T), C_2 = E_{k1}(T), C_3 = E_{k1}(T), \dots, C_N = E_{k1}(T), \quad (9.4)$$

$$T = D_{k2}(C_1) = D_{k2}(C_2) = D_{k2}(C_3) = \dots = D_{k2}(C_N). \quad (9.5)$$

В результате, даже если у криптоаналитика имеется шифртекст C_i и он угадает T , то в результате операции шифрования получится $C_j = E_{k1}(T)$. Вероятность того, что $C_i = C_j$ крайне низка. Таким образом, криптоаналитик даже не узнает, была ли правильной его догадка относительно T или нет.

Нижеследующие рассматриваются два алгоритма вероятностного шифрования:

- алгоритм шифрования Эль-Гамала;
- алгоритм на основе эллиптических кривых.

9.5. Алгоритм шифрования Эль-Гамала

Схема была предложена Тахером Эль-Гамалем в 1984 г. Он усовершенствовал систему Диффи-Хеллмана и получил два алгоритма, которые использовались для шифрования и обеспечения аутентификации. Стойкость данного алгоритма базируется на сложности решения задачи дискретного логарифмирования.

Суть задачи заключается в следующем. Имеется уравнение

$$g^x \bmod p = y. \quad (9.6)$$

Требуется по известным g , y и p найти целое неотрицательное число x (**дискретный логарифм**).

Порядок создания ключей приводится в следующей таблице.

Таблица 9.8. Процедура создания ключей

№ п/п	Описание операции	Пример
1	Выбирается простое число p .	$p = 37$

2	Выбирается число g , являющееся первообразным корнем по модулю p ^{*)} и меньшее p .	g = 2
3	Выбираются произвольное число x , меньшее p .	x = 5
4	Вычисляется y = g ^{x} mod p .	y = 2 ⁵ mod 37 = 32 mod 37 = 32
5	Открытый ключ - y , g и p . Причем g и p можно сделать общими для группы пользователей. Закрытый ключ - x .	

*) **Первообразный (примитивный) корень по модулю p** – наименьшее положительное число **g** такое, что

$$g^{\phi(p)} \bmod p = 1$$

и

$$g^i \bmod p \neq 1, \quad \text{для } 1 \leq i < \phi(p)$$

где $\phi(p)$ – функция Эйлера (т.к. **p** – простое число, то $\phi(p) = p - 1$).

Проверка. При **g** = 2 и **p** = 37, $\phi(37) = 37 - 1 = 36$.

$2^{36} \bmod 37 = 1;$
 $2^1 \bmod 37 = 2 (\neq 1);$
 $2^2 \bmod 37 = 4 (\neq 1);$
 $2^3 \bmod 37 = 8 (\neq 1);$
 $2^4 \bmod 37 = 16 (\neq 1);$
...;
 $2^{34} \bmod 37 = 28 (\neq 1);$
 $2^{35} \bmod 37 = 19 (\neq 1).$

Для шифрования каждого отдельного блока исходного сообщения должно выбираться случайное число **k** ($1 < k < p - 1$). После чего шифрограмма генерируется по следующим формулам

$$a = g^k \bmod p, \quad (9.7)$$

$$b = (y^k T) \bmod p, \quad (9.8)$$

где **T** – исходное сообщение;
(**a**, **b**) – зашифрованное сообщение.

Дешифрование сообщения выполняется по следующей формуле

$$T = (b (a^x)^{-1}) \bmod p \quad (9.9)$$

или

$$T = (b a^{p-1-x}) \bmod p, \quad (9.10)$$

где $(a^x)^{-1}$ – обратное значение числа a^x по модулю **p**.

Пример шифрования и дешифрования по алгоритму Эль-Гамала при **k** = 7 приведен в таблице, хотя для шифрования каждого блока (в нашем случае буквы) исходного сообщения надо использовать свое случайное число **k**.

Первая часть шифрованного сообщения – $a = 2^7 \bmod 37 = 17$.

$a^x = 17^5 = 1419857, (a^x)^{-1} = 2 (1419857 * 2 \bmod 37 = 1)$ или $a^{p-1-x} = 17^{37-1-5} \approx 1.3928892 * 10^{38}$.

Таблица 9.9. Пример шифрования по алгоритму Эль-Гамала (при **k** = const)

Открытое сообщение, T	Символ	A	Б	Р	A	М	О	В
	Код	1	2	18	1	14	16	3
Шифрование	Случайное число k	7	7	7	7	7	7	7
	Первая часть шифрограммы, $a = 2^k \bmod 37$	17	17	17	17	17	17	17
	Вторая часть шифрограммы, $b = (32^k * T) \bmod 37$	19	1	9	19	7	8	20
Расшифрование	Обратное значение числа a^x по модулю p, $(a^x)^{-1}$	2	2	2	2	2	2	2
	Открытое сообщение, $T = (b * (a^x)^{-1}) \bmod 37$	1	2	18	1	14	16	3

Ввиду того, что число **k** является произвольным, то такую схему еще называют схемой **вероятностного шифрования**. Вероятностный характер шифрования является преимуществом для схемы Эль-Гамала, т.к. у схем вероятностного шифрования наблюдается большая стойкость по сравнению со схемами с определенным процессом шифрования. Недостатком схемы шифрования Эль-Гамала является удвоение длины зашифрованного текста по сравнению с начальным текстом. Для схемы вероятностного шифрования само сообщение **T** и ключ не определяют шифртекст однозначно. В схеме Эль-Гамала необходимо использовать различные значения случайной величины **k** для шифровки различных сообщений **T** и **T'**. Если использовать одинаковые **k**, то для соответствующих шифртекстов (**a**, **b**) и (**a'**, **b'**) выполняется соотношение $b (b')^{-1} = T (T')^{-1} \bmod p$. Из этого выражения можно легко вычислить **T**, если известно **T'**.

Пример. Предположим злоумышленник перехватил зашифрованное сообщение **C** = ((**a**₁, **b**₁), (**a**₂, **b**₂), ..., (**a**_n, **b**_n)), для которого использовалось одно и тоже случайное число **k**. Он знает один из блоков $T_i = E_{k1}(C_i)$ или при известном открытом ключе (**y**, **g**, **p**) ему удалось подобрать **k'**, которое совпало с используемым при шифровании **k**. Например по второму варианту, для шифрования символа **X** (**T'** = 22) злоумышленник использовал **k'** = 7 (равное **k**). Тогда, $b(X) = b' = (32^7 * 22) \bmod 37 = 11, (b')^{-1} = 27, (T')^{-1} = 32$. Расшифрование перехваченного сообщения приведено в следующей таблице.

Таблица 9.10. Пример расшифрования перехваченного сообщения

Вторая часть перехваченной шифрограммы, b	19	1	9	19	7	8	20
$L = (b * (b')^{-1}) \bmod p = (b * 27) \bmod 37$	32	27	21	32	4	31	22
Вскрытое открытое сообщение,	Код, определяемый по уравнению $(T * (T')^{-1}) \bmod p = L$ $(T * 32) \bmod 37 = L$						
	1	2	18	1	14	16	3

9.6. Алгоритм на основе эллиптических кривых

Использование эллиптических кривых для создания криптосистем было независимо предложено Нилом Коблицем (Neal Koblitz) и Виктором Миллером (Victor Miller) в 1985 г. [8, 17]. При использовании алгоритмов на эллиптических кривых полагается, что не существует быстрых алгоритмов для решения задачи дискретного логарифмирования в группах их точек. В настоящий момент известны лишь экспоненциальные алгоритмы вычисления обратных функций для эллиптических кривых. По сравнению с субэкспоненциальными алгоритмами разложения числа на простые сомножители (см. криптосистему RSA), это позволяет при одинаковом уровне стойкости уменьшить размерность ключа в несколько раз, а, следовательно, упростить программную и аппаратную реализацию криптосистем.

Эллиптической кривой **E** называется множество точек (x, y) , удовлетворяющих однородному уравнению Вейерштрасса:

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5, \quad (9.11)$$

где a_i - коэффициенты уравнения.

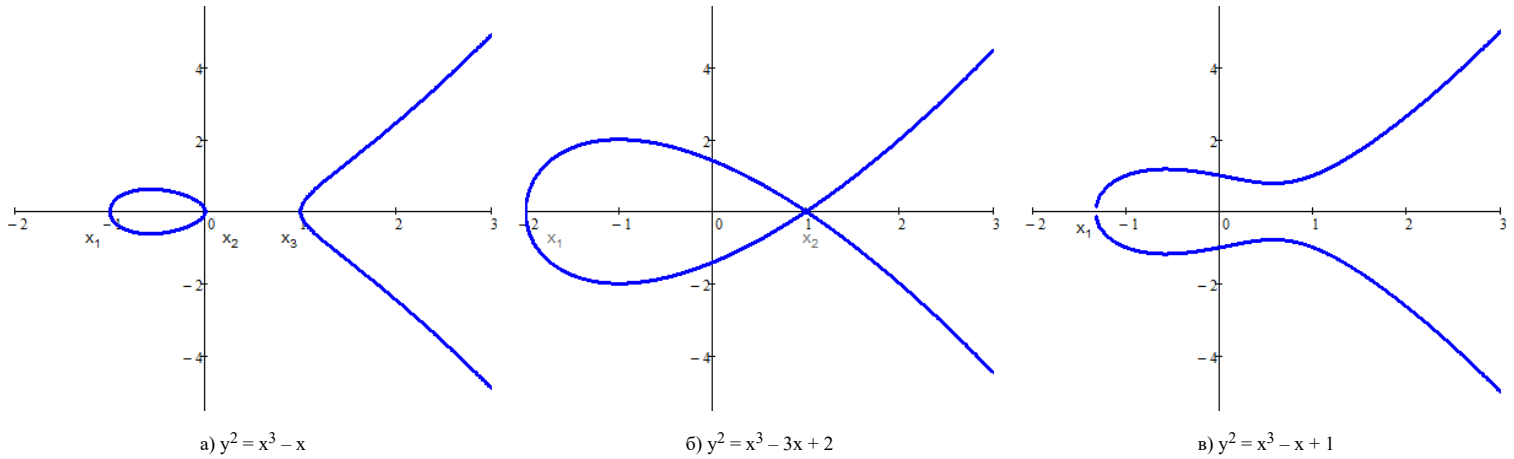


Рис.9.1. Примеры эллиптических кривых

В криптографии эллиптические кривые рассматриваются над двумя типами конечных полей: простыми полями нечётной характеристики ($\mathbb{Z}_n$, где $n > 3$ - простое число) и полями характеристики 2 ($\mathbb{GF}(2^m)$).

Эллиптические кривые над полями нечётной характеристики $\mathbb{Z}_n$ можно привести к виду, называемому эллиптической кривой в короткой форме Вейерштрасса:

$$y^2 = x^3 + Ax + B \pmod{n}, \quad (9.12)$$

где $A, B \in \mathbb{Z}_n$ - коэффициенты эллиптической кривой, удовлетворяющие $4A^3 + 27B^2 \neq 0 \pmod{n}$.

Поскольку $y = \pm\sqrt{x^3 + Ax + B}$, график кривой симметричен относительно оси абсцисс. Чтобы найти точки его пересечения с осью абсцисс, необходимо решить кубическое уравнение

$$x^3 + Ax + B = 0. \quad (9.13)$$

Это можно сделать с помощью известных формул Кардано. Дискриминант этого уравнения

$$\Delta = \left(\frac{A}{3}\right)^3 + \left(\frac{B}{2}\right)^2 = \frac{4A^3 + 27B^2}{108}. \quad (9.14)$$

Если $\Delta > 0$, то уравнение имеет три различных действительных корня (см. рис. 9.1а - x_1, x_2 и x_3). Если $\Delta = 0$, то уравнение имеет три действительных корня, по крайней мере, два из которых равны (см. рис. 9.1б - x_1 и x_2). Если $\Delta < 0$, то уравнение имеет один действительный корень (см. рис. 9.1в - x_1) и два комплексно сопряженных.

Используемые в криптографии кривые не должны иметь особых точек. Геометрически это значит, что график не должен иметь точек возврата и самопересечений (см. рис. 9.1б). Если кривая не имеет особых точек, то её график имеет две части при положительном дискриминанте (см. рис. 9.1а), и одну - при отрицательном (см. рис. 9.1в). Например, для графиков выше в первом случае дискриминант равен 64, а в третьем он равен -368.

Следует отметить, что в $\mathbb{Z}_n$ у каждого ненулевого элемента есть либо два квадратных корня, либо нет ни одного, поэтому точки эллиптической кривой разбиваются на пары вида $P = (x, y)$ и $-P = (x, -y)$. Например, эллиптическая кривая $y^2 = x^3 + 3x + 2$ при $x = 1$ и $n = 5$ имеет две точки в качестве решения: $P = (1, 1)$ и $-P = (1, -1)$, т.к. $1^2 \equiv 1^3 + 3 \cdot 1 + 2 \pmod{5}$ и $(-1)^2 \equiv 1^3 + 3 \cdot 1 + 2 \pmod{5}$.

Введем две операции, которые можно выполнять над точками кривой.

Сложение точек $P_3(x_3, y_3) = P_1(x_1, y_1) + P_2(x_2, y_2)$.

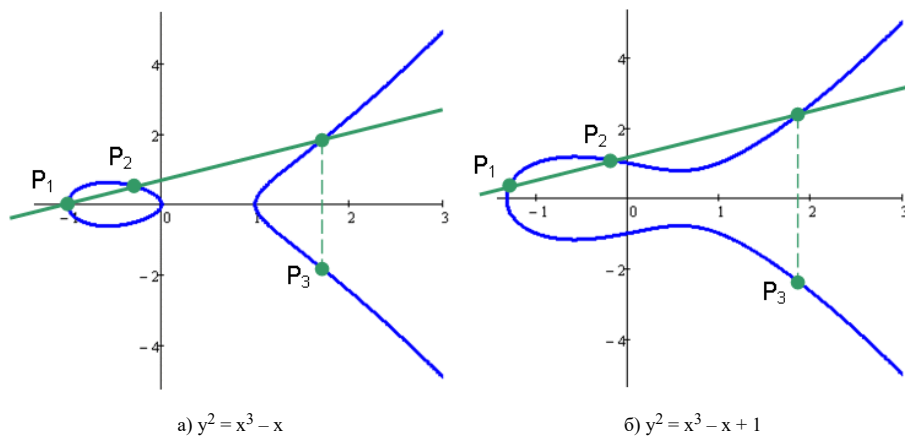


Рис.9.2. Сложение точек

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{3x_1^2 + A}{2y_1}, & x_1 = x_2 \end{cases} \quad (9.15)$$

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \quad (9.16)$$

В формулах 9.15 и 9.16 λ - угловой коэффициент прямой, проходящей через точки P_1 и P_2 . Если $P_1 = P_2$, то λ равен значению производной в точке P_1 .

Умножение точки на число $P_k(x_k, y_k) = k * P(x, y)$.

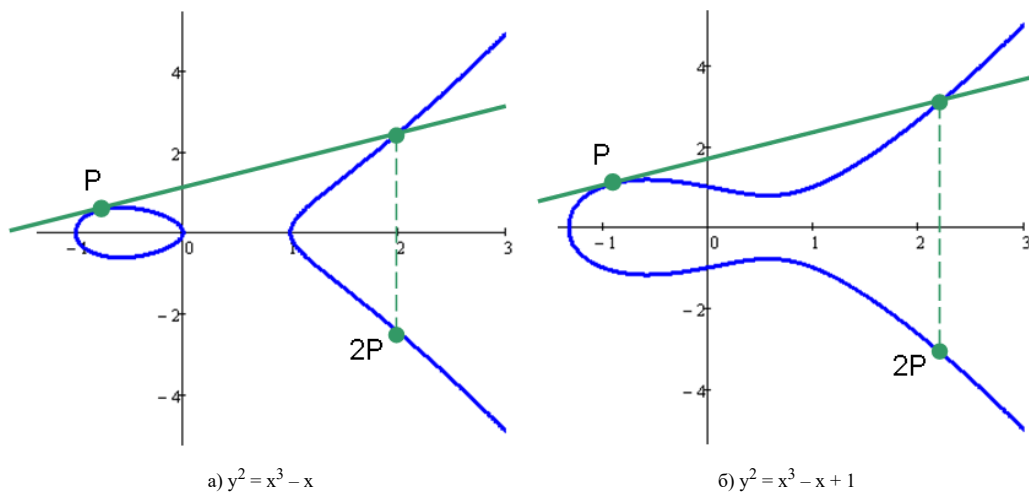


Рис.9.3. Удвоение точки

А) вариант 1 – выполнить сложение точки P k раз

$$P_k(x_k, y_k) = k \cdot P(x, y) = \underbrace{P + P + P + \dots + P}_k \quad (9.17)$$

В) вариант 2 – с использование двоичного представления числа $k = (b_L, \dots, b_2, b_1)$ и операции удвоения точки. Например, $k = 110_{10} = 1101110_2$, тогда $P_k = 64P + 32P + 8P + 4P + 2P$.

Алгоритм, вычисления P_k может выглядеть следующим образом.

```

1.  $P_k := \text{null}$ 
2.  $Q := P$ 
3. Цикл. Для  $i := 1$  до  $L$ 
    3.1. Если  $b_i = 1$ 
        то Если  $P_k = \text{null}$ 
            то  $P_k = Q$ 
            иначе  $P_k = P_k + Q$ 
    3.2.  $Q = 2 * Q$  //  $\approx Q = Q + Q$ 

```

Для $k = 110$ вместо 109 сложений будет 1 присваивание, 4 сложения и 6 удвоений (сложений).

Рассмотрим процедуру создания ключей.

Таблица 9.11. Процедура создания ключей

№ п/п	Описание операции	Пример
1	Выбирается модуль эллиптической кривой - простое число n ($n > 2^{255}$ - ГОСТ).	$n = 41$
2	Выбираются коэффициенты эллиптической кривой A и B . Должно соблюдаться условие $(4 A^3 + 27 B^2) \bmod n \neq 0$, в противном случае меняются параметры эллиптической кривой n, A или B.	$A = 3, B = 7$ $(4 * 3^3 + 27 * 7^2) \bmod 41 = 37$
3	Определяется точка эллиптической кривой P(x_p, y_p) и порядок циклической подгруппы группы точек эллиптической кривой q *). Принимается произвольное x_p ($0 < x_p < n$) и определяется y_p из уравнения эллиптической кривой. Должны соблюдаться условия: - для x_p должен существовать y_p (не для всякого x_p при данных параметрах кривой (A, B, n) может существовать y_p); - $P \neq O$ и $qP = O$, где O - нулевая точка эллиптической кривой ($P + (-P) = O$); - q – простое число; - $n^t \bmod q \neq 1$, для всех целых $t = 1, 2, \dots, T$, где $T \leq 31$; - $2^{254} < q < 2^{256}$ (ГОСТ). В противном случае меняются либо параметры эллиптической кривой n, A или B либо выбирается другая точка P.	$x_p = 7 ((7^3 + 3 * 7 + 7) \bmod 41 = 2),$ $y_p = 17 (17^2 \bmod 41 = 2)$ $q = 47$
4	Выбирается закрытый ключ d ($0 < d < q$).	$d = 10$
5	Определяется точка эллиптической кривой Q(x_q, y_q) : $Q(x_q, y_q) = d * P(x_p, y_p)$.	$x_q = 36,$ $y_q = 20$
6	Публикуется открытый ключ [(A, B), P(x_p, y_p), n, Q(x_q, y_q)] в специальном хранилище, где исключается возможность его подмены (общедоступном сертифицированном справочнике). Для выработки и проверки электронной цифровой подписи q является частью открытого ключа вместо n.	

*) Прямой способ вычисления порядка группы точек эллиптической кривой **q**.

1) Рассчитываются координаты первой точки из выражения

$$y^2 = x^3 + Ax + B \pmod n > y^2 = x^3 + 3x + 7 \pmod{41}.$$

Примем $x_1 = 7$, тогда $y_1^2 \bmod 41 = (7^3 + 3 * 7 + 7) \bmod 41 = 2$, откуда $y_1 = 17$.

$$P(x_p, y_p) = P(x_1, y_1) = P(7, 17).$$

2) Находим координаты второй точки. Для этого вначале вычисляется коэффициент λ

$$\lambda = \frac{(3x_1^2 + a)}{2y_1} \pmod n = \frac{3 * 7^2 + 3}{2 * 17} \pmod{41} = \frac{150}{34} \pmod{41} \Rightarrow$$
$$34\lambda \bmod 41 = 150 \bmod 41 \Rightarrow$$
$$34\lambda \bmod 41 = 27$$

Решая последнее уравнение, получаем $\lambda = 2$ ($34 * 2 \bmod 41 = 27$).

Координаты второй точки получаем путем удваивания первой из выражений

$$x_2 = (\lambda^2 - 2x_1) \bmod n = (2^2 - 2 * 7) \bmod 41 = -10 \bmod 41 = 31,$$

$$y_2 = (\lambda(x_1 - x_2) - y_1) \bmod n = (2(7 - 31) - 17) \bmod 41 = -65 \bmod 41 = 17.$$

3) Каждую следующую точку рассчитываем по формулам, пока в знаменателе первой формулы не будет получен 0:

$$\lambda_i = \frac{y_{i-1} - y_1}{x_{i-1} - x_1} \pmod n, \tag{9.18}$$

$$\begin{cases} x_i = (\lambda_i^2 - x_1 - x_{i-1}) \bmod n \\ y_i = (\lambda_i(x_1 - x_i) - y_1) \bmod n \end{cases} \tag{9.19}$$

Получаем:

- $\lambda_3 = 0, x_3 = 3, y_3 = 24$;
- $\lambda_4 = 29, x_4 = 11, y_4 = 31$;
- $\lambda_5 = 24, x_5 = 25, y_5 = 2$;
- ...;
- $\lambda_{46} = 2, x_{46} = 7, y_{46} = 24$.

К полученному числу точек добавляем точку **O**, в результате чего $q = 46 + 1 = 47$. Эта точка есть результат сложения любых двух точек $P(x_i, y_i)$ и $-P(x_i, -y_i)$ и представляет собой бесконечно удаленную точку, в которой гипотетически сходятся все вертикальные кривые.

Процедура шифрования отдельного блока выполняется следующим образом [25].

Таблица 9.12. Процедура шифрования отдельного блока (буквы)

№ п/п	Описание операции	Пример
1	Определяется десятичное представление буквы t .	Буква «К» $t = 12$
2	Выбирается случайное число k ($0 < k < n$).	$k = 5$
3	Определяется точка P_k(x_{pk}, y_{pk}) = k * P .	$P_k(25, 2)$
4	Определяется точка Q_k(x_{qk}, y_{qk}) = k * Q .	$Q_k(3, 24)$
5	Вычисляется c = (t * x_{qk}) mod n.	$c = (12 * 3) \bmod 41 = 36$
6	Шифрограмма – пара [P_k, c] .	$[P_k(25, 2), 36]$

Процедура расшифрования отдельного блока выполняется следующим образом.

Таблица 9.13. Процедура расшифрования отдельного блока (буквы)

№ п/п	Описание операции	Пример
1	Вычисляется точка $D(x_d, y_d) = d * P_k$.	$D(3, 24)$
2	Вычисляется десятичное представление зашифрованной буквы $t = (c * x_d^{-1}) \bmod n$, где x_d^{-1} – обратное число к x_d по модулю n .	$x_d^{-1} = 14 [(3 * 14) \bmod 41 = 1]$ $t = (36 * 14) \bmod 41 = 12$
3	Определяется исходное сообщение по ее десятичному представлению.	Буква «К»

Приведенный выше способ шифрования является вариацией шифрования Эль-Гамала. Если стойкость алгоритма шифрования Эль-Гамала базируется на сложности решения задачи дискретного логарифмирования, то стойкость шифрования с помощью эллиптических кривых базируется на сложности нахождения множителя **k** точки **P** по их произведению. Т.е. если **Q = k P**, то зная **P** и **k** довольно легко вычислить **Q**. Эффективное решение обратной задачи (найти **k** при известных **P** и **Q**) на текущий момент пока не опубликовано.

Вопросы для самопроверки

- 1. В чем заключается суть и основная предпосылка появления шифрования с открытым ключом?
- 2. Основные требования, предъявляемые к криптосистемам с открытым ключом.
- 3. Перечислите типы односторонних преобразований, применяемых при асимметричном шифровании.
- 4. Дайте краткую характеристику алгоритма RSA.
- 5. В чем отличие сверхвозрастающей последовательности от обыкновенной?
- 6. Что означает обратное число по модулю?
- 7. В чем отличие вероятностного шифрования с открытым ключом от детерминированного?
- 8. В чем суть задачи дискретного логарифмирования?
- 9. Приведите уравнение эллиптической кривой в короткой форме Вейерштрасса.

10. ХЕШ-ФУНКЦИИ

10.1. Основные понятия

Хеширование (иногда хэширование, англ. hashing) - преобразование входного массива данных произвольной длины в выходную строку фиксированной длины. Такие преобразования также называются **хеш-функциями** или **функциями свёртки**, входной массив – **прообразом**, а результаты преобразования - **хешем**, **хеш-кодом**, **хеш-образом**, **цифровым отпечатком** или **дайджестом сообщения** (англ. message digest).

Хеш-функция – легко вычисляемая функция, преобразующая исходное сообщения произвольной длины (прообраз) в сообщение фиксированное длины (хеш-образ), для которой не существует эффективного алгоритма поиска коллизий.

Коллизией для функции **h** называется пара значений **x, y**, $x \neq y$, такая, что $h(x) = h(y)$. Т.о. хеш-функция должна обладать следующими свойствами:

- для данного значения **h(x)** невозможно найти значение аргумента **x**. Такие хеш-функции называют **стойкими в смысле обращения** или **стойкими в сильном смысле**;
- для данного аргумента **x** невозможно найти другой аргумент **y** такой, что $h(x) = h(y)$. Такие хеш-функции называют **стойкими в смысле вычисления коллизий** или **стойкими в слабом смысле**.

В случае, когда значение хеш-функции зависит не только от прообраза, но и закрытого ключа, то это значение называют **кодом проверки подлинности сообщений (Message Authentication Code, MAC)**, **кодом проверки подлинности данных (Data Authentication Code, DAC)** или **имитовставкой**.

На практике хеш-функции используют в следующих целях:

- для ускорения поиска данных в БД;
- для проверки целостности и подлинности сообщений;
- для создания сжатого образа, применяемого в процедурах ЭЦП;
- для защиты пароля в процедурах аутентификации.

Ускорения поиска данных. Например, при записи текстовых полей в базе данных может рассчитываться их хеш-код и данные могут помещаться в раздел, соответствующий этому хеш-коду. Тогда при поиске данных надо будет сначала вычислить хеш-код текста и сразу станет известно, в каком разделе их надо искать, т.е. искать надо будет не по всей базе, а только по одному её разделу (это сильно ускоряет поиск).

Бытовым аналогом хеширования в данном случае может служить размещение слов в словаре по алфавиту. Первая буква слова является его хеш-кодом, и при поиске мы просматриваем не весь словарь, а только раздел с нужной буквой.

Процедура вычисления (стандартная схема алгоритма) хеш-функции представлена на следующем рисунке.

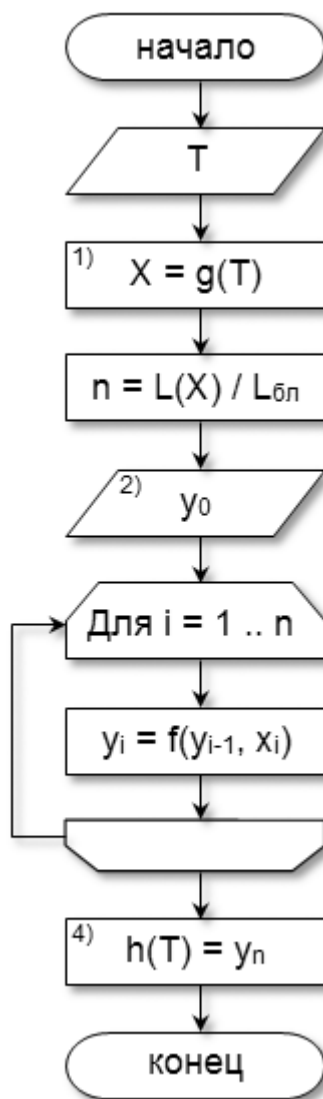


Рис.10.1. Процедура вычисления значения хеш-функции

1) К исходному сообщению T добавляется вспомогательная информация (например, длина прообраза, вспомогательные символы и т.д.) так, чтобы длина прообраза X стала кратной величине $L_{бл}$, определенной спецификацией (стандартом) хеш-функции.

2) Для инициализации процедуры хеширования используется синхропосылка y_0 .

3) Прообраз X разбивается на n блоков x_i ($i = 1 \dots n$) фиксированной длины $L_{бл}$, над которыми выполняется одностипная процедура хеширования $f(y_{i-1}, x_i)$, зависящая от результата хеширования предыдущего блока y_{i-1} .

4) Хеш-образом $h(T)$ исходного сообщения T будет результат процедуры хеширования y_n , полученный после обработки последнего блока x_n .

10.2. MD5

MD5 (англ. Message Digest 5) – 128-битный алгоритм хеширования, разработанный профессором Рональдом Л. Ривестом из Массачусетского технологического института (Massachusetts Institute of Technology, MIT) в 1991 г. Является улучшенной в плане безопасности версией MD4 [17].

Ниже приведен алгоритм вычисления хеша.

1. Выравнивание потока.

В конец исходного сообщения, длиной L , дописывают единичный бит, затем необходимое число нулевых бит так, чтобы новый размер L' был сравним с 448 по модулю 512 ($L' \bmod 512 = 448$). Добавление нулевых бит выполняется, даже если новая длина, включая единичный бит, уже сравнима с 448.

2. Добавление длины сообщения.

К модифицированному сообщению дописывают 64-битное представление длины данных (количество бит в сообщении). Т.е. длина сообщения T становится кратной 512 ($T \bmod 512 = 0$). Если длина исходного сообщения превосходит $2^{64} - 1$, то дописывают только младшие 64 бита. Кроме этого, для указанного 64-битного представления длины вначале записываются младшие 32 бита, а затем старшие 32 бита.

3. Инициализация буфера.

Для вычислений инициализируются 4 переменных размером по 32 бита и задаются начальные значения (шестнадцатеричное представление):

$A = 67\ 45\ 23\ 01$;
 $B = EF\ CD\ AB\ 89$;
 $C = 98\ BA\ DC\ FE$;
 $D = 10\ 32\ 54\ 76$.

В этих переменных будут храниться результаты промежуточных вычислений. Начальное состояние $ABCD$ называется инициализирующим вектором.

4. Вычисление хеша в цикле.

Исходное сообщение разбивается на блоки T , длиной 512 бит. Для каждого блока в цикле выполняется процедура, приведенная на рис.10.2. Результат обработки всех блоков исходного сообщения в виде объединения 32-битных значений переменных $ABCD$ и будет являться хешем.

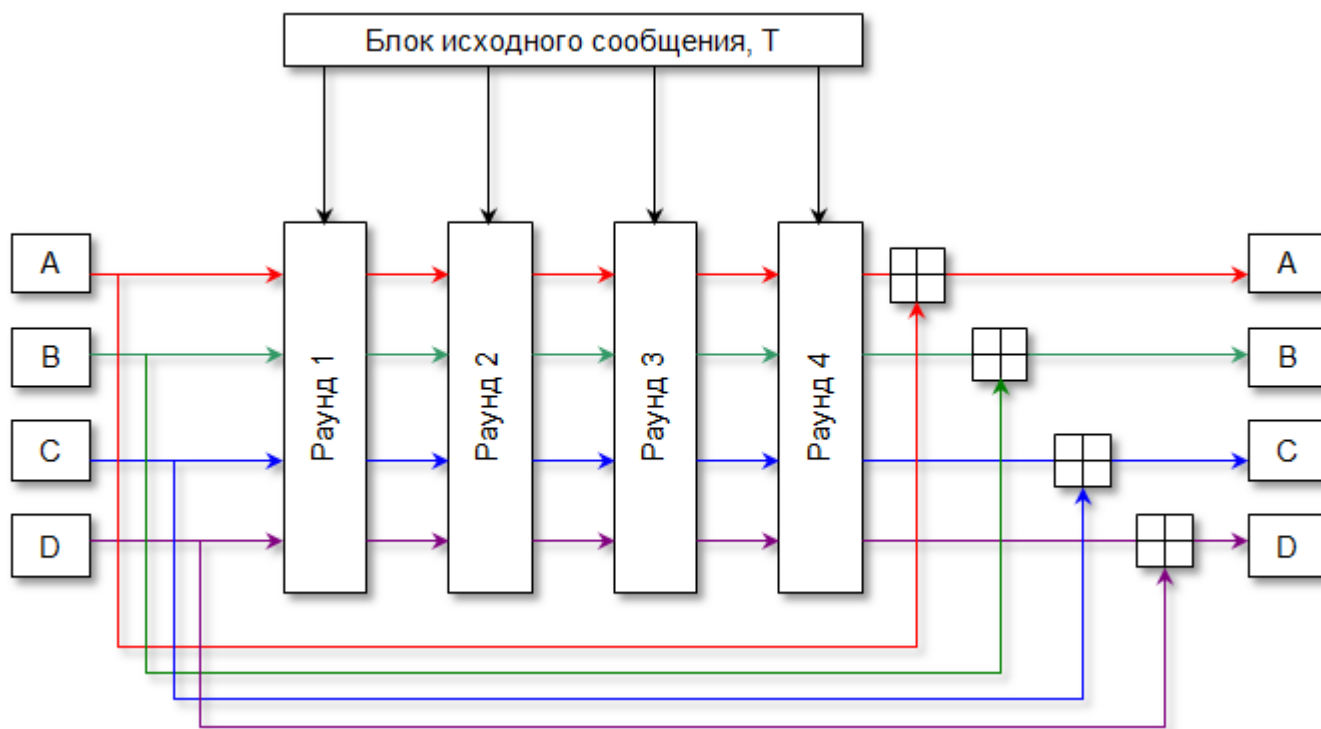


Рис.10.2. Шаг основного цикла вычисления хеша

В каждом раунде над переменными $ABCD$ и блоком исходного текста T в цикле (16 итераций)

выполняются однотипные преобразования по следующей схеме.

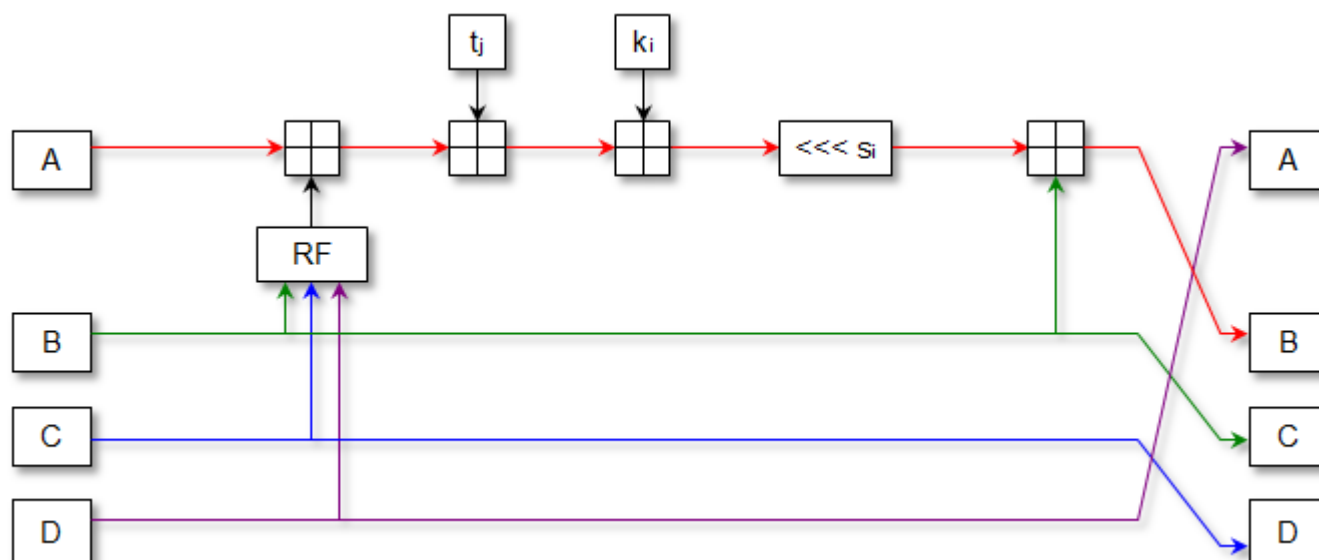


Рис.10.3. Одна итерация цикла раунда

Условные обозначения.

1) **RF** - раундовая функция, определяемая по следующей таблице.

Таблица 10.1. Раундовые функции RF

№ раунда	Обозначение функции	Формула расчета
1	F	$F(B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$
2	G	$G(B, C, D) = (B \wedge D) \vee (\neg D \wedge C)$
3	H	$H(B, C, D) = B \oplus C \oplus D$
4	I	$I(B, C, D) = C \oplus (\neg D \vee B)$

2) t_j - j -ая 32-битовая часть блока исходного сообщения T с обратным порядком следования байт;

3) k_i - целая часть константы, определяемой по формуле

$$k_i = 2^{32} * |\sin(i + 16 * (r - 1))|, \quad (10.1)$$

где i – номер итерации цикла ($i = 1..16$);

r – номер раунда ($r = 1..4$).

Аргумент функции $\sin$ измеряется в радианах.

4) $\boxplus$ – сложение по модулю 2^{32} .

5) $\lll s_i$ – циклический сдвиг влево на s_i разрядов.

Используемая 32-битовая часть блока исходного сообщения t_j и величина циклического сдвига влево s_j зависят от номера итерации и приведены в следующей таблице.

Таблица 10.2. Величины, используемые на шаге цикла раунда



№ итерации		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Раунд 1	t_j	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}	t_{11}	t_{12}	t_{13}	t_{14}	t_{15}	t_{16}
	s_i	7	12	17	22	7	12	17	22	7	12	17	22	7	12	17	22
Раунд 2	t_j	t_2	t_7	t_{12}	t_1	t_6	t_{11}	t_{16}	t_5	t_{10}	t_{15}	t_4	t_9	t_{14}	t_3	t_8	t_{13}
	s_i	5	9	14	20	5	9	14	20	5	9	14	20	5	9	14	20
Раунд 3	t_j	t_6	t_9	t_{12}	t_{15}	t_2	t_5	t_8	t_{11}	t_{14}	t_1	t_4	t_7	t_{10}	t_{13}	t_{16}	t_3
	s_i	4	11	16	23	4	11	16	23	4	11	16	23	4	11	16	23
Раунд 4	t_j	t_1	t_8	t_{15}	t_6	t_{13}	t_4	t_{11}	t_2	t_9	t_{16}	t_7	t_{14}	t_5	t_{12}	t_3	t_{10}
	s_i	6	10	15	21	6	10	15	21	6	10	15	21	6	10	15	21

После 4 раундов новое (модифицированное) значение каждой из переменных **ABCD** складывается ($\oplus$) с исходным (значением переменной до 1-го раунда).

5. Перестановка байт в переменных ABCD. После обработки всех блоков исходного сообщения для каждой переменной выполняется обратная перестановка байт.

Поиск коллизий.

В 2004 г. китайские исследователи Ван Сяюнь (Wang Xiaoyun), Фен Дэнгуо (Feng Dengguo), Лай Сюэцзя (Lai Xuejia) и Юй Хунбо (Yu Hongbo) объявили об обнаруженной ими уязвимости в алгоритме, позволяющей за небольшое время (1 час на кластере IBM p690) находить коллизии.

10.3. Применение шифрования для получения хеш-образа

Для выработки устойчивого к коллизиям хеш-образа могут применяться специальные режимы, предусмотренные в блочных шифрах (например, сцепление блоков шифра у DES), или в самой хеш-функции, как составная часть, может использоваться один из режимов блочного шифра (например, составной часть хеш-функции по ГОСТ 34.11-94¹ является режим простой замены алгоритма криптографического преобразования по ГОСТ 28147-89²).

Напомним что в случае, когда значение хеш-функции зависит не только от прообраза, но и закрытого ключа, то хеш-образ называют **кодом проверки подлинности сообщений (Message Authentication Code, MAC)**, **кодом проверки подлинности данных (Data Authentication Code, DAC)** или **имитовставкой**.

В качестве примера приведем режим DES-CBC (сцепление блоков шифра - Cipher Block Chaining).

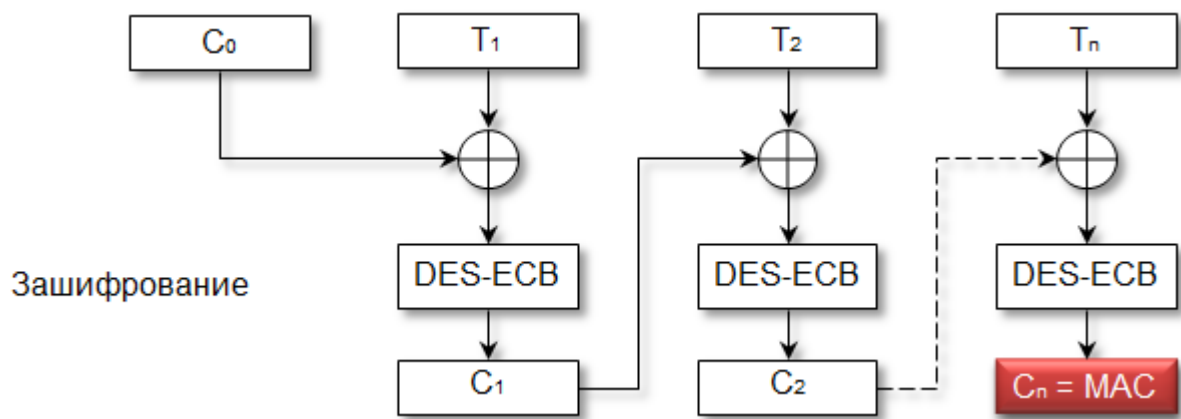


Рис.10.4. Схема алгоритма DES в режиме сцепления блоков шифра

Последний зашифрованный блок C_n и есть хеш-образ сообщения $T = \{T_1, T_2, \dots, T_n\}$.

¹ГОСТ 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

²ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Вопросы для самопроверки

1. Дайте определение понятиям: «хеширование», «хеш-функция», «коллизия».
2. В каких целях используют хеш-функции на практике?
3. Приведите стандартную схему алгоритма генерации хеш-образа.
4. Как называется хеш-образ, полученный с применением закрытого ключа шифрования?

11. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

В классической шенноновской модели¹ системы секретной связи имеются два полностью доверяющих друг другу участника, которым необходимо передавать между собой информацию, не предназначенную для третьих лиц. Задача обеспечения конфиденциальности (т.е. защиты секретной информации от внешнего противника), по крайней мере, исторически является **первой задачей криптографии**. Она традиционно решается с помощью криптосистем.

Кроме обеспечения конфиденциальности, криптография часто **используется для решения следующих задач**:

- проверка подлинности (аутентификация) – получатель сообщения должен иметь возможность установить его источник, а злоумышленник – не способен замаскироваться под кого-либо другого;
- обеспечение целостности – получатель сообщения может проверить, не было ли сообщение изменено в процессе доставки, а злоумышленник – не способен выдать ложное сообщение за подлинное;
- неотрицание авторства – отправитель сообщения впоследствии не должен иметь возможность отрицать посылку сообщения;
- обеспечение неотслеживаемости (анонимность) – отправитель сообщения может выполнять законные действия (например, оплату услуг через Интернет) не будучи опознанным (идентифицированным).

Если задача обеспечения конфиденциальности решается с помощью криптосистем, то для решения других задач разрабатываются криптографические протоколы. Имеются и другие **отличия криптографических протоколов от криптосистем**, из которых можно выделить следующие [9]:

- протоколы могут быть интерактивными, т.е. подразумевать многораундовый обмен сообщениями между участниками;
- в протоколе может быть задействовано более двух участников;
- участники протокола могут не доверять друг другу. Поэтому криптографические протоколы должны защищать их участников не только от внешнего противника, но и от нечестных действий партнеров.

Таким образом, **протокол** – совокупность правил, регламентирующих последовательность шагов, предпринимаемых двумя или большим количеством сторон для совместного решения некоторой задачи, а также регламентирующих форматы сообщений, пересылаемых между участниками обмена, и действия при возникновении сбоев.

Сбои при обмене сообщениями могут возникать в результате ошибочных, в т.ч. и преднамеренно ошибочных действий участников или изменении их последовательности, а также в результате пропадания или искажения передаваемых сообщений в передающей среде. На регламентацию действий в случае возникновения сбоев следует обратить особое внимание, поскольку ее часто упускают из виду, что может полностью разрушить безопасность участников даже в стойком криптографическом протоколе.

Описание протокола, исключаящее неоднозначность восприятия, называют **спецификацией протокола**.

Криптографические протоколы - сравнительно молодая отрасль математической криптографии. Первые протоколы появились примерно в конце 70-х г. двадцатого века. С тех пор эта отрасль бурно развивалась, и за последние десятилетия превратилась в основной объект исследований в теоретической криптографии. В

настоящий момент имеется уже не менее двух десятков различных типов криптографических протоколов. Все эти типы можно условно разделить на две группы: прикладные протоколы и примитивные. **Прикладной протокол** решает конкретную задачу, которая возникает (или может возникнуть) на практике. **Примитивные протоколы** используются как своеобразные «строительные блоки» при разработке прикладных протоколов.

В зависимости от наличия третьей стороны, которой безразличен результат исполнения протокола и его участники, протоколы делят на:

- протоколы с посредником. Посредник участвует в протоколе и помогает его исполнить двум сторонам. Стороны могут не доверять друг другу, но они полностью доверяют посреднику;
- протоколы с арбитром. Посредник вступает в протокол только в исключительных случаях - когда между сторонами возникают разногласия;
- самодостаточные протоколы. Честность сторон гарантируется самим протоколом.

Наиболее распространенными криптографическими протоколами являются:

- протоколы обмена ключами;
- протоколы аутентификации (идентификации);
- протоколы доказательства с нулевым разглашением;
- протоколы электронной цифровой подписи;
- протоколы контроля целостности;
- протоколы электронных платежей;
- протоколы голосования;
- протоколы тайных многосторонних вычислений;
- протоколы разбиения и разделения секрета и т.д.

¹Криптография была поставлена на научную основу во многом благодаря работам выдающегося американского ученого Клода Шеннона. Его доклад «Математическая теория криптографии» был подготовлен в секретном варианте в 1945 г., рассекречен и опубликован в 1948 г.

Вопросы для самопроверки

1. Перечислите основные задачи, для решения которых используется криптография.
2. Перечислите основные отличия криптопротоколов от традиционных криптосистем.
3. Дайте определение понятию «протокол».
4. Дайте классификацию криптопротоколов в зависимости от наличия третьей стороны.
5. Перечислите основные криптопротоколы.

12. ПРОТОКОЛЫ ОБМЕНА КЛЮЧАМИ

12.1. Общие положения

Для передачи секретной информации по открытым каналам связи абонентам необходимо иметь ключи. Либо единый ключ в случае использования симметричного шифрования, либо пару ключей для каждого абонента при асимметричном шифровании. Использование одного и того же ключа при многократном общении между абонентами позволяет противнику накопить богатый материал для криптоанализа. Поэтому в целях повышения безопасности обмена секретной информации широко используются сеансовые ключи. **Сеансовый (сессионный) ключ** – ключ, используемый абонентами в рамках одного сеанса (сессии, раунда) общения. Более того, в некоторых криптосистемах предусматривается многократная смена ключа в рамках одного сеанса, временные метки¹, некоторая дополнительная информация, усиливающие безопасность криптосистемы. Использование сеансовых ключей позволяет решить также и вторую проблему - ограничить размер ущерба при компрометации ключа.

Возможны следующие разновидности протоколов обмена ключами **в зависимости от стороны, вырабатывающей сеансовый ключ**:

- ключ вырабатывается одним из абонентов и высылается второму для последующего информационного обмена;
- совместная выработка ключа абонентами;
- ключ вырабатывается и предоставляется абонентам третьей стороной (доверенным центром).

Кроме этого, обмен ключами может выполняться как с помощью симметричного, так и асимметричного шифрования.

При традиционном симметричном шифровании и распределении ключей может использоваться третья сторона (доверенный центр) или абоненты могут обладать выделенным ключом (назовем его суперключ), который используется только для шифрования, пересылки и расшифрования сеансовых ключей (см. сервер аутентификации Kerberos). Ввиду того, что сеансовый ключ это случайный (псевдослучайный) набор 0 и 1 небольшой длины, то его перехват и дешифровка противником крайне затруднительна даже при многократном использовании суперключа.

Совместная выработка ключа может быть выполнена с использованием асимметричной или квантовой криптографии.

¹**Временные метки (метки времени)** используются для обеспечения гарантий своевременности и единственности сообщений, а также для обнаружения попыток навязывания ранее переданной информации.

12.2. Алгоритм Диффи-Хеллмана-Меркла

Если рассматривать стойкость симметричного и асимметричного шифрования, то при одинаковой длине ключа сравнение будет не в пользу последних. Более того, для асимметричного шифрования требуется времени на порядки больше, чем симметричных. В то же время, асимметричные методы шифрования

позволяют достаточно безопасно выполнять действия, которые с помощью симметричного шифрования выполнить невозможно. На одной из лекции отмечалась работа Уитфилда Диффи и Мартина Хеллмана, в которой содержалось описание алгоритма, позволявшего сторонам сгенерировать общий секретный ключ для информационного обмена посредством симметричного шифрования.

Этот алгоритм, предложенный в 1976 г., стал первым в истории **алгоритмом с открытым ключом** [8].

Таблица 12.1. Обмен ключами по алгоритму Диффи-Хеллмана-Меркла

№ п/п	Описание операции	Пример
1	А и Б вместе выбирают простое число n и первообразный корень по модулю $n^{*}) - g$. Числа n и g можно передавать по открытому каналу.	$n = 11$ $g = 2$
2	А выбирает случайное число x и посылает Б результат $X = g^x \bmod n$.	$x = 4$ $X = 2^4 \bmod 11 = 5$
3	Б выбирает случайное число y и посылает А результат $Y = g^y \bmod n$.	$y = 6$ $Y = 2^6 \bmod 11 = 9$
4	А вычисляет секретный ключ $k = Y^x \bmod n$.	$k = 9^4 \bmod 11 = 5$
5	Б вычисляет секретный ключ $k = X^y \bmod n$.	$k = 5^6 \bmod 11 = 5$

*) Определение первообразного корня по модулю см. в теме 9 «Шифрование с открытым ключом».

Значения k и k' оба равны $g^{xy} \bmod n$ ($2^{4*6} \bmod 11 = 5$). Данный протокол можно расширить на случай с тремя и более участниками. Например, для случая с тремя участниками, секретный ключ k будет равен $g^{xyz} \bmod n$. Вначале каждый участник вычисляет $X = g^x \bmod n$, $Y = g^y \bmod n$ и $Z = g^z \bmod n$. Затем передают эти значения по кругу и опять шифруют на собственном ключе $Z' = Z^X \bmod n$, $X' = X^Y \bmod n$ и $Y' = Y^Z \bmod n$. И снова передают по кругу и получают значение ключа $k = Y'^X \bmod n$, $k = Z'^Y \bmod n$ и $k = X'^Z \bmod n$.

12.3. Протокол BB84

BB84 (Bennet-Brassard - 1984) - первый протокол квантового обмена ключами, который был предложен в 1984 г. Чарльзом Беннетом и Жилем Брассардом. Квантовая криптография, как и асимметричная, также началась с протокола обмена ключами.

Для генерации ключа отправитель пропускает фотоны через четыре традиционных однонаправленных фильтра (линейных поляризатора). Получатель для определения посылаемых бит (поляризации фотонов) применяет две поляризационные разделительные призмы, работающие в прямолинейном и диагональном базисах.

Генерация общего ключа выполняется в следующей последовательности.

Этап 1. Отправитель генерирует случайную последовательность бит и для каждого из них, случайным образом выбирая один из двух возможных однонаправленных фильтров, посылает получателю

поляризованные фотоны.

Этап 2. Получатель измеряет поляризацию полученных фотонов, случайным образом чередуя прямолинейный и диагональный базисы. Т.к. он не знает последовательности фильтров, используемых отправителем, большая часть битов будет определена неправильно.

Этап 3. Получатель открыто сообщает отправителю порядок использования им базисов.

Этап 4. Отправитель открыто сообщает получателю, какие базисы были выбраны получателем правильно.

Этап 5. Биты для правильно выбранных базисов используются для проверки целостности переданных данных и формирования ключа. В оригинальном протоколе BB84 из этих «правильных» битов выбирается определенная часть и открыто сравнивается. В случае совпадения (канал не прослушивается и данные дошли без искажений), оставшаяся часть используется для формирования ключа требуемой длины. Для контроля целостности можно использовать и другие методы, например хеш-образы (контрольные суммы).

Таблица 12.2. Пример обмена ключами по протоколу BB84

Э т а п ы	1	Случайным образом сгенерированные биты	0	0	1	1	0	0	1
		Фильтры, выбранные отправителем							
	2	Фильтры, выбранные получателем							
		Биты, определенные получателем	0	1	1	1	1	0	0
	3, 4	Проверка правильности применения фильтров получателем	V			V		V	
	5	Биты для контроля целостности и формирования ключа	0			1		0	

- В случае применения получателем неправильно выбранных базисов возможны следующие ситуации:
- часть определенных получателем битов для одной и той же пары однонаправленных фильтров и базисов (см. биты 3 и 7) может иметь разные значения в силу особенностей прохождения призм фотонами;
 - биты, определенные получателем, могут совпасть со сгенерированными отправителем (см. бит 3), но они все равно отбрасываются из-за вероятностной природы этого совпадения. Правильность определения бит для неподходящих базисов можно выявить только открытым сравнением, что исключается.

Вопросы для самопроверки

1. Дайте определение понятию «сеансовый ключ».
2. Опишите алгоритм обмена ключами Диффи-Хеллмана-Меркла.

3. В чем отличие квантового шифрования от квантового протокола обмена ключами.

13. ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ (ИДЕНТИФИКАЦИИ)

13.1. Общие сведения

Идентификация (англ. identification) - процесс распознавания сущностей путем присвоения им уникальных меток (идентификаторов, логинов).

Аутентификация (англ. authentication) - проверка соответствия (подлинности) сущности предъявленному ею идентификатору. (Заметим, что происхождение русскоязычного термина «аутентификация» не совсем понятно. Английское «authentication» скорее можно прочитать как «аутентикация»; трудно сказать, откуда в середине взялось еще «фи» – может, из идентификации? Тем не менее, термин устоялся и закреплен в РД Гостехкомиссии РФ).

Для полноты картины приведем определение термина авторизация, который не следует путать с двумя вышеприведенными. **Авторизация** (англ. authorization) - предоставление сущности возможностей в соответствии с положенными ей правами или проверка наличия прав при попытке выполнить какое-либо действие.

Идентификация и аутентификация – это первая линия обороны, «входная дверь» в информационное пространство организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает.

Идентификация сродни присвоению имени ребенку (не совсем точное сравнение, но все же). В любой ИС должны быть определены все субъекты, участвующие в информационном обмене. Часть из них может быть сгруппирована, если они наделены одинаковыми (схожими) правами и обладают одинаковыми (схожими) характеристиками. Каждый субъект (группа субъектов) должен обладать уникальным именем (обозначением).

Аутентификация бывает **односторонней** (обычно клиент доказывает свою подлинность серверу) и **двусторонней** (взаимной). Пример односторонней аутентификации – процедура входа пользователя в систему.

Субъект может подтвердить свою подлинность, предъявив один из следующих **аутентификаторов**:

- нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);
- нечто, чем он владеет (паспорт, личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев, образец ДНК и т.п.).

В том случае, если в ходе процедуры аутентификации клиент должен предъявить сразу несколько аутентификаторов, аутентификация называется **многофакторной**. Например, в ходе двухфакторной аутентификации клиент должен знать пароль и воспользоваться личной карточкой.

Рассмотрим основные программно-технические способы реализации идентификации и аутентификации:

- пароли;
- с использованием хеш-функции;
- на основе шифрования с открытым ключом;
- сервер аутентификации Kerberos;
- биометрия;
- идентификационные карты и электронные ключи.

13.2. Парольная идентификация/аутентификация

Введенный пользователем пароль сравнивается с паролем, имеющимся в БД, хранящейся в защищаемой ИС, и если они совпадают, то дается разрешение на использование защищаемых ресурсов.

Главное **достоинство** парольной аутентификации – простота и привычность. Пароли давно встроены в ОС, СУБД и программные продукты. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Парольная аутентификация имеет массу **недостатков**:

- как правило, пароль генерируется в одном месте (например, на сервере) и должен быть передан во второе (например, клиенту). При передаче пароль может быть перехвачен злоумышленником;
- многие ОС и приложения имеют пароли, указанные производителем по умолчанию. После установки такой системы очень часто забывают их удалить. БД стандартных паролей можно найти в Интернете;
- злоумышленник может получить БД паролей, хранящихся в зашифрованном виде, и воспользоваться ей:
 - в Windows NT/2000/XP учетные записи (пользователи и пароли) хранятся в файле «%System Root%\System32\Config\sam». При работающем ОС пользователь не может выполнять операции чтения/записи с данным файлом (блокируется процессом lsass.exe, «убить» который невозможно). Получить доступ к файлу можно, загрузив ОС с другого носителя. Другой вариант заключается в использовании файла «%System Root%\Repair\sam». Он доступен для чтения/записи, но, как правило, содержит пароли «столетней» давности;
 - в ранних версиях Unix файл с учетными записями «/etc/passwd» был доступен для чтения любым желающим. В современных разновидностях Unix файл с паролями «/etc/shadow» или «etc/secure» доступен только с привилегиями супервизора. Другой способ получения доступа к паролям – обрушения процесса, обращающегося к файлу с паролями. При этом Unix создает файл «core dump», содержащий дампы памяти (с паролями) [26];
- после получения файла с зашифрованными паролями можно воспользоваться многочисленными программами-взломщиками. Одними из самых популярных взломщиков являются: для Windows – L0phtCrack, для Unix – John the Ripper. Время, требуемое для взлома пароля, зависит от его качества. Так, например, взлом пароля для L0phtCrack на компьютере с процессором Xeon 400 МГц при использовании [26]:
 - цифр и латиницы – 5,5 часов;
 - всех символов – 480 часов.
- кроме перечисленных выше приемов взлома паролей, их можно подсмотреть (например, с помощью оптических приборов), сообщить другу/подруге (если секрет знают двое – это уже не секрет), записать на бумажке и приклеить на клавиатуру или монитор и т.п.

Тем не менее, так как парольная защита используется во многих продуктах и системах, можно порекомендовать следующие **меры, позволяющие повысить надежность парольной защиты**:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.). Еще лучше воспользоваться программами - генераторами паролей (ключей);

- ограничение доступа к файлу с паролями;
- удаление резервных копий файлов с паролями («%System Root%\Repair\sam»);
- использование защищенных протоколов обмена ключами (например, основанные на протоколе обмена ключами Диффи-Хеллмана);
- ограничение числа неудачных попыток входа в систему (это затруднит применение «метода грубой силы»). В Windows 2000 и XP этот параметр устанавливается по пути «Администрирование / Локальная политика безопасности / Политики учетных записей / Политика блокировки учетной записи / Пороговое значение блокировки». Там же («Политики учетных записей») можно настроить срок блокировки учетной записи, минимальную длину пароля, сроки его действия и т.п.;
- управление сроком действия паролей, их периодическая смена, использование сеансовых ключей;
- удаление паролей уволенных или лишенных полномочий пользователей.

13.3. Протокол идентификации/аутентификации с использованием хеш-функции

Напомним, что хеш-функция – легко вычисляемая функция, преобразующая исходное сообщения произвольной длины (прообраз) в сообщение фиксированной длины (хеш-образ), для которой не существует эффективного алгоритма поиска коллизий.

При идентификации/аутентификации пользователь вводит пароль, а по каналу связи высылается его хеш-образ. Проверяющая система сравнивает введенный хеш-образ с образцом, хранящимся в ИС для этого пользователя и в случае их совпадения разрешает доступ. Т.о. система не хранит паролей, что повышает ее защищенность (**достоинство**).

Недостаток приведенной схемы заключается в том, что все равно необходимо как-то передавать хеш-образ для хранения в системе или для аутентификации и на этом пути его может перехватить злоумышленник, а затем воспользоваться им.

13.4. Протокол идентификации/аутентификации на основе шифрования с открытым ключом

Широкое распространение при идентификации и аутентификации получили протоколы на базе асимметричного шифрования. Существует десятки разновидностей таких протоколов, наиболее известными из которых являются протоколы на основе алгоритмов RSA, схемы Фейге-Фиата-Шамира, Эль-Гамала, Шнорра и т.д.

Протокол на основе алгоритма RSA.

Этап 1. Генерация ключей.

1. **A** генерирует открытый и закрытый ключи ($e=5$, $n=91$) и $d=29$).
2. **A** передает открытый ключ **B**.

Этап 2. Аутентификация.

Таблица 13.1. Аутентификация на основе алгоритма RSA

№ п/п	Описание операции	Пример
1	B выбирает случайное число $k \in \{1, \dots, n-1\}$, вычисляет $r = k^e \bmod n$ и посылает r A .	$k = 23$ $r = 23^5 \bmod 91 = 4$
2	A вычисляет $k' = r^d \bmod n$ и посылает k' B .	$k' = 4^{29} \bmod 91 = 23$
3	B проверяет соотношение $k = k'$ и, если оно истинно, принимает доказательство, в противном случае - отвергает.	$k = 23$ $k' = 23$

Схема Клауса Шнорра.

Этап 1. Генерация ключей (выполняет **A**).

Таблица 13.2. Генерация ключей по схеме Клауса Шнорра

№ п/п	Описание операции	Пример
1	Выбираются два простых числа p и q такие, что $(p-1) \bmod q \neq 0$.	$p = 23$, $q = 11$
2	Выбирается секретный ключ $x \in \{1, \dots, q-1\}$.	$x = 8$
3	Выбирается g такое, что $g^q \bmod p = 1$.	$g=3$ $3^{11} \bmod 23 = 1$
4	Вычисляется открытый ключ y такой, что $(g^x * y) \bmod p = 1$.	$y = 4$ $(3^8 * 4) \bmod 23 = 26244 \bmod 23 = 1$
5	Публикация открытого ключа y .	

Этап 2. Аутентификация.

Таблица 13.3. Аутентификация по схеме Клауса Шнорра

№ п/п	Описание операции	Пример
1	A выбирает случайное число $k \in \{1, \dots, q-1\}$, вычисляет $r = g^k \bmod p$ и посылает r B .	$k = 6$ $r = 3^6 \bmod 23 = 16$
2	B выбирает случайное число $e \in \{0, \dots, 2^t-1\}$, где t - некоторый параметр, и посылает e A .	$e = 4$
3	A вычисляет $s = (k + x * e) \bmod q$ и посылает s B .	$s = (6 + 8 * 4) \bmod 11 = 5$
4	B проверяет соотношение $r = (g^s * y^e) \bmod p$ и, если оно выполняется, принимает доказательство, в противном случае - отвергает.	$16 = (3^5 * 4^4) \bmod 23$

Для обеспечения стойкости протокола в 1989 г. Шнорр рекомендовал использовать **p** длиной 512 бит, **q** длиной 140 бит и $t = 52$.

Схема на основе протокола с нулевым разглашением.

Суть доказательства с нулевым разглашением очень популярно можно объяснить на примере «пещеры Аладдина» (авторы - Жан-Жак Кискатер и Луи Гийу).

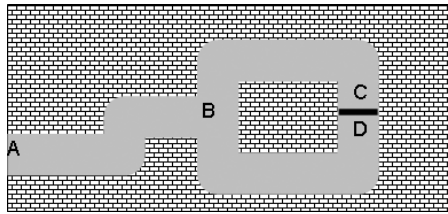


Рис.13.1. Пещера Аладдина

В пещере имеется потайная дверь **C-D**, открыть которую может только тот, кто знает волшебные слова. Алиса хочет доказать Бобу, что знает волшебные слова, но не хочет их раскрыть Бобу. Тогда Алиса может убедить Боба следующим образом.

1. Боб стоит в точке **A**.
2. Алиса проходит к точке **C** или **D**.
3. Боб проходит к точке **B** и предлагает Алисе появиться с левого прохода или с правого.
4. Алиса выполняет просьбу, используя, если необходимо, волшебные слова.
5. Алиса и Боб **n** раз повторяют шаги 1-4.

Если Алиса не знает секрета, то вероятность правильно выйти у нее в каждом раунде 50%:50%. Если шаги повторить **t** раз, то вероятность правильного выхода во всех случаях 1 шанс на 2^t . Например, при $t=16$ у Алисы всего 1 шанс из 65536.

Практическая реализация протокола рассматривается на примере схемы аутентификации Фейге-Фиата-Шамира.

Упрощенная схема аутентификации Фейге-Фиата-Шамира.

Этап 1. Генерация ключей (выполняет Посредник).

Таблица 13.4. Генерация ключей по схеме Фейге-Фиата-Шамира

№ п/п	Описание операции	Пример
1	Выбирает модуль n , равный произведению двух простых чисел.	$p = 5, q = 7, n = 35$
2	Выбирает число v (открытый ключ), являющееся квадратичным вычетом по модулю n и имеется обратное значение v^{-1} по модулю n . Квадратичный вычет – число, удовлетворяющее выражению $x^2 \bmod n = v$, где $1 \leq x \leq n$. Для модуля $n = 35$, квадратичными вычетами являются 1 ($x = 1, 6, 29, 34$), 4, 9, 11, 14, 15, 16, 21, 25, 29, 30. Обратное значение вычисляется по формуле $(v * v^{-1}) \bmod n = 1$. У квадратичных вычетов 14, 15, 21, 25 и 30 нет обратных значений по модулю. Таким образом, $v \in \{1, 4, 9, 11, 16, 29\}$.	$v = 16$ $v^{-1} = 11$ $(16 * 11) \bmod 35 = 176 \bmod 35 = 1$
3	Определяет закрытый ключ s - наименьшее значение, удовлетворяющее выражению $s^2 \bmod n = v^{-1}$.	$s = 9$ $9^2 \bmod 35 = 11$
4	Публикация открытого ключа – v и n . Передача закрытого ключа s A .	

Этап 2. Аутентификация.

Таблица 13.5. Аутентификация по схеме Фейге-Фиата-Шамира

№ п/п	Описание операции	Пример	
1	A выбирает случайное число $r \in \{1, \dots, n-1\}$, вычисляет $z = r^2 \bmod n$ и посылает z B .	$r = 8$ $z = 8^2 \bmod 35 = 29$	
2	B посылает A случайный бит b .	$b = 0$	$b = 1$
3	Если $b=0$, то A посылает B r , иначе $y = (r * s) \bmod n$.	$r = 8$	$y = (8 * 9) \bmod 35 = 2$
4	Если $b=0$, то B проверяет, что $z = r^2 \bmod n$, иначе $z = (y^2 * v) \bmod n$.	$29 = 8^2 \bmod 35$	$29 = (2^2 * 16) \bmod 35$

Рассмотренный порядок операций, выполненный 1 раз называется **аккредитацией**. Если первую операцию поменять местами со второй, то **A**, даже не зная закрытого ключа **s**, может подобрать такое значение **r**, которое будет приводить к успешной аккредитации в обоих случаях ($b=0$ и $b=1$). Подобрать же такое **r**, которое будет приводить к успешной аккредитации в обоих случаях одновременно невозможно. Таким образом, если **A** не знает закрытого ключа **s**, то вероятность успешной аккредитации (подбора **r**) равна $1/2$. Аккредитация повторится **t** раз, пока не будет достигнута требуемая вероятность $1/2^t$, что **A** не знает закрытого ключа **s**.

13.5. Сервер аутентификации Kerberos

Kerberos¹ – программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных ОС.

Kerberos предназначен для решения следующей задачи. Имеется открытая (незащищенная) сеть, в узлах которой сосредоточены субъекты – пользователи, а также клиентские и серверные программные компоненты. Каждый субъект обладает секретным ключом. Чтобы субъект **C** мог доказать свою подлинность субъекту **S** (без этого **S** не станет обслуживать **C**), он должен не только назвать себя, но и продемонстрировать знание секретного ключа. **C** не может просто послать **S** свой секретный ключ, во-первых, потому, что сеть открыта (доступна для пассивного и активного прослушивания), а, во-вторых, потому, что **S** не знает (и не должен знать) секретный ключ **C**. Требуется менее прямой способ демонстрации знания секретного ключа.

Система Kerberos представляет собой доверенную третью сторону (т.е. сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в парной проверке подлинности.

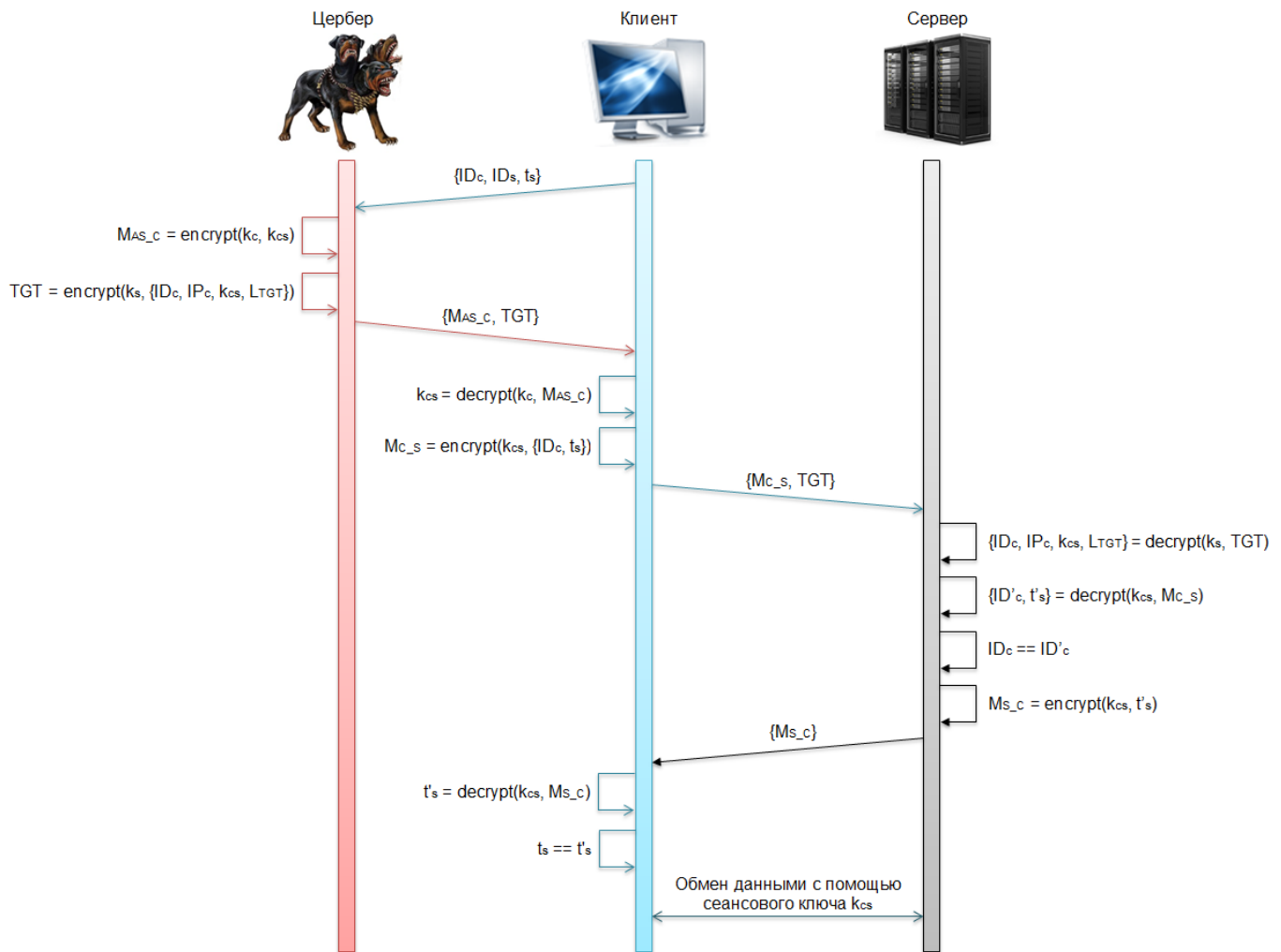


Рис.13.2. Проверка сервером S подлинности клиента C

Упрощенно последовательность идентификации/аутентификации с помощью Kerberos версии 5.0 на основе спецификации RFC 1510 ["Request for Comments: 1510. The Kerberos Network Authentication Service (V5)" - "Запрос для комментариев: 1510. Сетевой сервис аутентификации Kerberos"] выглядит следующим образом.

- (1) Клиент посылает Kerberos запрос, содержащий свой идентификатор ID_c и идентификатор сервера (запрашиваемой услуги) ID_s , а также метку времени t_s .
- (2) Kerberos:
 - по метке времени t_s проверяет синхронизацию своих часов с часами клиента;
 - формирует сообщение M_{AS_c} - зашифровывает сеансовый ключ k_{cs} ключом клиента k_c ;
 - формирует билет TGT - зашифровывает идентификатор клиента ID_c , его IP-адрес IP_c , сеансовый ключ k_{cs} и время жизни билета (сеансового ключа) L_{TGT} ключом сервера k_s ;
 - отправляет сообщение M_{AS_c} и билет TGT клиенту.
- (3) Клиент:
 - расшифровывает сообщение M_{AS_c} с помощью своего ключа k_c для получения сеансового ключа k_{cs} ;
 - формирует сообщение M_{c_s} - зашифровывает свой идентификатор ID_c и метку времени t_s сеансовым ключом k_{cs} ;
 - отправляет сообщение M_{c_s} и билет TGT серверу.
- (4) Сервер:
 - расшифровывает билет TGT с помощью своего ключа k_s для получения идентификатора клиента ID_c , его IP-адреса IP_c , сеансового ключа k_{cs} и времени жизни билета L_{TGT} ;
 - расшифровывает сообщение M_{c_s} с помощью сеансового ключа k_{cs} для получения идентификатора клиента ID'_c и метки времени t'_s ;
 - для аутентификации клиента выполняет сравнение идентификаторов ID_c и ID'_c , полученных, соответственно, из билета TGT и сообщения M_{c_s} ;
 - формирует сообщение M_{s_c} - зашифровывает метку времени t'_s сеансовым ключом k_{cs} ;
 - отправляет сообщение M_{s_c} клиенту.
- (5) Клиент:
 - расшифровывает сообщение M_{s_c} с помощью сеансового ключа k_{cs} для получения метки времени t'_s ;
 - для аутентификации сервера выполняет сравнение меток времени t_s и t'_s .
- (6) Обмен данными между клиентом и сервером выполняется с помощью сеансового ключа k_{cs} в течение времени жизни билета (сеансового ключа) L_{TGT} .

Как видно из данного протокола, помимо идентификации/аутентификации, параллельно решается вопрос с обменом сеансовым ключом. Согласно RFC 1510 все ключи, включая сеансовый, используются для симметричного шифрования (в частности DES). В RFC 1510 рассмотрены дополнительные детали: применение хеширования для контроля целостности (в частности MD4 или MD5), сообщения в случае ошибочных действий сторон и т.д. В отдельных спецификациях рассмотрены расширения для Kerberos:

- RFC 3962 ["Request for Comments: 3962. Advanced Encryption Standard (AES) Encryption for Kerberos 5" - "Запрос для комментариев: 3962. Расширенный стандарт шифрования для Kerberos 5"] - применение современного стандарта США симметричного шифрования AES;

- RFC 4556 ["Request for Comments: 4556. Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)" - "Запрос для комментариев: 4556. Шифрование с открытым ключом для предварительной аутентификации в Kerberos (PKINIT)"] - применение асимметричного шифрования (в частности RSA) для предварительной аутентификации клиента перед Kerberos;

- и др.

¹ **Kerberos** (от др.-греч. Κέρβερος – Цербер или Кербер) – в греческой мифологии порождение Тифона и Ехидны (Тартара и Геи), трёхголовый пёс, у которого из пастьей течёт ядовитая смесь. Цербер охранял выход из царства мёртвых Аида, не позволяя умершим возвращаться в мир живых.

13.6. Идентификация/аутентификация с помощью биометрических данных

Биометрия – древнейший способ идентификации. Собаки различают друг друга по лаю, кошки – по запаху, люди – по лицам, голосу, подписи и т.д. [18, 28]

В общем виде в ИС работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается БД характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в БД.

В дальнейшем для идентификации и аутентификации пользователя процесс снятия и обработки повторяется, после чего производится поиск в БД шаблонов (верификация). В случае успешного поиска личность пользователя и ее подлинность считаются установленными.

Классификация наиболее распространенных биометрических характеристик представлена на следующем рисунке.

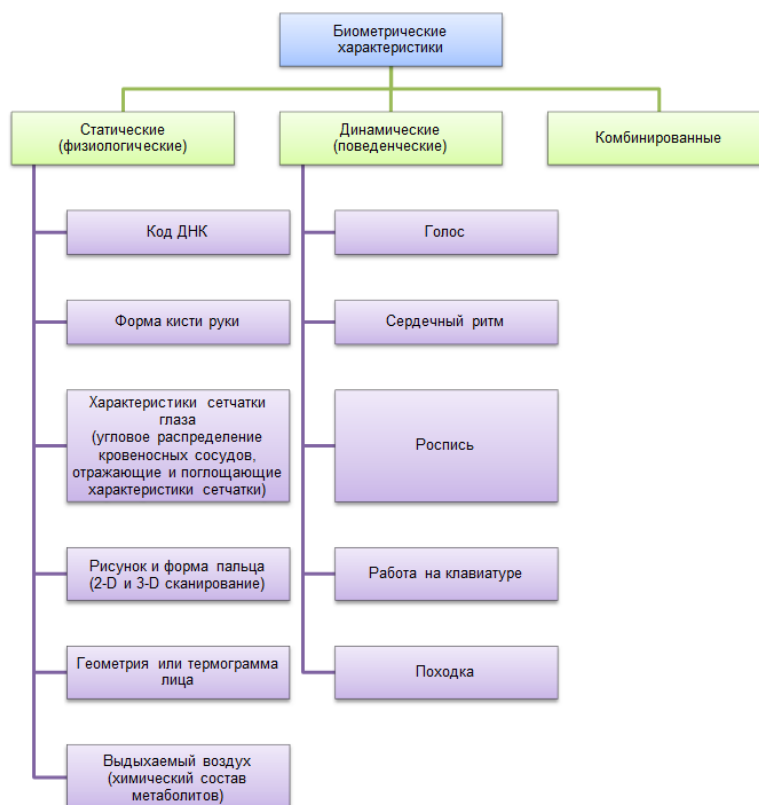


Рис.13.3. Классификация биометрических характеристик

Активность в области биометрии в настоящий момент очень велика. Организован соответствующий консорциум (www.biometrics.org), активно ведутся работы по стандартизации разных аспектов технологии (формата обмена данными, прикладного программного интерфейса (API) и т.п.), публикуется масса рекламных статей, в которых биометрия преподносится как средство обеспечения сверхбезопасности, ставшее доступным широкой массам.

В то же время **недостатки** биометрических средств отмечаются во многих исследованиях:

- биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути может много чего произойти;
- база шаблонов может быть изменена злоумышленником;
- следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в «полевых» условиях, когда, например, к устройству сканирования могут поднести муляж и т.п.;
- некоторые биометрические данные человека меняются (как в результате старения, так и травм, ожогов, порезов, болезни, ампутации и т.д.), так что база шаблонов нуждается в постоянном сопровождении, а это создает определенные проблемы и для пользователей, и для администраторов;
- если у Вас крадут биометрические данные или их компрометируют, то это, как правило, на всю жизнь. Пароли, при всей их ненадежности, в крайнем случае можно сменить. Палец, глаз или голос сменить нельзя, по крайней мере быстро;
- биометрические характеристики являются уникальными идентификаторами, но их нельзя сохранить в секрете [8].

До 11 сентября 2001 г., биометрические системы обеспечения безопасности использовались только для защиты государственных секретов и самой важной коммерческой информации. После потрясения весь мир террористического акта ситуация резко изменилась. Сначала биометрическими системами доступа оборудовали аэропорты, крупные торговые центры и другие места скопления народа. Повышенный спрос спровоцировал исследования в этой области, что, в свою очередь, привело к появлению новых устройств и целых технологий. Естественно, увеличение рынка биометрических устройств привело к увеличению числа компаний, занимающихся ими, создавшаяся конкуренция послужила причиной к весьма значительному уменьшению цены на биометрические системы обеспечения информационной безопасности.

В рамках безвизовой программы Visa Waiver США подписали с 27 странами соглашение, по которому граждане этих государств смогут въезжать на территорию США сроком до 90 дней без визы при обязательном наличии биометрических паспортов. Начало действия программы - 26 октября 2005 г. Среди государств, участвующих в программе - Австралия, Австрия, Бельгия, Великобритания, Германия, Италия, Лихтенштейн, Люксембург, Монако, Нидерланды, Португалия, Сингапур, Финляндия, Франция, Швейцария, Швеция и Япония. В 2002 г. 118 стран мира

(на текущий момент более 200) подписали Новоеорлеанское соглашение, признавшее биометрию лица основной технологией идентификации для паспортов и въездных виз следующего поколения.

Стандарты на машиночитываемые проездные документы (МСПД), к которым относятся и биометрические загранпаспорта граждан РФ, разрабатываются Международной организацией гражданской авиации (англ., International Civil Aviation Organization - ICAO). Скачать стандарты «Doc Series 9303. Machine Readable Travel Documents» можно на сайте организации по адресу www.icao.int/publications/pages/publication.aspx?docnum=9303.

Первый биометрический загранпаспорт на территории РФ был выдан 22 мая 2006 г. Это нововведение было ориентировано, в первую очередь, на повышение доверия к документам российских граждан со стороны зарубежных государств, а также для упрощения международных поездок. В России с 2009 г. во всех субъектах РФ действуют пункты выдачи паспортно-визовых документов нового поколения. В пластиковую страницу загранпаспорта встроена бесконтактная пассивная карта RFID (англ. Radio Frequency IDentification - радиочастотная идентификация) ближнего радиуса действия (до 10 см), соответствующая типу A или B стандарта ISO/IEC 14443 «Identification cards. Contactless integrated circuit(s) cards. Proximity cards» (ГОСТ Р ИСО/МЭК 14443 «Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты ближнего действия»). Данные на карте защищены с помощью технологии контроля доступа ВАС (Basic access control), которая позволяет произвести чтение данных только после ввода номера паспорта, даты рождения владельца и даты окончания действия паспорта (обычно осуществляется с помощью распознавания машиночитываемой зоны паспорта), что исключает несанкционированный доступ к данным на карте. Логическая структура данных (англ. Logical Data Structure - LDS), хранящихся на карте представлена на следующем рисунке.

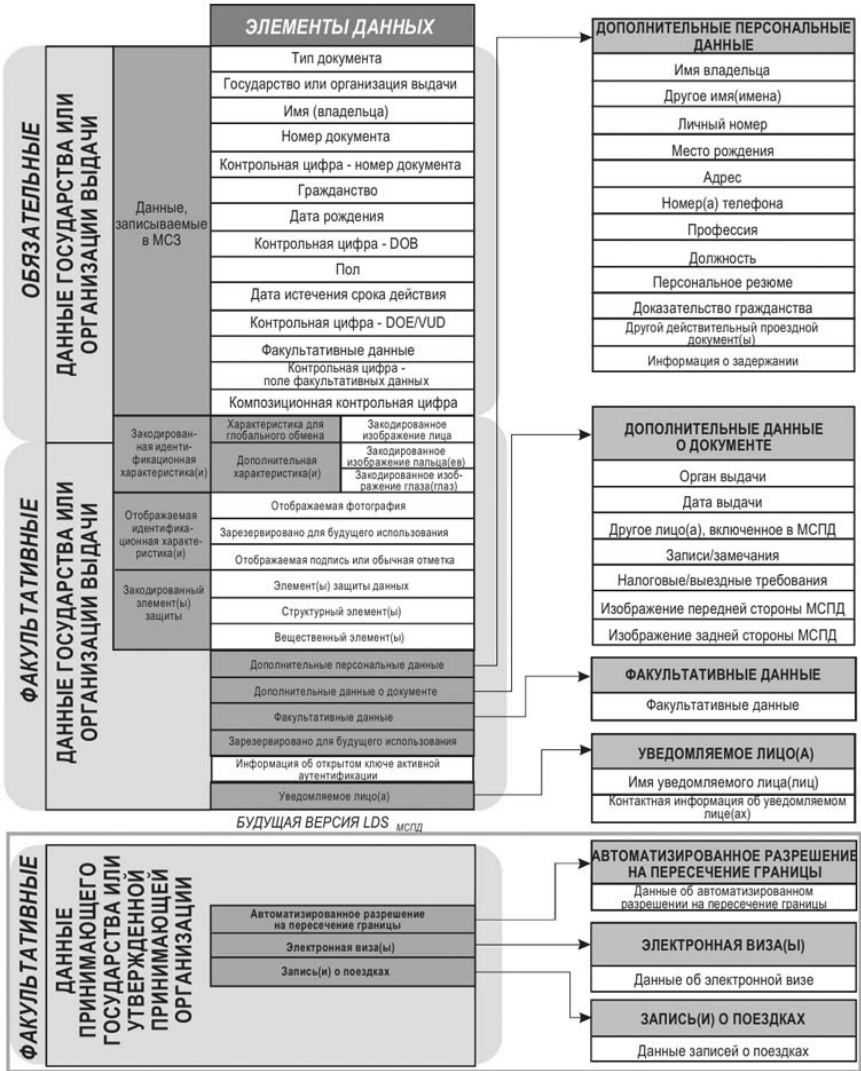


Рис.13.4. Обязательные и факультативные элементы данных МСПД

Текущий стандарт на МСПД определяют три способа биометрической идентификации - по изображению лица, пальцев и радужной оболочки глаз. При этом обязательным является только изображение лица. На карте российского загранпаспорта содержатся данные следующих групп (англ. Data Group - DG):

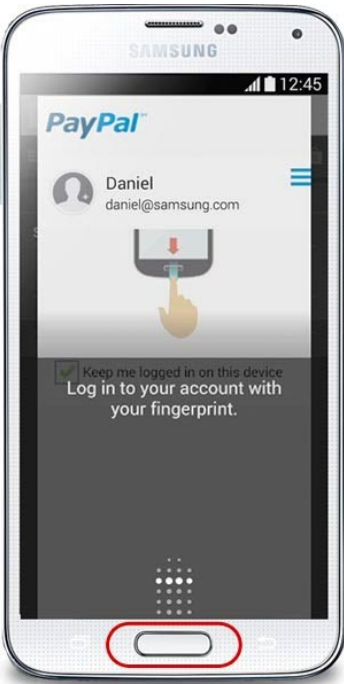
- DG1 - данные, записываемые в машиночитываемую зону;
- DG2 - закодированное изображение лица;
- DG11 - дополнительные персональные данные (дата и место рождения);
- DG12 - дополнительные данные о документе (дата выдачи паспорта и орган, выдающий документ).

В некоторых странах, помимо изображения лица, на карте в обязательном порядке (согласно местному законодательству) хранится дополнительная биометрическая информация (в частности в Латвии, Молдавии и Эстонии - отпечатки пальцев).

В настоящий момент биометрические средства находят широкое применение и в устройствах личного пользования. В частности ведущие производители сотовых телефонов в 2013-2014 гг. выпустили модели со сканерами отпечатков пальцев.

Таблица 13.6. Сотовые телефоны со сканерами отпечатков пальцев

Наименование модели	iPhone 6	HTC One max	Samsung Galaxy S5

Положение сканера (выделен красной областью)			
Функции	1) Разблокирование телефона; 2) Покупки в iTunes и App Store; 3) API для встраивания биометрической идентификации в приложения.	1) Разблокирование телефона.	1) Разблокирование телефона; 2) Покупки в Samsung Apps; 3) Покупки с помощью системы электронных платежей PayPal.

На сайте Apple (<http://www.apple.com/ru/iphone-6/touch-id/>) приведено краткое описание технологии Touch ID, используемой ею в своих мобильных устройствах: «Под поверхностью кнопки «Домой» расположена целая технологическая система. Окружающее кнопку кольцо из нержавеющей стали реагирует на прикосновение и активирует ёмкостный сенсор. Вырезанная лазером из сапфирового стекла поверхность кнопки передаёт изображение пальца на сенсор, который распознаёт его рисунок, позволяя получить детальный отпечаток. Затем программное обеспечение считывает ваш отпечаток и находит соответствие, позволяя разблокировать телефон».

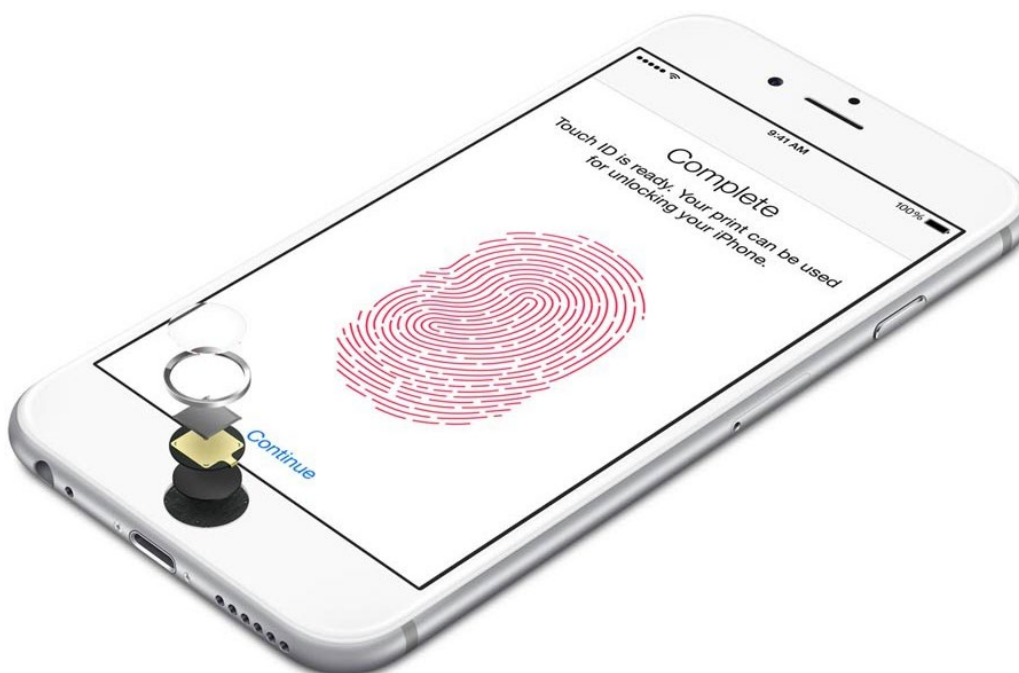


Рис.13.5. Сканер отпечатков пальцев iPhone 6 (iPhone 5s).

13.7. Идентификационные карты и электронные ключи

13.7.1. Общие сведения

История персональной идентификации, в частности идентификационных карт (ID-cards), стара и по большей части весьма неприглядна. Еще в Римской империи более 2 тыс. лет назад использовались таблички, так называемые тессера (tesserae), которые должны были иметь при себе граждане, солдаты и рабы. У каждого была своя уникальная табличка. Рабам, правда, чаще выжигали тавро. Карточки вводились и в странах, участвующих в больших войнах, — как дешевое и эффективное средство учета и распределения людских и материальных ресурсов. В Южной Африке во времена апартеида карточки использовались для сегрегации² жителей [29].

Если в ретроспективе материальным носителем идентификатора чаще всего являлся бумажный документ, то сейчас речь идет главным образом об электронных носителях информации, имеющих тот или иной механизм хранения (и, возможно, обработки) персональных данных. Этим механизмом могут быть пластиковые карты с магнитными полосами, смарт-карты, USB-ключи, RFID-метки и т.п. В настоящее время карты (схемы, документы) персональной идентификации в разных формах применяются в более чем ста странах.

Решающим признаком того, наличия или отсутствия в стране системы персональной идентификации, является, по-видимому, следующее обстоятельство: если госслужащий может потребовать от частного лица предъявить некий символ (пластиковую карточку, бумажку и т.п.), на основании которого немедленно будут сделаны выводы относительно качеств этой персоны, система идентификации существует. Если у человека такого символа нет (не важно, по какой причине), то он может быть задержан (ограничен в свободе) до выяснения обстоятельств.

Помимо учета граждан на государственном уровне, персональная идентификация с использованием карт и ключей нашла широкое применение в СКУД (Системах Контроля и Управления Доступом) организаций, а также в финансовой сфере при оплате товаров и услуг.

В настоящее время наиболее распространенными разновидностями карт и ключей являются:

- карты с магнитной полосой;
- контактные смарт-карты и USB-ключи;
- бесконтактные RFID-карты.

² **Сегрегация** (позднелат. segregatio — отделение) — политика принудительного отделения какой-либо группы населения (обычно упоминается как одна из форм религиозной и расовой дискриминации).

13.7.2. Карты с магнитной полосой

История.

История создания пластиковых карт с магнитной полосой началась в 1960 г., когда ЦРУ поручило IBM создать автоматизированную компьютерную систему контроля доступа своих сотрудников на подведомственных объектах. Инженеру IBM Форресту Перри (Forrest Parry) пришла идея наклеить кусочек магнитной ленты из ленточного накопителя на пластиковую карту. Он перепробовал несколько десятков разновидностей клея, но результаты оказались неутешительными. Полоски ленты деформировались или их характеристики ухудшались из-за действия клея, делая непригодными к использованию. После очередного дня разочарований Форрест пришел домой и рассказал о своей проблеме жене Дороти, которая в это время гладила его рубашки. Смышленая Дороти попросила его принести образцы карты и магнитной ленты. На следующий день, проделав некоторые манипуляции по настройке утюга, им удалось впрессовать ленту в пластик, достигнув достаточно высокой степени сцепления между материалами.



Рис.13.6. Один первых прототипов карты с магнитной полосой на картонной основе

Первая пластиковая карта с магнитной полосой была выпущена в 1970 г. в рамках совместного проекта IBM, American Express и American Airlines для оплаты авиабилетов.

Стандарты и спецификации.

Формат записи данных на карты для финансовых операций определяется стандартами ISO/IEC 7811 «Карты идентификационные. Способ записи», ISO/IEC 7813 «Информационные технологии. Карты идентификационные. Карты финансовых операций» и ISO/IEC 4909 «Карты банковские. Карты для финансовых операций. Содержание данных на магнитной полосе для 3-й дорожки».

	Кодировка символов	Максимальное количество символов	Плотность записи
Дорожка 1	7 бит (буквы, цифры и служебные символы)	79	210 bpi
промежуток			
Дорожка 2	5 бит (цифры и служебные символы)	40	75 bpi
промежуток			
Дорожка 3	5 бит (цифры и служебные символы)	107	210 bpi

Рис.13.7. Структура магнитной полосы на пластиковых картах

Кодирование символов выполняется с учетом контроля целостности. Последний бит каждого символа является четным паритетным битом.

Исторически первая дорожка была предназначена для банковских карт, и до конца прошлого века большинство карт имело только одну эту дорожку. Вторая дорожка задействована для хранения исключительно числовых данных, за счет чего она имеет меньшую длину и меньше шансов повреждения данных. Третья дорожка в банковской сфере не используется и предназначена карт прочих систем (например, дисконтные карты). Формат записи данных для первой и второй дорожки банковских карт представлен на следующем рисунке.

%	B	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	^	P	U	P	K	I	N	/	V	A	S	I	L	I	Y	^	1	5	1	2	2	0	1	1	0	9	7	5	7	5	4	?	0																																																			
Начало	Код формата (B – Bank / financial)	PAN - Primary Account Number Максимум 19 цифр																Разделитель	Фамилия и имя владельца Максимум 26 символов																Разделитель	Срок действия карты в формате ГГММ																Служебные коды																PVKI - PIN Verification Key Index PWV - PIN Verification Value или IBM 3624-offset CWW - Card Verification Value Discretionary data Максимум 21 цифра																Конец	LRC - Longitudinal Redundancy Check															

Рис.13.8

Discretionary data (дискреционные данные) – данные зарезервированные для карточного эмитента³ и используемые им по своему усмотрению. Тем не менее, первые 8 символов этого поля стандартизованы и предназначены для подтверждения правильности введенного PIN-кода⁴, выявления ситуаций повреждения магнитной полосы или грубой подделки карты.

PVV (значение проверки PIN-кода) и **IBM 3624-offset** представляют собой зашифрованное значение PIN-кода . В частности, алгоритм **VISA PVV** представляет собой следующую последовательность операций.

CVV (значение проверки подлинности карты) определяется по тому же алгоритму, что и **PVV**, только шифруемая строка (аналог TSP) формируется из следующих данных: 10 цифр PAN (за исключением крайней правой цифры) плюс срок действия карты (в формате ММГГ) плюс служебные коды (для приведенного выше примера, шифруемая строка – 789012344 1215 2010). Из-за того, что **CVV/CVC** слабо защищены от клонирования, в настоящее время он практически не используется и вместо него на картах ставятся нули.

На обратной стороне карты печатается код **CVV2**.

Рис. 13.9. CVV2

Генерация кода CVV2 осуществляется по тому же алгоритму и с использованием тех же ключей, что и обычного CVV. При этом есть следующие особенности шифруемой строки: срок действия карты берется в формате ГГММ, а вместо служебных кодов указываются нули (для приведенного выше примера, шифруемая строка – 789012344 1512 000₁₀).

Таблица 13.7. Коды проверки подлинности карты

VISA	CVV - Card Verification Value	CVV2 - Card Verification Value 2
MasterCard	CVC - Card Verification Code	CVC2 - Card Verification Code 2
American Express	CSC - Card Security Code	CID - Card Identification Number*
Discover	CVV - Card Verification Value	CID - Card Identification Number
JBC - Japan Credit Bureau (Японское кредитное бюро)	CAV - Card Authentication Value	CAV2 - Card Authentication Value 2

* Код CID карт American Express состоит из четырех цифр и печатается на лицевой стороне карты.

Сферы применения.

Карты с магнитной полосой нашли широкое применение в общественной жизни. Среди них можно отметить карты:

- банковские;
- социальные;
- подарочные;
- дисконтные;
- телефонные;
- проездные;
- визитные (клубные);
- развлекательных центров;
- и т.д.

³ **Эмитент** (англ. issuer) — орган исполнительной власти, местного самоуправления или юридическое лицо, которому в установленном порядке и на определенных условиях предоставлено право эмиссии (выпуска в обращение) денег, ценных бумаг и других финансово-платежных инструментов.

⁴ **PIN-код** (англ. Personal Identification Number) — персональный идентификационный номер.

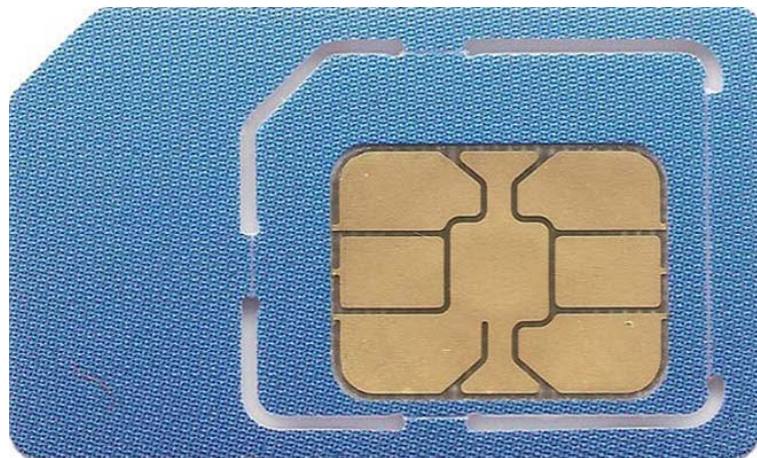
13.7.3. Контактные смарт-карты и USB-ключи

История.

Первая смарт-карта (карта со встроенной микросхемой, англ. integrated circuit card, ICC - карта с интегрированными электронными цепями) была выпущена в 1983 г. во Франции и использовалась для оплаты телефонных счетов (France Telecom). В 1991 г. немецкой компанией Giesecke & Devrient были выпущены первые SIM-карты⁵ (разновидность смарт-карты) для телефонов стандарта GSM⁶. В банковской сфере смарт-карта впервые стала использоваться во французской платежной системе Carte Bleue (русс. «Голубая карта») в 1992 г.



а) банковская карта



б) SIM-карта

Рис.13.10. Контактные смарт-карты

В большинстве случаев смарт-карты, помимо модуля памяти, содержат также микропроцессор и операционную систему. Назначение смарт-карт - одно- и двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде.

Отцом смарт-карты принято считать французского изобретателя Ролана Морено. Его первоначальная патентная заявка предполагала использование микросхемы в перстне, но уже в 1975 г. был подан патент (Data-transfer system, US 4007355) на систему передачи данных (например, при кассовых операциях), в которой портативное устройство с микросхемой памяти предполагалось изготавливать в виде плоской карты. В 1976 г. он продемонстрировал совместную работу считывающего устройства и смарт-карты для проведения финансовых операций. Будучи поклонником фильмов Вуди Аллена, свой проект он назвал кодовым именем TMR – аббревиатура фильма «Take the Money and Run» (русс. «Бери деньги и беги»).

В некоторых источниках отцами смарт-карты называют немецких изобретателей Гельмута Гретттрупа и Юргена Деслофа, но в поданном ими в 1968 г. патенте на идентификационный переключатель (Identification switch, US 3678250 / DE 1945777) трудно уловить сходство с современными смарт-картами. А вот в патенте 1970 г. на идентификационную систему (Identification system, US 3641316) речь действительно идет о плоских картах с интегральными схемами. В 1976 г. Юрген Деслоф подал патент на защищенную идентификационную систему (Identification system safeguarded against misuse, US 4105156), предусматривающую наличие на смарт-карте, помимо модуля памяти, еще и микропроцессора.

Различают **контактные** и **бесконтактные** (работающие на некотором расстоянии от считывающего устройства) смарт-карты.

Наиболее распространенными смарт-картами являются следующие:

- контактные смарт-карты с интерфейсом ISO 7816;
- контактные смарт-карты с USB-интерфейсом;
- бесконтактные (RFID) смарт-карты.

1. Контактные смарт-карты с интерфейсом ISO 7816.

Стандарты и спецификации.

Физические параметры смарт-карт, расположение и назначение контактов, протокол обмена, механизм действия команд и т.д. описывается стандартом ISO/IEC 7816 «Карты идентификационные. Карты на интегральных схемах с контактами».

Расположение и назначение контактов приведены во 2-ой части стандарта.

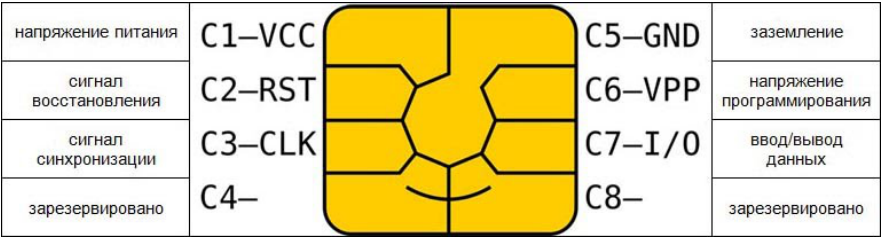


Рис.13.11

В 6-ой части стандарта определяются элементы данных (англ. Data element - DE), которые могут храниться на смарт-карте в виде информационных объектов (англ. Data object - DO) и использованы для обмена данными. Под **элементом данных** подразумевается смысловое (содержательное) описание единицы информации, для которого определены наименование, описание логического содержания, формат и кодирование. **Информационный объект** – информация, состоящая из тега, длины и значения. Тег DO однозначно определяет (идентифицирует) элемент данных.

Различают **простой** и **составной** DO. Например:

- простой DO – «дата истечения срока действия карты» в формате «ГГММ», тег «5916», длина 2 байта;
- составной DO – «имя», тег «5B16», максимальная длина 39 байт. Включает в себя элементы данных:
 - фамилия;
 - имя (имена);
 - уточняющее дополнение к имени (например, младший, номер и т.п.);
 - символ-заполнитель.

На смарт-карте могут содержаться DO различного назначения. Некоторые из них приведены в следующей таблице.

Таблица 13.8. Некоторые теги для смарт-карт стандарта ISO 7816

Тег (hex)	Наименование элемента данных	Примечания
Персональные (идентификационные) данные		
5B	Имя	Имя физического лица
5F2B	Дата рождения	Дата рождения физического лица
5F35	Пол	Пол физического лица
5F42	Адрес	Адрес физического лица
5F2C	Гражданство держателя карты	Держатель карты – владелец счета, к которому привязана карта
Данные для аутентификации		
5F2F	Стратегия использования PIN-кода	Определяет необходимость запроса терминалом введения PIN-кода и при каких условиях
5F3C	Динамическая взаимная аутентификация	Составной DO, используемый для идентификации алгоритма и ключа, которые должны использоваться в процессе взаимной аутентификации
5F3B	Динамическая внешняя аутентификация	Составной DO, используемый для идентификации алгоритма и ключа, которые должны использоваться в команде ВЫПОЛНИТЬ ВНЕШНЮЮ АУТЕНТИФИКАЦИЮ
5F3A	Динамическая внутренняя аутентификация	Составной DO, используемый для идентификации алгоритма и ключа, которые должны использоваться в команде ВЫПОЛНИТЬ ВНУТРЕННЮЮ АУТЕНТИФИКАЦИЮ
6C	Образцы держателя карты	Составной тег, содержащий, по меньшей мере, один из трех DO, указанных ниже
5F2E	Биометрические данные держателя карты	Отпечатки пальцев, ладоней, характеристики голоса, динамические характеристики подписи и т.д.
5F40	Портретное изображение держателя карты	
5F43	Изображение рукописной подписи держателя карты	
Данные для использования ЭЦП		
7F21	Сертификат держателя карты	Составной DO, содержащий открытый ключ держателя карты, дополнительную информацию, подпись органа по сертификации
5F49	Открытый ключ держателя карты	Содержит открытый ключ держателя карты для ЭЦП, использующей асимметричные механизмы
5F48	Секретный ключ держателя карты	Содержит секретный ключ держателя карты для ЭЦП, использующей асимметричные механизмы
5F4A	Открытый ключ органа по сертификации	Содержит открытый ключ органа по сертификации для ЭЦП, используемой для подтверждения подлинности сертификата
Дополнительные данные		
45	Данные эмитента	По ISO/IEC 7816-4
5F34	Порядковый номер карты	
55A	Первичный идентификатор счета (PAN)	
5F28	Код страны	Код для представления названия страны (по ISO 3166)
5F26	Дата активации карты	Дата, начиная с которой карта может использоваться под ответственность ее эмитента
59	Дата истечения срока действия карты	Дата, после которой карта считается недействительной
43	Данные об услугах, предоставляемых картой	По ISO/IEC 7816-4
5F2A	Код валюты	Код для представления валют и денежных средств (по ISO 4217)
5F21	Дорожка 1 (карта)	Информация, закодированная на дорожке 1-ой магнитной полосы (в соответствии с ISO/IEC 7813), включая разделители полей, но исключая сигнальные метки начала и конца и символ LRC

		(при наличии на пластиковой карте магнитной полосы)
5F22	Дорожка 2 (карта)	Информация, закодированная на дорожке 2-ой магнитной полосы (в соответствии с ISO/IEC 7813), включая разделители полей, но исключая сигнальные метки начала и конца и символ LRC (при наличии на пластиковой карте магнитной полосы)

Сферы применения и реализуемые механизмы защиты.

Информационные объекты, хранящиеся на смарт-карте, могут быть использованы для обеспечения следующих механизмов защиты:

- аутентификация участвующей стороны по паролю (проверка введенного PIN-кода);
- аутентификация участвующей стороны по ключу (аутентификация с использованием шифрования с открытым ключом);
- аутентификация данных (обеспечение целостности хранимых или пересылаемых данных с использованием криптографической контрольной суммы или ЭЦП);
- шифрование данных (обеспечение конфиденциальности хранимых или пересылаемых данных).

Смарт-карты с интерфейсом ISO 7816 получили наибольшее распространение в банковской сфере (пластиковые кредитные и дебетовые карты) и мобильной телефонии (SIM-карты).

2) Контактные смарт-карты с USB-интерфейсом (USB-ключи).

Стандарты и спецификации.

Как правило, представляют собой обычную смарт-карту стандарта ISO 7816, совмещенную с микропроцессором и USB-считывателем в одном корпусе.



а) Рутокен



б) eToken

Рис.13.12. USB-ключи

Сферы применения и реализуемые механизмы защиты.

Наличие USB-порта подразумевает подключение данных устройств к компьютеру. Совместная работа USB-ключей и установленного на компьютере специального ПО позволяет решать следующие задачи:

- усовершенствовать процесс аутентификации (двухфакторная аутентификация) на локальном компьютере и в корпоративной сети, а также защищенный доступ к бизнес-приложениям;
- зашифровать данные на серверах, ноутбуках и рабочих станциях;
- обеспечить защиту персональных данных;
- защитить электронную почту и взаимодействие с коллегами в системах электронного документооборота;
- обезопасить финансовые операции в системах дистанционного банковского обслуживания (ДБО);
- внедрить ЭЦП и защитить документы в системах сдачи электронной отчетности через Интернет;
- обеспечить защиту корпоративного сайта в Интернет;
- и т.д.

В частности, рутокены российского производителя ЗАО «Актив-софт» [www.rutoken.ru] имеют следующие механизмы защиты данных:

- аутентификация:
- поддержка 3-х категорий владельцев: Администратор, Пользователь, Гость;
- поддержка 2-х Глобальных PIN-кодов: Администратора и Пользователя;
- поддержка Локальных PIN-кодов для защиты конкретных объектов (например, контейнеров сертификатов) в памяти устройства;
- настраиваемый минимальный размер PIN-кода (для любого PIN-кода настраивается независимо);
- поддержка комбинированной аутентификации: по схеме «Администратор или Пользователь» и аутентификация по Глобальным PIN-кодам в сочетании с аутентификацией по Локальным PIN-кодам;
- шифрование и ЭЦП:
- поддержка алгоритма ГОСТ 28147-89: генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ);
- поддержка алгоритмов DES (3DES), RC2, RC4, MD4, MD5, SHA-1;
- выработка сессионных ключей (ключей парной связи) по схемам VKO GOST R 34.10-2001 (RFC4357) и VKO GOST R 34.10-2012;
- генерация последовательности случайных чисел требуемой длины;

- поддержка алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001: генерация ключевых пар, формирование и проверка ЭЦП;
- поддержка алгоритмов ГОСТ Р 34.11-2012 и ГОСТ Р 34.11-94: вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭЦП;
- поддержка PKCS#11 версии 2.20 (англ. Public Key Cryptography Standards - Стандарты криптографии с открытым ключом, разработанные и опубликованные RSA Laboratories);
- поддержка алгоритма RSA с ключами до 2048 бит;
- расшифрование по схеме EC El-Gamal;
- интеграция с MS Windows посредством интерфейсов Microsoft Crypto API и Microsoft Smartcard API.

⁵ **SIM-карта** (англ. Subscriber Identification Module - модуль идентификации абонента) - идентификационный модуль абонента, применяемый в мобильной связи стандарта GSM.

⁶ **GSM** (англ. Global System for Mobile communications) - глобальный стандарт цифровой мобильной сотовой связи с разделением каналов по времени и частоте.

13.7.4. Бесконтактные RFID-карты

RFID (англ. Radio Frequency IDentification, радиочастотная идентификация) - способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах (RFID-метках, RFID-тегах) [17].

Большинство RFID-меток состоит из двух частей. Первая - интегральная схема для хранения и обработки информации, модулирования и демодулирования радиочастотного сигнала и некоторых других функций. Вторая - антенна для приема и передачи сигнала.

История [45, 17].

Принято считать, что технология радиочастотной идентификации берет свое начало с изобретения радара перед Второй мировой войны.

В 1904 г. немецкий инженер Кристиан Хюльсмейер продемонстрировал работу радиолокационного устройства для обнаружения корабля в густом тумане. Более совершенное устройство (телемобилоскоп), на которое он получил патент в 1905 г., уже позволяло определять расстояние до корабля. Одно из первых устройств, предназначенных для радиолокации воздушных объектов, продемонстрировал 26 февраля 1935 г. шотландский физик Роберт Ватсон-Ватт, который примерно за год до этого получил патент на изобретение подобной системы.

В Советском Союзе осознание необходимости средств обнаружения авиации, свободных от недостатков звукового и оптического наблюдения, привела к разворачиванию исследований в области радиолокации. Идея, предложенная молодым артиллеристом Павлом Ощепковым, получила одобрение высшего командования: наркома обороны СССР К. Е. Ворошилова и его заместителя - М. Н. Тухачевского.

3 января 1934 г. в СССР был успешно проведен эксперимент по обнаружению самолета радиолокационным методом. Самолет, летящий на высоте 150 метров, был обнаружен на дальности 600 метров от радарной установки. Эксперимент был организован представителями Ленинградского Института Электротехники и Центральной Радиолaborатории. Руководил экспериментом военный инженер М. М. Лобанов. В 1934 г. маршал Тухачевский в письме правительству СССР написал: «Опыты по обнаружению самолетов с помощью электромагнитного луча подтвердили правильность положенного в основу принципа». Первая опытная установка «Рапид» была опробована в том же году, в 1936 г. советская сантиметровая радиолокационная станция «Буря» засекла самолет с расстояния 10 километров. Первые РЛС в СССР, принятые на вооружение РККА и выпускавшиеся серийно были: РУС-1 - с 1939 г. и РУС-2 - с 1940 г.

Технология, наиболее близкая к RFID, - система распознавания «свой-чужой» (англ. Identification Friend or Foe, IFF) была изобретена Исследовательской лабораторией ВМС США в 1937 г. и активно применялась союзниками во время Второй мировой войны. В СССР первые серийные авиационные радиоответчики СЧ-1 были приняты на вооружение РККА и начали поступать в войска с начала 1943 г.

В 1945 г. советский инженер Л.С. Термен изобрел устройство, которое позволило накладывать аудиоинформацию на случайные радиоволны. Звук вызывал колебание диффузора, которое незначительно изменяло форму резонатора, модулируя отраженную радиочастотную волну. И хотя устройство представляло лишь пассивный передатчик (т.н. «жучок»), это изобретение причисляют к первым предшественникам RFID-технологии.

Развитие радарных и радиочастотных передач продолжалось в 50-е и 60-е гг. Ученые в США, Европе и Японии проводили исследования и представляли отчеты, объясняющие, как радиочастотная энергия могла быть использована для удаленной идентификации объектов.

Первый настоящий предок современных RFID-технологий (активная перезаписываемая метка) был запатентован Марио Кардулло в январе 1973 г. (Transponder apparatus and system, US 3713148 A), хотя устройство, с почти дословным сочетанием слов в аббревиатуре RFID, было запатентовано Чарльзом Уолтоном только в 1983 г. (Portable radio frequency emitting identifier - портативный радиочастотный излучающий идентификатор, US 4384288 A).

В 1970-х годах Национальная Лаборатория в Лос-Аламосе по заданию Департамента энергетики США разработала RFID-систему для отслеживания ядерных материалов (метки размещались на грузовиках, выполняющих перевозку материалов), а по заданию Департамента сельского хозяйства - для отслеживания перемещения коров и контроля получения ими лекарств (метки в стеклянной капсуле вживлялись под кожу).

Классификация RFID-систем [17]:

- по дальности считывания:
 - ближней идентификации (считывание производится на расстоянии до 20 см);
 - идентификации средней дальности (от 20 см до 5 м);
 - дальней идентификации (свыше 5 м);
- по рабочей частоте:
 - диапазона LF (англ. Low Frequency – низкая частота) - 125 .. 134 кГц;
 - диапазона HF (англ. High Frequency – высокая частота) - 13.56 МГц;
 - диапазона UHF (англ. Ultra High Frequency – ультравысокая частота) - 860 .. 960 МГц;
 - диапазона SHF (англ. Super High Frequency – сверхвысокая частота) - 2.4 ГГц;
- по типу используемой памяти:
 - RO (англ. Read Only) - идентификационные данные записываются только один раз, сразу при изготовлении;
 - WORM (англ. Write Once Read Many) - содержат идентификатор и блок однократно записываемой памяти;
 - RW (англ. Read and Write) - содержат идентификатор и блок многократно перезаписываемой памяти;
- по источнику питания:
 - пассивные. Не имеют встроенного источника питания. Электрический ток, индуцированный в антенне электромагнитным сигналом от считывателя, обеспечивает достаточную мощность для функционирования чипа, размещенного в метке, и передачи ответного сигнала. Дальность действия меток составляет 1-200 см (ВЧ-метки) и 1-10 метров (СВЧ-метки);
 - активные. Имеют собственный источник питания. Дальность действия меток до 300 м;
 - полупассивные.

Стандарты и спецификации.

Стандартизацией RFID-систем занимается несколько международных организаций. Ими разработано и опубликовано несколько десятков стандартов, в т.ч. под эгидой ISO:

- ISO 11784 «Идентификация животных радиочастотным кодом. Структура кода»;
- ISO 11785 «Идентификация животных по радиочастотным сигналам. Техническая концепция»;
- ISO 14223 «Радиочастотная идентификация животных. Современные датчики»;
- ISO 10536 «Карты идентификационные. Карты на интегральных схемах бесконтактные»;
- ISO 14443 «Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты ближнего действия»;
- ISO 15693 «Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты с радиосвязью через большой зазор»;
- DIN/ISO 69873 «Носители данных для инструмента и зажимных приспособлений»;
- ISO 17363 «Применение радиочастотной идентификации (RFID) в цепи поставок. Контейнеры грузовые»;
- VDI 4470 «Системы охраны товаров»;
- ISO 15961 «Информационные технологии. Распознавание радиочастот для управления элементом. Протокол данных: прикладной интерфейс»;
- ISO 15962 «Информационные технологии. Идентификация радиочастоты для управления элементом данных. Протокол данных: правила кодирования данных и логические функции памяти»;
- ISO 15963 «Информационные технологии. Радиочастотная идентификация для управления предметами. Уникальная идентификация радиочастотных меток»;
- ISO 18000 «Информационные технологии. Идентификация радиочастотная для управления предметами»;
- и др.

Одна из организаций, занимающаяся разработкой и продвижением RFID-технологий в различных секторах экономики является GS1 (англ. Global Standard One). В спецификации этой организации «EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID. Version 2.0.0.0» (EPC Gen2) определена структура памяти RFID-метки для продуктов (товаров), содержащая четыре раздела (банка):

- **Банк 00₂ – RESEVED**. Используется для хранения ACCESS- и KILL-паролей. После производства метки значения паролей нулевые. Их установка возможна с помощью соответствующей команды радиоинтерфейса. Если значение ACCESS-пароля (32 бита) ненулевое, то чтение/запись данных на метку возможны только при знании этого пароля. Если значение KILL-пароля (32 бита) ненулевое, то чтение/запись данных на метку невозможны (метка перестает реагировать на команды без возможности восстановления ее работы);
- **Банк 01₂ – EPC** (англ. Electronic Product Code – электронный код продукта). Используется для хранения уникального идентификатора продукта. Наиболее распространенная длина идентификатора 64 или 96 бит. В настоящий момент разрабатывается спецификация на 256 битовый EPC. В банке хранится также идентификатор протокола обмена информацией с RFID-меткой (StoredPC) и значение циклического контроля кода (StoredCRC). Последний вычисляется по полиному CRC-16-CCITT в целях контроля целостности значений StoredPC и EPC;
- **Банк 10₂ – TID** (Tag ID). Используется для хранения уникального идентификатора метки, указывающего на ее изготовителя. Значение TID в соответствии с ISO 15963 состоит из трех полей: кода категории (AC); регистрационного номера организации (изготовителя метки), присваивающей TID; серийного номера метки. Если AC = 1110000₂ (E0₁₆), тогда ID изготовителя и серийный номер устанавливаются в соответствии с ISO 1816-6, если AC = 11100010₂ (E2₁₆) – в соответствии со спецификациями GS1, ISO 18000-6 (для радиочастотных меток типа C) и ISO 18000-3 (для систем радиочастотной идентификации, работающих в режиме 3);
- **Банк 11₂ – User**. Необязательный банк, используемый для хранения произвольной информации. Может отсутствовать в конкретной модели метки.

Сферы применения.

RFID-системы нашли широкое применение в различных сферах деятельности. В следующей таблице представлены некоторые из них.

Таблица 13.9. Сферы применения RFID-меток [17]	
Сфера применения	Примеры
Промышленность	1) RFID-метка с набором конечных требований к изделию может быть помещена на раму или корпус собираемого на конвейере автомобиля и в процессе конвейерного производства на различных участках (сборка, окраска и т.п.) автомобиль может быть автоматически окрашен определённым образом, могут быть установлены другие колёсные диски, изменён цвет обивки и т.п.
	2) Оператор, имеющий карточку с RFID-меткой может управлять оборудованием в определённой локации.
Транспорт	1) В 2014 г. в Зеленограде (Московская область) начат пилотный проект по оснащению общественного и спецтранспорта RFID-метками для беспрепятственного пропуска на перекрестках, оборудованных светофорами. Светофоры оборудуют считывателями, которые смогут распознавать сигнал от RFID-меток, установленных на спецтранспорте, и максимально быстро (в течение 10-15 секунд) включать зелёный свет.
	2) В конце марта 2013 г. на общественное обсуждение был вынесен проект национального стандарта для комплексов фотовидеофиксации. Новый ГОСТ подразумевает оснащение RFID-метками регистрационных номеров машин и RFID-считывателями дорожных камер, чтобы они могли распознавать грязные номера.
	3) С помощью RFID-меток на производстве жевательных резинок Wrigley отслеживается маршрут перевозки сырья.
	4) Морские контейнерные перевозки. Каждый контейнер оснащается RFID-меткой, содержащей информацию о грузе и скомбинированной с датчиками (например, открытия, содержания кислорода и т. п.) и передающей данные на центральную станцию сбора данных на борту контейнеровоза, которая в свою очередь передаёт данные через спутниковую связь. Т.о. владелец груза получает возможность отслеживать местоположение и сохранность груза.
	5) Начиная с 2004 г., функция Smart Key/Smart Start стала доступна в Toyota Prius. С тех пор Toyota встроила эту функцию во многие другие модели брендов Toyota и Lexus. Ключ содержит активную RFID-микросхему, позволяющей машине идентифицировать его с расстояния до 1 метра от антенны. Водитель может открыть дверь и завести машину, не вынимая ключ из кармана.
	6) Ford, Honda и некоторые другие производители используют основанные на RFID ключи зажигания в качестве антиугонной системы.
Транспортные платежи	1) В Гонконге транспортные перевозки оплачиваются в основном с использованием RFID-технологии, названной Octopus Card (англ. Octopus - осьминог). Она была запущена в 1997 г. для сбора оплаты за проезд, но «выросла» до масштабов обычной платежной карты, которая может использоваться в торговых автоматах, фастфудах и супермаркетах. Карта может быть перезаряжена (добавлены наличные) в специальных автоматах или в магазинах и может быть считана на расстоянии в несколько сантиметров от считывателя.
	2) JR East в Японии ввела Suica (англ. Super Urban Intelligent Card - умная городская суперкарта) для оплаты проезда в железнодорожном транспорте в ноябре 2001 г., используя технологию FeliCa (англ. Felicity Card - карта счастья) фирмы SONY.
	3) В Самаре с 1 июля 2008 г. введена система оплаты проезда в общественном транспорте с помощью RFID-смарткарт.
Складской учет	1) Немецкий производитель подъемно-погрузочного оборудования Jungheinrich внедрил технологию RFID в систему складской навигации.
	2) Компания «Марс» запустила систему складского учета упаковок кормов для животных (Pedigree, Whiskas, Chappi) на базе RFID-технологии.
	3) В 2012 г. сеть магазинов электроники и бытовой техники Media Markt совместно с METRO Group RFID Innovation Center (Германия) внедрила пилотный проект с технологией RFID в одном из отделов в ТЦ «Золотой Вавилон Ростокино» (Москва). RFID-метки применялись для автоматизации приемки и учета товара, а также в

	торговом зале для контроля за наличием товара на полке.
Торговля	В Германии на экспериментальной площадке сети гипермаркетов METRO проводится эксперимент по внедрению радиочастотных меток во всех магазинах сети, в т.ч. и в России. Планируется, что ручные считыватели у кассиров в ближайшее время перестанут использоваться. В случае, когда товар маркирован радиочастотными метками, покупатель, набрав продукты в тележку, провозит её через своеобразный турникет на расчётно-кассовом узле. Установленные сканеры автоматически считывают по радиоканалу всю информацию о товаре, который лежит в тележке и сразу же печатается чек. Если расчёт покупатель ведет с помощью кредитной карты, то и присутствие кассира в этом случае уже не требуется.
Системы контроля и управления доступом (СКУД)	1) Идентификация и ограничение доступа на заданную территорию. 2) Учёт рабочего времени. 3) Автоматическое разблокирование эвакуационных выходов и закрывание противопожарных дверей в случае пожарной тревоги.
Медицина	1) RFID-браслеты используют для отождествления младенца с матерью. 2) Поиск ушедшего из своей палаты пациента, требующего по состоянию здоровья постоянного присмотра (например, страдающего болезнью Альцгеймера), или срочно разыскиваемого врача. 3) Немецкий концерн Siemens AG, совместно с компанией Schweizer electronic разработали RFID-чип со встроенным датчиком температуры, выдерживающий операции стерилизации и пастеризации, а также ускорение до 5000 g, развиваемое на центрифуге. Данный чип предназначен, например, для использования в банках крови. 4) RFID-метки для идентификации людей использовались после урагана Катрина (август 2005 г.) - все данные о погибших, которые собирали эксперты, записывались в метку, навешиваемую ярлыком на ногу.
Человеческие имплантаты	1) В 2004 г. Министерство юстиции Мексики имплантировало 18 своим сотрудникам VeriChip для контроля за доступом в комнаты с государственными секретами. 2) Ночные клубы в Барселоне и Роттердаме, используют имплантируемую метку для идентификации своих VIP-посетителей, которые, в свою очередь, пользуются ими для оплаты за выпивку.
Маркировка (чипирование) животных	1) Опознавание животных при помощи микрочипов применяется для упрощения их учёта, перемещения через границу, страхования, исключения подмены при разведении. Использование уникального номера позволяет отслеживать животных от фермы до потребителя, проверять своевременность обязательных вакцинаций и лечения. 2) Согласно Регламенту Европейского Парламента № 998/2003, вступившему в силу 3 июля 2004 г., домашние животные (собаки, кошки и хорьки), путешествующие через границы Европейского союза, должны быть идентифицированы микрочипом либо отчетливым клеймом. 3) В Канаде с 2005 г. требуется наличие электронной метки у всех животных, покидающих хозяйство, где они появились.
Библиотеки	1) Учет перемещений книг и документов, защита от краж или случайного выноса. 2) Обустройство пунктов приема и выдачи книг: идентификация книг и читательских билетов. 3) Инвентаризация и поиск книг, контроль правильности размещения книг. 4) Оснащение комплексов и терминалов автоматической выдачи и приема книг, систем автоматической сортировки. 5) Одно из самых крупных библиотечных применений RFID - библиотека Ватикана, насчитывающая в своем фонде более двух миллионов экземпляров книг.
Паспортный контроль	1) Первые RFID-паспорта (e-паспорта) были введены в Малайзии в 1998 г. 2) RFID-метки включены в новые (биометрические) загранпаспорта граждан России с 2006 г.
Спорт	RFID-браслеты, одеваемые на спортсменов, используются в спортивном ориентировании, триатлоне и некоторых других видах спорта.

На следующих фотографиях показан внешний вид некоторых RFID-меток.



1) ключ для домофона; ISO 14443A



2) ключ для домофона; ISO 14443A



3) браслет; ISO10536/14443/15693



4) браслет; ISO10536/14443/15693



5) ушная клипса для животных; ISO 11784/11785



6) имплантат для животных и людей; ISO14443A



7) паспорт; ISO 14443



8) для забивки в деревянные изделия; ISO 17364; HID



9) на металл; EPC Class1 Gen2 и ISO 18000-6C; Confidex



10) на металл; EPC Class1 Gen2 и ISO 18000-6C; Confidex



11) на металл; EPC Class1 Gen2 и ISO 18000-6C; Confidex



12) на металл; EPC Class1 Gen2 и ISO 18000-6C; Confidex



13) для пластиковых контейнеров и возвратной тары; EPC Class1 Gen2 и ISO 18000-6C; Confidex



14) для пластиковых контейнеров и возвратной тары; EPC Class1 Gen2 и ISO 18000-6C; Confidex



15) для прачечных производств, медицинских учреждений для автоматизированного учета и сортировки изделий из ткани, постельного белья, одежды; ISO 18000-3; HID



16) для прачечных производств, медицинских учреждений для автоматизированного учета и сортировки изделий из ткани, постельного белья, одежды, хирургических инструментов; EPC Class1 Gen2 и ISO 18000-6C; HID



17) для дорогостоящих товаров; ISO 15693/18000-3; HID



18) для крепления на контейнеры с отходами; EPC Class1 Gen2 и ISO 18000-6C; HID

Рис.13.13. Внешний вид RFID-меток

(назначение; стандарты; производитель)

Система персональной карточной идентификации специфична для каждого государства. Одним из признаков жесткости системы идентификации является объем и степень детализации информации о субъекте, связанной с его уникальным идентификатором. В Малайзии действует одна из самых развитых систем такого рода. Там электронный паспорт на персону включает следующие данные: имя, дата рождения, пол, имена родителей, исповедуемая религия, этническая принадлежность, физические характеристики, фотография, отпечатки пальцев и идентификационный номер. Кроме того, эти карточки разных цветов: синяя — для граждан, красная — для постоянно проживающих, зеленая — для временно проживающих, коричневая — для бывших заключенных или диссидентов.

Системы поголовной идентификации трактовались в «свободном западном мире» как один из порочных атрибутов тоталитарного общества. Теперь же в этом самом мире развернулись дискуссии о введении надежной идентификации собственных граждан, как эффективном инструменте противодействия терроризму, оказания социальных услуг и защиты социальной справедливости в условиях массовой миграции населения [30].

Южной Корее ИС на основе ID-cards получили наибольшее распространение. К сентябрю 1999 г. все 37 миллионное население Кореи в возрасте до 18 лет получило национальные идентификационные карты. Карта используется для регистрации проживания, в качестве водительского удостоверения, пенсионного и медицинского страхового свидетельства. Она опционально может использоваться при выплате налогов, для оплаты телефонных звонков и в качестве электронного кошелька. Ее использование позволило снизить среднее время оказания различных услуг с 67 до 15 минут, а в области здравоохранения - с 55 до 5 минут [31].

В 2003г. завершена выдача подобных карт в Тайване (22 млн. населения) [30].

ID-карта гражданина Эстонии является первичным удостоверением личности и действительна в пределах Эстонии. Она признана всеми членами Евросоюза и государствами-членами Шенгенского соглашения, не входящими в Европейский Союз, в качестве официального удостоверения для путешествующего лица. Она используется крупными банками Эстонии в качестве средства аутентификации, может использоваться в качестве проездного билета в общественном транспорте городов Таллина и Тарту, для получения медицинских услуг и электронного голосования на выборах. В феврале 2007 г. Эстония была первой страной в мире, которая ввела электронное голосование на парламентских выборах. Более 30000 человек приняло участие в электронном голосовании [17].

[17, 36] В России был принят Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», в котором дается определение универсальной электронной карты, целей ее создания и областей применения. **Универсальная электронная карта (УЭК)** — российская пластиковая карта, объединяющая в себе идентификационное и платежное средство.

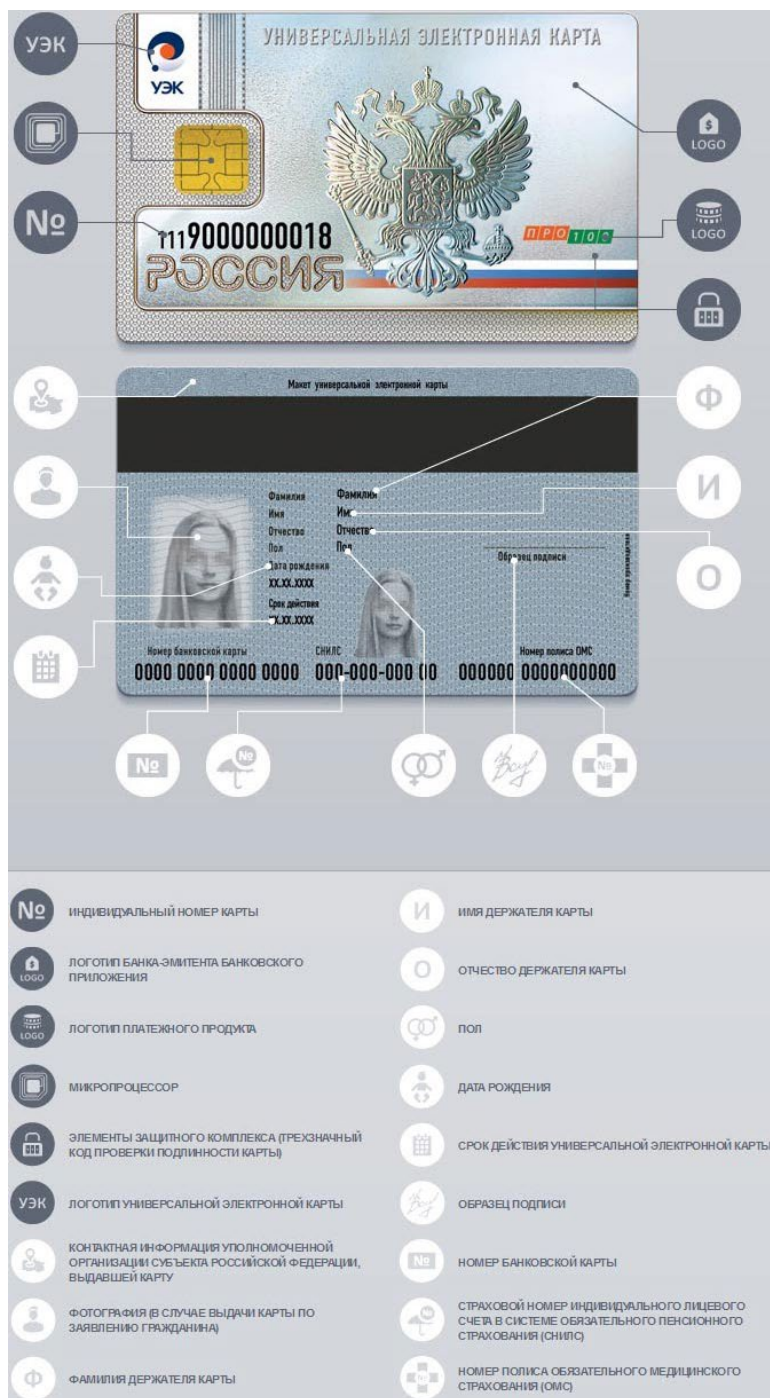


Рис.13.6. Универсальная электронная карта

С февраля 2012 г. в девяти пилотных регионах России начата выдача карты участникам проекта, с целью проверить, как она работает на практике. Масштабная выдача УЭК гражданам началась с января 2013 г. Она выдавалась гражданам России бесплатно по личному заявлению. Использование и подключенного к ней банковского счета бесплатно (за исключением стоимости считывателя карт). Срок действия универсальной электронной карты - 5 лет.

Основные возможности применения карты:

- идентификационное приложение — позволяет идентифицировать себя для получения государственных, муниципальных и коммерческих услуг, в том числе в медицинских учреждениях и в пенсионной системе (содержит паспортные данные, данные полиса обязательного медицинского страхования и страхового свидетельства государственного пенсионного страхования);
- электронная подпись — позволяет подписывать электронные документы усиленной квалифицированной электронной подписью при совершении юридически значимых действий в электронном виде;
- платежное приложение — позволяет осуществлять обычные банковские операции с расчетным счетом: оплата товаров и услуг, оплата государственных услуг, снятие денежных средств, перевод денежных средств и т. п. Держатель карты УЭК может совершать оплату дистанционно через Интернет, а также в более 100 000 торговых и сервисных предприятиях в России, которые обслуживаются банками, входящими в российскую платежную систему ПРО100 (на банкомате должна быть соответствующая наклейка). Для активации банковского приложения необходимо посетить выбранный банк, чтобы открыть расчетный счет. Комиссия за использование расчетного счета не взимается;
- держатель карты имеет возможность просматривать записанные на карту идентификационные данные (фамилия, имя, отчество, дата рождения и т. п.) и редактировать свои данные, предназначенные для заполнения различных электронных документов: почтовый адрес, номер телефона, адрес электронной почты. Наличие широкого спектра персональных данных на карте позволяет мгновенно заполнять заявления при обращении в многофункциональный центр или при подаче заявлений через Интернет.

Кроме этого, планировалось использовать карту, как универсальный проездной документ, электронный ключ, электронный кошелек, единую дисконтную и бонусную карту.

Для реализации указанных выше возможностей в «Спецификации универсальной электронной карты» (ред.2.1. от 2014г.) для карт на базе интегральных схем с криптографическими сопроцессорами (смарт-карт) регламентируется поддержка следующих **криптографических алгоритмов**:

- 3DES – время шифрования блока данных длиной 128 байт на ключе длиной 112 бит в режиме CBC-режим - не более 20 мс;
- RSA (поддерживаемая длина модуля ключей: для проверки электронной подписи – не менее 1984 бит, для вычисления электронной подписи – не менее 1024 бита) – время формирования ЭЦП (при представлении ключей RSA в формате CRT) над данными длиной 1024 бит – не более 250 мс; время проверки ЭЦП (при представлении ключей RSA в формате CRT) над данными длиной 1024 бит - не более 100 мс;
- SHA1 – время формирования проверочного значения (свертки, хеш-образа) сообщения (при длине 18 байт) – не более 30 мс;
- ГОСТ Р 34.10-2001 (действует до окончания срока действия сертификата ФСБ России) – время вычисления электронной подписи не более 250 мс, время проверки электронной подписи не более 500 мс;
- ГОСТ Р 34.10-2012 (начиная с 01.01.2015);
- ГОСТ 28147-89 – время криптографического преобразования (зашифрования/расшифрования) не более 2 мс;
- ГОСТ Р 34.11-94 (до окончания срока действия сертификата ФСБ России) – время формирования проверочного значения (свертки, хеш-образа) сообщения (при длине 32 байта) – не более 30 мс.

Хранение информации для считывания аппаратными средствами осуществляется на следующих **носителях**:

- магнитной полосе (по ГОСТ Р ИСО/МЭК 7811-6–2010);
- контактной смарт-карте (по ГОСТ Р ИСО/МЭК 7816-1–2010);
- бесконтактной (RFID) смарт-карте (по ГОСТ Р ИСО/МЭК 14443-1–2004).

Функции координатора и оператора проекта по внедрению УЭК осуществляет ФУО ОАО «Универсальная электронная карта» (ОАО «УЭК»). На официальном сайте ОАО «УЭК» <http://www.uecard.ru> на конец августа 2014 г. зарегистрировано более 450 000 заявлений от граждан РФ на получение карты.

28 декабря 2016 г. Президент РФ В.В. Путин подписал закон № 471-ФЗ, регламентирующий отмену УЭК как обязательного инструмента предоставления государственных и муниципальных услуг. Закон признаёт утратившей силу главу 6 («Организация деятельности по выпуску, выдаче и обслуживанию универсальных электронных карт») закона № 210-ФЗ от 27 июля 2010 г. «Об организации предоставления государственных и муниципальных услуг». Упоминания об УЭК удаляются также из отдельных положений, связанных с картой, из законов «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» и «Об обязательном медицинском страховании в Российской Федерации». Выпуск и выдача УЭК полностью прекращены с 1 января 2017 г. УЭК, выданная до 31 декабря 2016 г., может применяться до истечения срока ее действия. Приложения карты (банковское и идентификационное, содержащее СНИЛС и полис ОМС) также могут быть использованы для получения услуг до конца действия карты — при условии обеспечения технической возможности их приема. То же самое относится и к региональным приложениям, размещенным на карте.

В заключении следует отметить, что разумное применение ID-cards с ограниченной сферой действия и детализацией персональных данных представляется вполне разумной и оправданной мерой.

Вопросы для самопроверки

1. Дайте определение понятиям: «идентификация», «аутентификация», «авторизация».
2. Что может служить в качестве аутентификатора?
3. Перечислите основные способы организации идентификации и аутентификации.
4. Перечислите достоинства и недостатки парольной аутентификации.
5. Опишите схему протокола идентификации и аутентификации на основе алгоритма RSA.
6. В чем суть доказательства с нулевым разглашением.
7. Опишите схему протокола сервера аутентификации Kerberos.
8. Перечислите основные биометрические характеристики.

14. ПРОТОКОЛЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

14.1. Общие сведения

Протоколы ЭЦП с одной стороны относят к протоколам аутентификации, т.к. гарантируют, что сообщение поступило от достоверного отправителя, а с другой стороны к протоколам контроля целостности, т.к. гарантируют, что сообщение пришло в неискаженном виде. Более того, получатель в дальнейшем может использовать ЭЦП как доказательство достоверности сообщения третьим лицам (арбитру) в том случае, если отправитель впоследствии попытается отказаться от него.

Говоря о схеме цифровой подписи, обычно имеют в виду следующую **классическую ситуацию** [8]:

- отправитель знает содержание сообщения, которое он подписывает;
- получатель, зная открытый ключ проверки подписи, может проверить правильность подписи полученного сообщения в любое время без какого-либо разрешения и участия отправителя;
- безопасность схемы подписи гарантируется.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий *идентифицировать владельца* сертификата ключа подписи, а также *установить отсутствие искажения информации* в электронном документе (Федеральный закон № 1-ФЗ "Об электронной цифровой подписи" от 10.01.2002г.).

Электронная цифровая подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для *определения лица, подписывающего информацию* (Федеральный закон № 63-ФЗ "Об электронной подписи" от 06.04.2011г.).

[Электронная цифровая] подпись – строка бит, полученная в результате процесса формирования подписи (ISO/IEC 14888-1:2008 "Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения" и ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи").

При создании цифровой подписи по классической схеме отправитель:

- применяет к исходному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ **r** сообщения;
- вычисляет цифровую подпись **s** по хеш-образу **r** с использованием своего закрытого ключа;
- посылает сообщение **T** вместе с цифровой подписью **s** получателю.

Получатель, отделив цифровую подпись от сообщения, выполняет следующие действия:

- применяет к полученному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ **r** сообщения;
- расшифровывает хеш-образ **r'** из цифровой подписи **s** с использованием открытого ключа отправителя;
- проверяет соответствие хеш-образов **r** и **r'** и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

Как видно из этой схемы, порядок использования ключей обратный тому, который используется при передаче секретных сообщений. Вначале отправитель использует свой закрытый ключ, а затем получатель применяет открытый ключ отправителя.

Существует несколько схем ЭЦП, которые, как правило, применяются совместно с определенными хеш-функциями. Некоторые из них приведены в таблице.

Таблица 14.1. Схемы ЭЦП

Схема цифровой подписи	Задача, лежащая в основе стойкости	Хеш-функция
RSA	Разложение числа на множители	MD4 или MD5 (Message Digest Algorithm - алгоритм краткого изложения сообщения, Р. Ривест)
DSS (NIST ¹ . FIPS Publication 186: Digital Signature Standard (DSS). May 1994) DSS – Федеральный стандарт цифровой подписи США	Дискретное логарифмирование по схеме Эль-Гамала	SHA-1 (NIST. FIPS Publication 180: Secure Hash Standard (SHS). May 1993) SHS – стандарт хэш-функции США SHA - Secure Hash Algorithm – алгоритм хеш-функции
ECDSA (Elliptic Curve Digital Signature Algorithm) - алгоритм цифровой подписи на эллиптических кривых Принят в качестве стандарта ISO ² 14888-3 в 1998 г., ANSI ³ X9.62 – 1999 г., IEEE ⁴ 1363 – 2000 г. и NIST 186-2 – 2000 г. (последняя редакция – NIST. FIPS Publication 186-3: Digital Signature Standard (DSS). June 2009)	Дискретное логарифмирование в группе точек эллиптической кривой	SHA (NIST. FIPS 180-3: Secure Hash Standard (SHS). October 2008)
ГОСТ 34.10-94 (Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма)	Дискретное логарифмирование по схеме Эль-Гамала	ГОСТ 34.11-94 (Информационная технология. Криптографическая защита информации. Функция хэширования)
ГОСТ Р 34.10-2001 (Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи)	Дискретное логарифмирование в группе точек эллиптической кривой	ГОСТ 34.11-94 (Информационная технология. Криптографическая защита информации. Функция хэширования)
ГОСТ Р 34.10-2012 (Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи)	Дискретное логарифмирование в группе точек эллиптической кривой	ГОСТ Р 34.11-2012 (Информационная технология. Криптографическая защита информации. Функция хэширования)

Примечания.

¹NIST - Национальный Институт стандартов и технологий, США (The National Institute of Standards and Technology).

²ISO - Международная организация по стандартизации (International Organization for Standardization).

³ANSI - Американский национальный институт стандартов (American National Standards Institute).

⁴IEEE - Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers).

14.2. Протокол на базе алгоритма RSA

Этап 1. Выработка ключей (выполняет отправитель **A**) - см. лекцию "Шифрование с открытым ключом".

Этап 2. Отправка сообщения и электронной подписи (выполняет отправитель **A**).

Таблица 14.2. Отправка сообщения и ЭЦП на базе алгоритма RSA

№ п/п	Описание операции	Пример
1	Вычисление хеш-образа $h = h(T)$, где T – исходное сообщение, h(T) – хеш-функция (для MD5 длина хеш-образа 128 битов).	$h = 7$
2	Выработка цифровой подписи $s = h^d \bmod n$, где d – закрытый ключ отправителя A , n – часть открытого ключа отправителя A .	$s = 7^{29} \bmod 91 = 63$
3	Отправка получателю B исходного сообщения T и цифровой подписи s .	

Этап 3. Получение сообщения и проверка электронной подписи (выполняет получатель **B**).

Таблица 14.3. Получение сообщения и проверка ЭЦП на базе алгоритма RSA

№ п/п	Описание операции	Пример
1	Вычисление хеш-образа по полученному сообщению $h' = h(T')$, где T' – полученное сообщение. Если $T = T'$, то должно быть $h = h'$.	$h' = 7$
2	Вычисление хеш-образа из цифровой подписи $h = s^e \bmod n$, где e и n – открытый ключ отправителя A .	$h = 63^5 \bmod 91 = 7$
3	Если $h' = h$, то получатель B делает вывод, что полученное сообщение $T' = T$ и оно действительно отправлено A .	

14.3. Алгоритм цифровой подписи ГОСТ 34.10-94

Алгоритм цифровой подписи ГОСТ 34.10-94 похож на DSS-94, вариация на тему алгоритмов Шнорра и Эль-Гамала.

Этап 1. Выработка ключей (выполняет отправитель **A**).

Таблица 14.4. Выработка ключей для ЭЦП по ГОСТ 34.10-94

№ п/п	Описание операции	Пример
1	Выбор p - простого числа (для ГОСТ $509 < p < 512$ битов, либо $1020 < p < 1024$ битов).	$p = 79$
2	Выбор q - простого числа - множителя ($p - 1$) (для ГОСТ $254 < q < 256$ битов).	$q = 13$
3	Выбор a - любого числа, меньшего ($p - 1$), для которого $a^q \bmod p = 1$.	$8^{13} \bmod 79 = 1, a = 8$
4	Выбор закрытого ключа x - числа, меньшего q .	$x = 4$
5	Вычисление открытого ключа $y = a^x \bmod p$.	$y = 8^4 \bmod 79 = 67$
6	Публикация ключей. Первые три параметра p , q и a - открыты и могут совместно использоваться пользователями сети, y – персональный открытый ключ для одного пользователя, x – персональный закрытый ключ отправителя A .	

Этап 2. Отправка сообщения и электронной подписи (выполняет отправитель **A**).

Таблица 14.5. Отправка сообщения и ЭЦП по ГОСТ 34.10-94

№ п/п	Описание операции	Пример
1	Вычисление хеш-образа h = $h(T)$ (для ГОСТ длина хеш-образа 256 битов).	$h = 7$
2	Выбор k - любого числа, меньшего q .	$k = 11$
3	Вычисление двух значений: $w = a^k \bmod p$ и $w' = w \bmod q$ (для ГОСТ длина w' 256 битов). Если $w' = 0$, перейти к этапу 2 и выбрать другое значение числа k .	$w = 8^{11} \bmod 79 = 21$ $w' = 21 \bmod 13 = 8$
4	Вычисление $s = (x w' + k h) \bmod q$ (для ГОСТ длина s 256 битов). Если $s = 0$, перейти к этапу 2 и выбрать другое значение числа k .	$s = (4 \cdot 8 + 11 \cdot 7) \bmod 13 = 5$
5	Отправка получателю B исходного сообщения T и цифровой подписи (w', s).	

Этап 3. Получение сообщения и проверка электронной подписи (выполняет получатель **B**).

Таблица 14.6. Получение сообщения и проверка ЭЦП по ГОСТ 34.10-94

№ п/п	Описание операции	Пример
1	Вычисление хеш-образа по полученному сообщению $h' = h(T')$. Если $T = T'$, то должно быть $h = h'$.	$h' = 7$
2	Вычисление $v = h'^{q-2} \bmod q$.	$v = 7^{11} \bmod 13 = 2$

3	Вычисление двух значений: $z_1 = (s \cdot v) \bmod q$ и $z_2 = ((q - w') \cdot v) \bmod q$.	$z_1 = (5 \cdot 2) \bmod 13 = 10$ $z_2 = ((13 - 8) \cdot 2) \bmod 13 = 10$
4	Вычисление $u = ((a^{z_1} \cdot y^{z_2}) \bmod p) \bmod q$.	$u = ((8^{10} \cdot 67^{10}) \bmod 79) \bmod 13 = 8$
5	Если $w' = u$, то получатель В делает вывод, что полученное сообщение $T' = T$ и оно действительно отправлено А .	

14.4. Алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012

Алгоритмы цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 совпадают и похожи на ECDSA.

Этап 1. Выработка ключей (выполняет отправитель **А**) - см. лекцию "Шифрование с открытым ключом".

Этап 2. Отправка сообщения и электронной подписи (выполняет отправитель **А**).

Таблица 14.7. Отправка сообщения и ЭЦП по ГОСТ 34.10-2001 (34.10-2012)

№ п/п	Описание операции	Пример
1	Вычисление хеш-образа $h = h(T)$ (для ГОСТ длина хеш-образа 256 битов).	$h = 7$
2	Вычисление $e = h \bmod q$, где q – часть открытого ключа отправителя А .	$e = 7 \bmod 47 = 7$
3	Выбор k - любого числа, меньшего q .	$k = 11$
4	Определение точки эллиптической кривой $C(x_c, y_c) = k P(x_p, y_p)$, где $P(x_p, y_p)$ – часть открытого ключа отправителя А .	$C = 11 \cdot P(7, 17) = (16, 16)$
5	Вычисление $r = x_c \bmod q$. Если $r = 0$, перейти к этапу 2 и выбрать другое значение числа k .	$r = 16 \bmod 47 = 16$
6	Вычисление $s = (r \cdot d + k \cdot e) \bmod q$, где d - закрытый ключ отправителя А . Если $s = 0$, перейти к этапу 2 и выбрать другое значение числа k .	$s = (16 \cdot 10 + 11 \cdot 7) \bmod 47 = 2$
7	Отправка получателю В исходного сообщения T и цифровой подписи (r, s) .	

Этап 3. Получение сообщения и проверка электронной подписи (выполняет получатель **В**).

Таблица 14.8. Получение сообщения и проверка ЭЦП по ГОСТ 34.10-2001 (34.10-2012)

№ п/п	Описание операции	Пример
1	Вычисление хеш-образа по полученному сообщению $h' = h(T')$. Если $T = T'$, то должно быть $h = h'$.	$h' = 7$
2	Вычисление $e' = h' \bmod q$.	$e' = 7 \bmod 47 = 7$
	-1	-1

3	Вычисление $v = e' \mod q$. $(e' * e'^{-1}) \mod q = 1$.	$e' = 27$ $v = 27 \mod 47 = 27$
4	Вычисление двух значений: $z_1 = (s v) \mod q$ и $z_2 = ((q - r) v) \mod q$.	$z_1 = (2 * 27) \mod 47 = 7$ $z_2 = ((47 - 16) * 27) \mod 47 = 38$
5	Определение точки эллиптической кривой $C'(x_{c'}, y_{c'}) = z_1 P(x_p, y_p) + z_2 Q(x_q, y_q)$, где $Q(x_q, y_q)$ – часть открытого ключа отправителя A .	$C' = 7 P(7, 17) + 38 Q(36, 20) = (22, 26) + (11, 31) = (16, 16)$
6	Вычисление $r' = x_{c'} \mod q$.	$r' = 16 \mod 47 = 16$
7	Если $r' = r$, то получатель B делает вывод, что полученное сообщение $T' = T$ и оно действительно отправлено A .	

14.5. Разновидности ЭЦП

Кроме классической схемы ЭЦП различают еще несколько **специальных** [8]:

- схема "конфиденциальной" (неотвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;
- схема подписи "вслепую" ("затемненной" подписи) - отправитель не знает подписанного им сообщения;
- схема "мультиподписи" - вместо одного отправителя сообщение подписывает группа из нескольких участников;
- схема "групповой" подписи - получатель может проверить, что подписанное сообщение пришло от члена некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано. В то же время, в случае необходимости, отправитель может быть определен;
- и др.

14.6. Юридические основания использования ЭЦП

10 января 2002 г. Президент Российской Федерации В.В. Путин подписал Федеральный закон № 1-ФЗ "Об электронной цифровой подписи". **Цель Федерального закона № 1-ФЗ** - обеспечение правовых условий использования ЭЦП в электронных документах, при соблюдении которых ЭЦП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

В настоящий момент действует Федеральный закон № 63-ФЗ "Об электронной подписи" от 06.04.2011 г. **Сфера действия (цель) Федерального закона № 63-ФЗ** - регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

В системах, где число пользователей исчисляется сотнями и тысячами, для проверки ЭЦП используются так называемые сертификаты ЭЦП (ЭП).

Сертификат ЭЦП – открытый ключ с некоторой дополнительной информацией о его владельце (регистрационный номер сертификата, ФИО владельца, срок действия и т.д.), подписанный ключом **Центра сертификации** (ЦС, Certificate Authority, CA, Удостоверяющий центр, УЦ).

В Федеральном законе "Об электронной подписи" даны следующие определения.

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.

Квалифицированный сертификат ключа проверки электронной подписи – сертификат ключа проверки ЭП, выданный аккредитованным УЦ или доверенным лицом аккредитованного УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП.

При получении документа, подписанного ЭЦП, вначале подается запрос в ЦС, который высылает сертификат ЭЦП, информацию об окончании срока его действия или информацию об отсутствии сертификата. Если ЦС выслал сертификат, то считается, что документ послал именно тот, кто указан в сертификате. Для автоматизации деятельности ЦС применяется системы, называемые **системы поддержки инфраструктуры открытых ключей** (Public Key Infrastructure, PKI).

Впервые ссуда под ЭЦП (на покупку дома) была выдана в США 25 июля 2000г.

Вопросы для самопроверки

1. Дайте определение понятию "электронная цифровая подпись".
2. Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.
3. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП?
4. Опишите схему протокола ЭЦП на основе алгоритма RSA.
5. Перечислите специальные схемы ЭЦП.
6. Назовите цель введения в действие Федерального закона "Об электронной цифровой подписи".

15. ПРОТОКОЛЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ

15.1. Общие сведения

Как было отмечено в первой лекции, целостность является одним из трех ключевых свойств информации (доступность, целостность и конфиденциальность). При этом под **целостностью** понимается свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению.

Рассмотрим некоторые способы и методы контроля целостности.

15.2. Проверка четности

Представляет собой самый простой способ обеспечения целостности при хранении или передаче данных. Битовая строка (обычно длиной 7-8 бит), контроль которой необходимо выполнить, дополняется одним, так называемым **паритетным битом** (англ. parity bit). Существует две разновидности проверки четности: с **четным (even)** и **нечетным (odd)** паритетным битом. В первом случае при записи или пересылке данных паритетный бит устанавливается равным 1, если количество единиц в контролируемой строке нечетное, и 0 – если четное. В случае нечетного паритетного бита поступают наоборот.

Таблица 15.1. Примеры установки бита четности

Битовая строка	Паритетный бит	
	четный (even)	нечетный (odd)
1100 1011	1	0
1001 1001	0	1
1111 1111	0	1
0000 0000	0	1

Недостатки:

- исправление ошибки невозможно;
- в случае изменения состояния четного количества бит (например, двух), вычисленный паритетный бит совпадет с записанным. Т.е. ошибка не будет обнаружена. В то же время, согласно статистики, приблизительно 90% всех ошибок памяти происходит именно с одиночным разрядом. Т.о. проверки четности бывает достаточно для большинства ситуаций.

15.3. Использование контрольных цифр

В отличие от предыдущего способа для контроля целостности используется не бит, а цифра. Обычно, контролируемый набор цифр вначале по определенным правилам складывается, а затем берется остаток от деления по модулю, который и является контрольной цифрой. Ниже рассматриваются некоторые системы кодирования с использованием контрольной цифры:

- алгоритм Луна;
- штрихкод по стандарту EAN-13;
- заграничный паспорт гражданина РФ с биометрическими данными;
- индивидуальный номер налогоплательщика;
- коды станций на железнодорожном транспорте.

Алгоритм Луна (англ. Luhn algorithm) - алгоритм вычисления контрольной цифры в соответствии со стандартом ISO/IEC 7812 «Идентификационные карты. Идентификация эмитентов». Алгоритм разработан сотрудником фирмы IBM Гансом Питером Луном в 1954 г. Используется для подсчета контрольной цифры:

- номеров всех банковских карт;
- номеров некоторых дисконтных карт;
- кодов полисов обязательного медицинского страхования;
- единого 8-значного номера железнодорожного вагона на РЖД;
- IMEI-кодов (англ. International Mobile Equipment Identity - международный идентификатор мобильного оборудования);
- ICCID-кодов (англ. Integrated Circuit Card ID - идентификатор карты с интегрированной микросхемой);
- т.д.



а) банковская карта



б) полис медицинского страхования



в) цистерна



г) мобильный телефон (IMEI)



д) SIM-карта (ICCID)

Рис.15.1. Номера и коды с контрольными цифрами

В следующей таблице приведен порядок вычисления контрольной цифры на примере кода полиса медицинского страхования (рис. 15.16).

Таблица 15.2. Вычисление контрольной цифры по алгоритму Луна (если количество цифр в коде четное)

№ п/п	Описание операции	Пример
1	Каждая из цифр, стоящая в нечетной позиции, умножается на 2, после чего вычисляется остаток от деления на 9.	$(2 * 2) \bmod 9 = 4$ $(5 * 2) \bmod 9 = 1$ $(6 * 2) \bmod 9 = 3$ $(0 * 2) \bmod 9 = 0$ $(4 * 2) \bmod 9 = 8$ $(0 * 2) \bmod 9 = 0$ $(0 * 2) \bmod 9 = 0$ $(1 * 2) \bmod 9 = 2$
2	Вычисляется сумма остатков S_n .	$S_n = 4 + 1 + 3 + 0 + 8 + 0 + 0 + 2 = 18$
3	Вычисляется сумма цифр S_q , стоящих в четных позициях, за исключением последней.	$S_q = 7 + 8 + 2 + 8 + 2 + 0 + 2 = 29$
4	Вычисляется контрольная (последняя) цифра cd из уравнения $(S_n + S_q + cd) \bmod 10 = 0$.	$cd = 3$ $(18 + 29 + 3) \bmod 10 = 0$

Если количество цифр в коде нечетное (например, для IMEI-кодов), то 1 и 2 операция выполняются для цифр, стоящих в четных позициях, 3 операция – для цифр, стоящих в нечетных позициях.

Штрихкод по стандарту EAN-13 - одна из вариаций Европейского стандарта штрихкода, предназначенного для кодирования идентификатора товара и производителя. Регламентируется ГОСТ ИСО/МЭК 15420-2001 «Автоматическая идентификация. Кодирование штриховое. Спецификация символики EAN/UPC (EAN/ЮПиСи)».



Рис.15.2. Штрихкод EAN-13

В следующей таблице приведен порядок вычисления контрольной цифры по стандарту EAN-13.

Таблица 15.3

№ п/п	Описание операции	Пример
1	Вычисляется сумма цифр S_n , стоящих в нечетных позициях, за исключением последней.	$S_n = 5 + 0 + 2 + 4 + 2 + 4 = 17$
2	Вычисляется утроенная сумма цифр S_q , стоящих в четных позициях.	$S_q = 3 * (9 + 1 + 3 + 1 + 3 + 5) = 66$
3	Вычисляется контрольная (последняя) цифра cd из уравнения $(S_n + S_q + cd) \bmod 10 = 0$.	$cd = 7$ $(17 + 66 + 7) \bmod 10 = 0$

В России с 2009 г. во всех субъектах РФ действуют пункты выдачи паспортно-визовых документов нового поколения - **заграничных паспортов гражданина РФ с биометрическими данными.**

P<RUSANISIMOV<<VLADIMIR<<<<<<<<<<<<<<<<<<
725436239[5]RUS730107[2]M230712[7]<<<<<<<<<<<<<[02]

В нижней строке МСЗ используются пять контрольных цифр. Ее структура приведена в следующей таблице.

Контрольная цифра	Позиции знака, используемые для расчета контрольных цифр	Позиция контрольной цифры
Номер паспорта	1-9	10
Дата рождения	14-19	20
Дата истечения срока действия паспорта	22-27	28
Личный номер	29-42	43
Заключительная контрольная цифра	1-10, 14-20, 22-43 (позиции 11-13 и 23 исключаются из расчета)	44

Таблица 15.5. Пример расчета контрольных цифр нижней строки МСЗ

Назначение	Номер паспорта									КЦ				Дата рождения									КЦ				Дата истечения срока действия									КЦ				Личный номер				КЦ		КЦ	
№ позиции	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	...	42	43	44														
Нижняя строка МСЗ	7	2	5	4	3	6	2	3	9	5	R	U	S	7	3	0	1	0	7	2	M	2	3	0	7	1	2	7	<	...	<	0	2														
Весовой показатель	7	3	1	7	3	1	7	3	1	7				7	3	1	7	3	1	7		7	3	1	7	3	1	7	7	...	3	1															
Расчет контрольной цифры в элементе данных	$(7*7+2*3+5*1+4*7+3*3+6*1+2*7+3*3+9*1) \bmod 10 = 135 \bmod 10 = 5$													$(7*7+3*3+0*1+1*7+0*3+7*1) \bmod 10 = 72 \bmod 10 = 2$													$(2*7+3*3+0*1+7*7+1*3+2*1) \bmod 10 = 77 \bmod 10 = 7$													$(0*7+...+0*3) \bmod 10 = 0$							
Расчет заключительной контрольной цифры	$[(135 + 5*7) + (72 + 2*7) + (77 + 7*7) + (0 + 0*1)] \bmod 10 = 382 \bmod 10 = 2$																																														

Индивидуальный номер налогоплательщика (ИНН) - уникальный идентификатор, присваиваемый юридическому или физическому лицу для учета уплаты налогов в Российской Федерации. При постановке на налоговый учет подотчетному лицу выдается свидетельство, в котором указывается его ИНН.

Министерство Российской Федерации по налогам и сборам

СВИДЕТЕЛЬСТВО

о постановке на учет в налоговом органе
физического лица по месту жительства на территории Российской Федерации

Настоящее Свидетельство выдано в соответствии с положением части первой Налогового кодекса Российской Федерации, принятого Федеральным законом от 31 июля 1998 года N146-ФЗ, физическому лицу _____ (фамилия, имя, отчество)

пол муж.

дата рождения 7 января 1973 года (число, месяц, год)

место рождения БЕЛОГОРСК Г., 643 (указывается в полном соответствии с записью в документе, удостоверяющем личность)

и подтверждает постановку физического лица на учет 22 марта 2000 года (число, месяц, год постановки на учет)

в ИНСПЕКЦИИ МНС РОССИИ ПО ЖЕЛЕЗНОДОРОЖНОМУ РАЙОНУ
г. ХАБАРОВСКА 2 7 2 4

_____ (наименование государственной налоговой инспекции и ее код)

Идентификационный номер налогоплательщика (ИНН) 2 7 2 4 0 7 0 3 1 7 9 0

Дата выдачи Свидетельства 22 марта 2000 года (число, месяц, год)

Свидетельство применяется во всех предусмотренных законодательством случаях и предъявляется вместе с документом, удостоверяющим личность физического лица и место его жительства на территории Российской Федерации.

Свидетельство подлежит замене в случае переезда физического лица на новое место жительства на территории, подведомственную другой государственной налоговой инспекции, изменения приведенных в нем сведений, а также в случае порчи, утери.

Руководитель инспекции МНС России по Железнодорожному району г. Хабаровска _____ (подпись) **Д. Г. Бурковская**

М.П. МНС РОССИИ ПО ЖЕЛЕЗНОДОРОЖНОМУ РАЙОНУ г. ХАБАРОВСКА серия 27 № 0042973

Рис. 15.4. Свидетельство о постановке на учет

Контрольная (контрольные) цифра ИНН определяется по следующим формулам:

- для десятизначного ИНН юридического лица:

$$n_{10} = ((2n_1 + 4n_2 + 10n_3 + 3n_4 + 5n_5 + 9n_6 + 4n_7 + 6n_8 + 8n_9) \bmod 11) \bmod 10; \quad (15.1)$$

- для двенадцатизначного ИНН физического лица:

$$n_{11} = ((7n_1 + 2n_2 + 4n_3 + 10n_4 + 3n_5 + 5n_6 + 9n_7 + 4n_8 + 6n_9 + 8n_{10}) \bmod 11) \bmod 10, \quad (15.2)$$

$$n_{12} = ((3n_1 + 7n_2 + 2n_3 + 4n_4 + 10n_5 + 3n_6 + 5n_7 + 9n_8 + 4n_9 + 6n_{10} + 8n_{11}) \bmod 11) \bmod 10, \quad (15.3)$$

где n_i - i -ая цифра ИНН.

Для ИНН физического лица, отображенного на рис. 15.4, контрольные цифры:

$$n_{11} = ((7*2 + 2*7 + 4*2 + 10*4 + 3*0 + 5*7 + 9*0 + 4*3 + 6*1 + 8*7) \bmod 11) \bmod 10 = (185 \bmod 11) \bmod 10 = 9 \bmod 10 = 9,$$

$$n_{12} = ((3*2 + 7*7 + 2*2 + 4*4 + 10*0 + 3*7 + 5*0 + 9*3 + 4*1 + 6*7 + 8*9) \bmod 11) \bmod 10 = (241 \bmod 11) \bmod 10 = 10 \bmod 10 = 0.$$

Коды станций на железнодорожном транспорте. В информационных системах железнодорожного транспорта приняты различные способы кодирования станций. В АСУЖТ используется код станции, состоящий из 6 цифр ($n_1 n_2 n_3 n_4 n_5 n_6$). Последняя цифра кода (n_6) является контрольной и определяется по следующей формуле:

$$n_6 = (1n_1 + 2n_2 + 3n_3 + 4n_4 + 5n_5) \bmod 11. \quad (15.4)$$

Если остаток от деления меньше 10, то он является контрольной цифрой, иначе выполняют сдвиг весового ряда на две позиции и вычисления повторяют:

$$n_6 = (3n_1 + 4n_2 + 5n_3 + 6n_4 + 7n_5) \bmod 11. \quad (15.5)$$

Если новый остаток от деления вновь получится равным 10, то контрольная цифра принимается равной 0, иначе - остатку, вычисленному по формуле 15.5.

Первые четыре цифры АСУЖТ для станций, открытых для грузовых операций, называют кодом **Единой сетевой разметки (ЕСР)**. Вариация кода ЕСР с контрольной цифрой состоит из 5 знаков ($n_1 n_2 n_3 n_4 n_5$), последний из которых (n_5) определяется точно также, как и для кода станции в АСУЖТ. Отличие заключается в использовании сокращенных весовых рядов (1, 2, 3, 4) и (3, 4, 5, 6). Т.к. пятая цифра для грузовых станций в АСУЖТ принимается равной 0, то контрольные цифры кодов станций АСУЖТ и ЕСР совпадают. В частности, код станции Хабаровск-1 Дальневосточной железной дороги:

- АСУЖТ: код - 970406, контрольная цифра - $n_6 = (1*9 + 7*2 + 0*3 + 4*4 + 5*0) \bmod 11 = 39 \bmod 11 = 6$;

- ЕСР: код - 97046, контрольная цифра - $n_5 = (1*9 + 7*2 + 0*3 + 4*4) \bmod 11 = 39 \bmod 11 = 6$.

15.4. Использование контрольных сумм

Контрольные суммы (checksums или CRC) являются более надежным способом обеспечения целостности, чем биты четности или контрольные цифры. В англоязычной литературе CRC расшифровывается двояко в зависимости от контекста: Cyclic Redundancy Code или Cyclic Redundancy Check. Под первой расшифровкой понимают циклический код, под второй – хеш-образ.

Циклические коды основаны на полиномиальной арифметике по модулю 2 (полиномиальном делении без переноса). Вместо представления делимого (исходного сообщения, входных данных), делителя (порождающего полинома), частного (целой части) и остатка (контрольной суммы, CRC) в виде положительных целых чисел, их можно представить в виде полиномов с двоичными коэффициентами или в виде строки бит, каждый из которых является коэффициентом полинома. Например, десятичное число 19_{10} в двоичной системе счисления имеет вид 10011_2 , что совпадает с полиномом

1*x^4 + 0*x^3 + 0*x^2 + 1*x^1 + 1*x^0 = x^4 + x^1 + x^0. (15.6)

Значение контрольной суммы с порождающим полиномом G(x) определяется по формуле:

R(x) = P(x) * x^N mod G(x), (15.7)

где R(x) - полином, представляющий значение контрольной суммы;
P(x) - полином, представляющий входные данные;
G(x) - порождающий полином;
N - максимальная степень порождающего полинома.

Умножение x^N эквивалентно приписыванию N нулевых битов к входным данным. Полиномиальное деление без переноса выполняется по следующим правилам:

- при наличии у промежуточного остатка в качестве старшего бита «1», он складывается по модулю 2 (XOR, исключающее ИЛИ) с битовым представлением порождающего полинома и в частное записывается «1»;
- в противном случае выполняется сложение по модулю 2 промежуточного остатка с нулевой битовой строкой длиной N+1 и в частное записывается «0».

В следующей таблице приведены примеры определения контрольных сумм для порождающего полинома G(x) = x^4 + x^1 + x^0 (делитель - 10011₂, 19₁₀; N = 4; x^N = 10000₂).

Таблица 15.6. Примеры определения контрольных сумм

Делимое P(x) (входные данные)	10111 ₂ (23 ₁₀)	10011 ₂ (19 ₁₀)	10001 ₂ (17 ₁₀)
P(x) * x^N	101110000 ₂ (368 ₁₀)	100110000 ₂ (304 ₁₀)	100010000 ₂ (272 ₁₀)
Деление P(x) * x^N mod G(x)	101110000 10011 1 01000 00000 0 10000 10011 1 00110 00000 0 01100 00000 0 1100	100110000 10011 1 00000 00000 0 00000 00000 0 00000 00000 0 00000 00000 0 0000	100010000 10011 1 00100 00000 0 01000 00000 0 10000 10011 1 00110 00000 0 0110
Частное	10100 ₂ (20 ₁₀)	10000 ₂ (16 ₁₀)	10010 ₂ (18 ₁₀)
Остаток R(x) (контрольная сумма)	1100 ₂ (12 ₁₀)	0000 ₂ (0 ₁₀)	0110 ₂ (6 ₁₀)
Входные данные с контрольной суммой	10111 1100 ₂ (380 ₁₀)	10011 0000 ₂ (304 ₁₀)	10001 0110 ₂ (278 ₁₀)

Принимающая сторона для проверки целостности полученных данных может сделать одно из следующих равноценных действий:

- выделить входные данные, вычислить для них контрольную сумму (не забыв при этом дополнить данные N нулевыми битами) и сравнить ее с переданной;
- поделить входные данные с контрольной суммой (последняя строка табл. 15.6) на делитель, представляющий порождающий полином G(x). В результате должен получиться нулевой остаток.

Как было отмечено выше, использование циклических кодов является более надежным способом контроля целостности, чем биты четности. В то же время, при передаче исходного сообщения P(x) возможна такая его модификация, что контрольная сумма для него и принятого искаженного сообщения P'(x) будут совпадать. Т.е. циклические коды не лишены проблемы возникновения коллизий.

Выбор и применение на практике вида порождающего полинома определяется требованиями производительности и минимизации возникновения коллизий. В следующей таблице приведены некоторые разновидности порождающих полиномов, используемые в информационных системах.

Таблица 15.7. Разновидности порождающих полиномов

Название	Порождающий полином G(x)	Нормальное представление	Применение
CRC-1	x + 1	01 ₁₆	аппаратный контроль ошибок (нечетный паритетный бит)
CRC-4-ITU	x^4 + x + 1	03 ₁₆	
CRC-7	x^7 + x^3 + 1	09 ₁₆	системы телекоммуникации, MMC, SD
CRC-12	x^12 + x^11 + x^3 + x^2 + x + 1	080F ₁₆	системы телекоммуникации
CRC-16-IBM	x^16 + x^15 + x^2 + 1	8005 ₁₆	USB, ANSI X3.28
CRC-16-CCITT	x^16 + x^12 + x^5 + 1	1021 ₁₆	X.25, Bluetooth, SD, RFID
CRC-24-Radix-64	x^24 + x^23 + x^18 + x^17 + x^14 + x^11 + x^10 + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1	864CFB ₁₆	OpenPGP
CRC-32-IEEE 802.3	x^32 + x^26 + x^23 + x^22 + x^16 + x^12 + x^11 + x^10 + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1	1EDC6F41 ₁₆	V.42, MPEG-2, PNG
CRC-64-ISO	x^64 + x^4 + x^3 + x + 1	1B ₁₆	HDLC

Нормальное представление полинома указывается в стандартах, как правило, в шестнадцатеричном виде. При этом преобразование битовой строки полинома выполняется без учета старшего единичного бита. Например, для CRC-12 битовая строка порождающего полинома выглядит 1100000001111₂. Отбросив старший бит (100000001111₂) и преобразовав в шестнадцатеричный вид, получаем 080F₁₆.

Другой вариант использования контрольных сумм - проверка целостности хранимых файлов с целью обнаружения их искажения (например, вирусами) или подмены (например, rootkit в Unix-системах). В этом случае обычно применяют хеш-образы файлов, которые хранятся в защищенном месте и периодически используются для контроля целостности файлов. Хеш-образы активно применяют для проверки целостности скачиваемых файлов. В частности на многих сайтах, помимо дистрибутивов ПО, выкладываются также их контрольные хеш-образы.

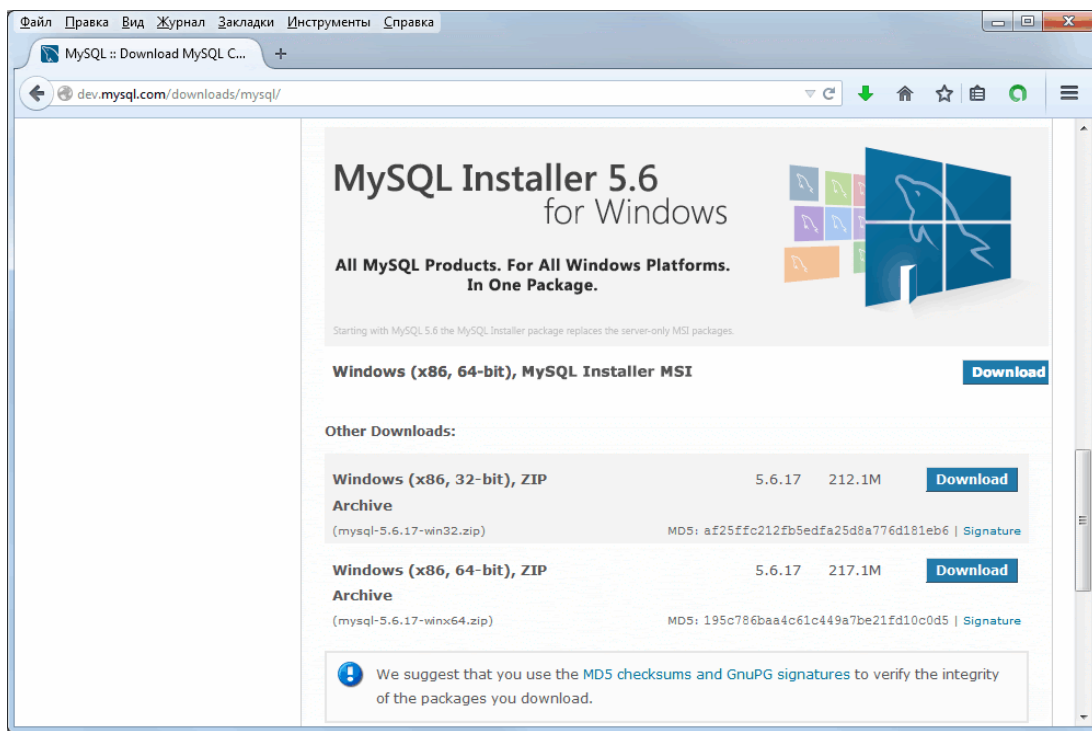


Рис.15.5. Контрольные суммы (хеш-образы MD5) для дистрибутивов СУБД MySQL

15.5. Использование кодов Хэмминга

Одним из существенных недостатков рассмотренных выше способов контроля целостности является невозможность устранения обнаруженных ошибок. В случае приема искаженных данных через сеть выполняется их повторная пересылка. Другим способом устранения этого недостатка является использование **самокорректирующихся кодов** - кодов, в которых возможно автоматическое исправление ошибок. Одним из них является код Хэмминга.

Код Хэмминга обычно обозначается (m, x) , где m - количество информационных и контрольных битов в блоке данных, x - количество информационных битов. Формула классического кода Хэмминга имеет вид $(2^r - 1, 2^r - r - 1)$, где r - количество контрольных битов (например: (7,4), (15,11) или (31,26)). Данная формула позволяет обнаруживать и исправлять одиночную ошибку, но при условии, что ошибок не более одной. В противном случае (возникновение двух и более ошибок в данных) использование кода Хэмминга некорректно.

Рассмотрим алгоритмы получения контрольных битов и проверки целостности данных на примере информационной битовой строки $X = 10010010111_2$ ($m = 15$ бит, $x = 11$ бит, $r = 4$ бита).

Номер позиции бита	1	2	3	4	5	6	7	8	9	10	11
Обозначение бита	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}
Значение бита, X	1	0	0	1	0	0	1	0	1	1	1

Алгоритм получения контрольных бит (кодирования).

1) В блок исходных данных вставляются контрольные биты ($r_1 \dots r_4$) таким образом, чтобы номера их позиций представляли собой целые степени двойки, начиная с нуля - $(2^0, 2^1, 2^2, 2^3) = (1, 2, 4, 8)$. Первоначально контрольные биты устанавливаются равными нулю.

Номер позиции бита	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Обозначение бита	r_1	r_2	x_1	r_3	x_2	x_3	x_4	r_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}
Значение бита, XR	0	0	1	0	0	0	1	0	0	0	1	0	1	1	1

2) К полученной таблице добавляются строки, число которых соответствует количеству контрольных битов. В столбцы добавленных строк записываются двоичные представления номеров позиций битов, причем порядок следования битов двоичного представления будет обратный - младший бит располагается в верхней строке, старший - в нижней.

Номер позиции бита	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Обозначение бита	r_1	r_2	x_1	r_3	x_2	x_3	x_4	r_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}
Значение бита, XR	0	0	1	0	0	0	1	0	0	0	1	0	1	1	1
Двоичное представление номера позиции бита, N	1	0	1	0	1	0	1	0	1	0	1	0	1	0	r_1
	0	1	1	0	0	1	1	0	0	1	1	0	0	1	r_2
	0	0	0	1	1	1	1	0	0	0	1	1	1	1	r_3
	0	0	0	0	0	0	1	1	1	1	1	1	1	1	r_4

3) Определение значений контрольных битов выполняется по формуле

$$r_j = \left(\sum_{i=1}^m XR_i * N_{ji} \right) \bmod 2, \quad (15.8)$$

где j - номер контрольного бита, $j = 1 \dots r$;
 i - номер позиции бита, $i = 1 \dots m$.

В терминах матричной алгебры получение вектора контрольных битов R является результатом перемножения вектора XR на транспонированную матрицу N (строки заменены на столбцы) по модулю 2.

$$R = (XR * N^T) \bmod 2. \quad (15.9)$$



Номер позиции бита	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Обозначение бита	r ₁	r ₂	x ₁	r ₃	x ₂	x ₃	x ₄	r ₄	x ₅	x ₆	x ₇	x ₈	x ₉	x ₁₀	x ₁₁	
Значение бита, XR	1	1	1	0	0	0	1	0	0	0	1	0	1	1	1	pb
Двоичное представление номера позиции бита, N	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	s ₁
	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	s ₂
	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	s ₃
	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	s ₄

Таким образом, блок данных вместе с контрольными битами будет выглядеть 10010010111 11000₂, где последний ноль - четный паритетный бит **pb**.

На этапе декодирования выполняется анализ вектора синдромов **S**, а также сравнение считанного (переданного) паритетного бита **pb** с вновь рассчитанным **pb'**. Возможны следующие случаи.

а) Ошибок нет. Вектор синдромов состоит из нулей, паритетные биты совпадают **pb = pb'**.

Номер позиции бита	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Обозначение бита	r ₁	r ₂	x ₁	r ₃	x ₂	x ₃	x ₄	r ₄	x ₅	x ₆	x ₇	x ₈	x ₉	x ₁₀	x ₁₁	
Значение бита, XR'	1	1	1	0	0	0	1	0	0	0	1	0	1	1	1	pb'
Двоичное представление номера позиции бита, N	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	s ₁
	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	s ₂
	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	s ₃
	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	s ₄

б) Одиночная исправимая ошибка. В векторе синдромов есть единицы, паритетные биты не совпадают **pb ≠ pb'**.

Номер позиции бита	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Обозначение бита	r ₁	r ₂	x ₁	r ₃	x ₂	x ₃	x ₄	r ₄	x ₅	x ₆	x ₇	x ₈	x ₉	x ₁₀	x ₁₁	
Значение бита, XR'	1	1	1	0	0	0	0	0	0	0	1	0	1	1	1	pb'
Двоичное представление номера позиции бита, N	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	s ₁
	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	s ₂
	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	s ₃
	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	s ₄

в) Двойная неисправимая ошибка. В векторе синдромов есть единицы, паритетные биты совпадают **pb = pb'**.

Номер позиции бита	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Обозначение бита	r ₁	r ₂	x ₁	r ₃	x ₂	x ₃	x ₄	r ₄	x ₅	x ₆	x ₇	x ₈	x ₉	x ₁₀	x ₁₁	
Значение бита, XR'	1	1	1	1	0	0	0	0	0	0	1	0	1	1	1	pb'
Двоичное представление номера позиции бита, N	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	s ₁
	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	s ₂
	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	s ₃
	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	s ₄

г) Тройная неисправимая ошибка. В векторе синдромов есть единицы или он нулевой, паритетные биты не совпадают **pb ≠ pb'**.

Номер позиции бита	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Обозначение бита	r ₁	r ₂	x ₁	r ₃	x ₂	x ₃	x ₄	r ₄	x ₅	x ₆	x ₇	x ₈	x ₉	x ₁₀	x ₁₁	
Значение бита, XR'	1	1	1	1	1	0	0	0	0	0	1	0	1	1	1	pb'
Двоичное представление номера позиции бита, N	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	s ₁
	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	s ₂
	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	s ₃
	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	s ₄

д) Четверная необнаруживаемая ошибка. Вектор синдромов состоит из нулей, паритетные биты совпадают **pb = pb'**.

Номер позиции бита	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Обозначение бита	r ₁	r ₂	x ₁	r ₃	x ₂	x ₃	x ₄	r ₄	x ₅	x ₆	x ₇	x ₈	x ₉	x ₁₀	x ₁₁	
Значение бита, XR'	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	pb'
Двоичное представление номера позиции бита, N	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	s ₁
	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	s ₂
	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	s ₃
	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	s ₄

Как видно из приведенных выше примеров, данный способ контроля целостности корректно ведет себя в случаях (а)-(в) и некорректно - (г)-(д).

15.7. Использование ЭЦП

Предыдущий способ для передачи и хранения критичных данных (конфиденциальной информации или исполняемых компонентов (ActiveX, exe-модулей и т.д.)) не годится. Злоумышленник может подменить передаваемые данные и контрольную сумму к ним, т.к. алгоритм генерации контрольных данных не является секретом и может быть известен любому желающему.

В случае использования ЭЦП эта проблема решается. Кроме того, можно также убедиться, что сообщение пришло от того, кто знает секретный ключ владельца подписи.

В Windows 2000 и XP все системные файлы и драйверы (с расширениями sys, dll, ocx, ttf, fon и exe) защищены с помощью ЭЦП. Данная функция работает в фоновом режиме и защищает все файлы,

установленные программой Windows Setup. Если новая версия не является корректной, то она заменяется копией из каталога %SystemRoot%\System32\Dllcache или диска дистрибутива. По умолчанию эта функция активирована и позволяет выполнить замену файлов только в случае установки следующих видов ПО:

- сервисных пакетов Windows;
- дистрибутивные пакеты типа Hotfix;
- обновление версии ОС с помощью Winnt32.exe;
- ПО Windows Update.

Для установки или просмотра опций защиты системных файлов необходимо выбрать «Мой компьютер \ пункт меню Свойства \ вкладка Оборудование \ кнопка Подписывание драйверов».

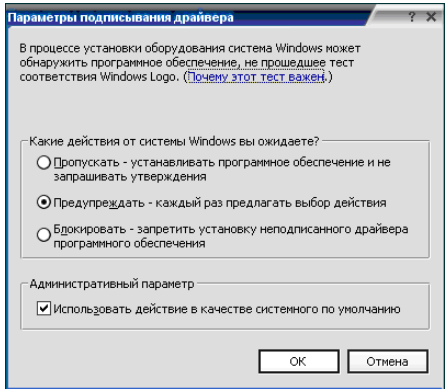


Рис.15.6. Параметры подписывания драйверов

Для проверки системных файлов можно воспользоваться стандартной утилитой командной строки Sfc.exe (System File Checker). В случае обнаружения некорректной версии файла она будет при возможности заменена.

С помощью стандартной утилиты sigverif.exe можно выявить все файлы в папке %SystemRoot% не имеющие подписи.

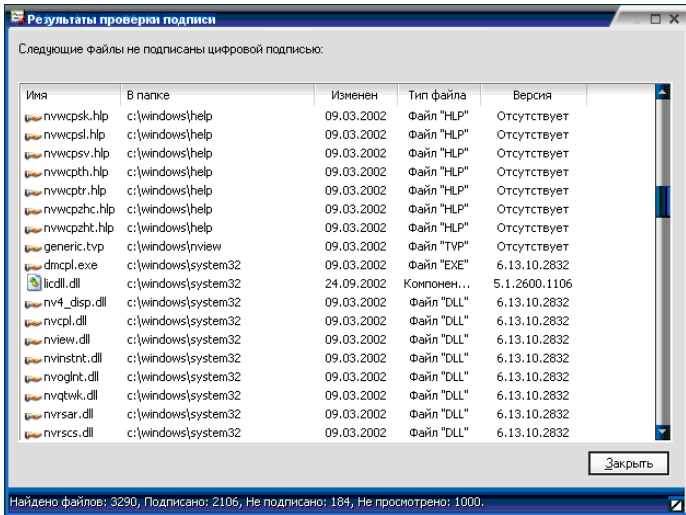


Рис.15.7. Результаты проверки подписи драйверов

15.8. Использование MAC-кодов

Код проверки подлинности сообщения (Message Authentication Code, MAC, имитовставка), известный также как код проверки подлинности данных (Data Authentication Code, DAC), представляет собой однонаправленную хеш-функцию с добавлением закрытого ключа. Значение хеш-образа зависит не только от документа, но и от ключа. В качестве примера MAC-кода можно привести последний 64-битовый блок, получаемый при шифровании DES в режиме CBC (Cipher Block Chaining, сцепление блоков шифра) [8].

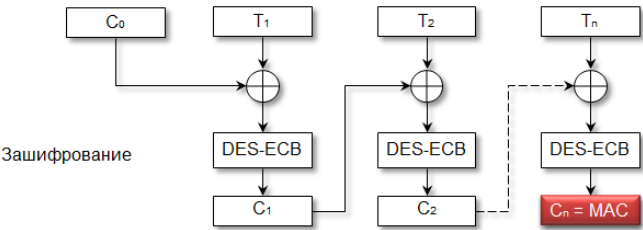


Рис.15.8. Схема алгоритма DES в режиме сцепления блоков шифра для получения MAC-кода

Сфера применения MAC-кодов аналогична ЭЦП, только в отличие от ЭЦП для их генерации используется симметричное шифрование.

15.9. Комбинированные методы (на примере жестких магнитных дисков)

Структура сектора жесткого магнитного диска приведена на следующем рисунке.

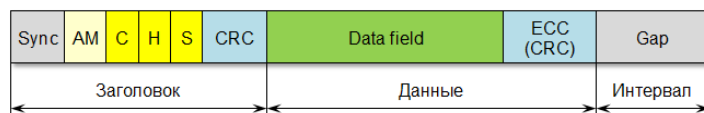


Рис.15.9. Структура сектора жесткого магнитного диска

Заголовок сектора содержит следующие поля:

- блок синхронизирующих байтов (Sync), обозначающих начало сектора и служащих для определения правильности позиционирования головки жесткого диска над дорожкой и сектором;
- адресный маркер (AM – address mark) – специальный байт, предваряющий идентификатор сектора;
- идентификатор сектора в формате CHS (C, cylinder – цилиндр; H, head – головка; S, sector – сектор);
- контрольная сумма (CRC) для проверки правильности чтения идентификатора сектора.

За пользовательскими данными (Data field) следует своя контрольная сумма (CRC) или код коррекции ошибок (ECC) для проверки/коррекции правильности чтения/записи данных. У современных жестких дисков, поддерживающих Advanced Format¹, размер пользовательских данных увеличен с 512 байтов до 4 килобайтов, а размер ECC с 50 до 100 байтов.

Интервал (Gap) дополняет сектор до требуемых размеров.

Между различными полями и блоками сектора могут присутствовать дополнительные байты-пробелы и служебные данные. В частности, практически у всех винчестеров в заголовке (например, после CRC заголовка или в 7 бите номера головки H) пишется информация о пригодности сектора для чтения/записи, т.е. ставится пометка сектора как «good» (хороший) или «bad» (плохой).

Bad-секторы (англ. bad - плохой, негодный) есть на любых винчестерах. Как бы тщательно не были изготовлены их диски, на каждом из них найдется несколько мест, запись или чтение которых сопровождается ошибками. Кроме того, на них встречаются участки поверхности, которые могут со временем перерасти в дефекты. Поэтому каждый накопитель после изготовления на заводе, проходит тщательное тестирование, в процессе которого выявляются испорченные секторы. Они помечаются как негодные и заносятся на диск в специальную таблицу - дефект-лист (**P-list**, Primary-list). Кроме заводского P-list'a дефектов накопитель имеет еще **G-list** (Grown-list) - в него заносятся сведения о bad-секторах, обнаруженных в процессе эксплуатации.

Для того, чтобы у пользователя создать иллюзию отсутствия дефектов на диске, на нем имеется резервная область с запасными дорожками или запасной сектор на каждой дорожке. Специальный «транслятор» диска пропускает через себя все обращения BIOS, ОС и прикладных программ к секторам и в случае необходимости перенаправляет их в резервную область. Только в случае переполнения G-list на диске появляются «видимые» bad-сектора.

Почти все винчестеры, выпущенные после 95-го года, имеют систему оперативного наблюдения за своим состоянием - **S.M.A.R.T.** (Self Monitoring And Reporting Technology). Эта технология позволяет в любое время оценить такие важные параметры накопителя, как количество отработанных часов, число возникших в процессе чтения/записи ошибок и многое другое.

Стандарт SMART-II регламентирует выполнение внутренней диагностики. Эта функция основана на проведении серии автономных внутренних тестов и предназначена для углубленного контроля за состоянием механики накопителя, поверхности дисков и многих других параметров. После выполнения тестов, накопитель должен записывать показания в SMART-атрибуты.

Для просмотра smart-статуса жесткого диска используют программы, называемые **smart-мониторами**. Одна из них - SmartMon (<http://www.kursknet.ru/~boa/delphi/SmartView.zip>, с исходными текстами на Паскале).

Id	Attribute Name	Value	Threshold	Worst Value	Raw Value
1	Raw Read Error Rate	71	34	64	00000B7DFE24
3	Spin Up Time	90	0	88	000000000000
4	Start/Stop Count	100	20	100	000000000058
5	Reallocated Sector Count	100	36	100	00000000000C
7	Seek Error Rate	80	30	60	00000616C9E4
9	Power On Hours Count	96	0	96	000000000F3D
10	Spin Retry Count	100	97	100	000000000000
12	Power Cycle Count	99	20	99	0000000006E9
194	Temperature	46	0	51	00000000002E
195	Unknown attribute	71	0	64	00000B7DFE24
197	Current Pending Sector Count	100	0	100	000000000000
198	Uncorrectable Sector Count	100	0	100	000000000000
199	UltraDMA CRC Error Rate	200	0	200	000000000000
200	Write Error Rate	100	0	253	000000000000
202	Unknown attribute	100	0	253	000000000000
130	Unknown attribute	1	0	0	01000100031B
218	Unknown attribute	0	0	5	0A0A0A0A0A0B
10	Spin Retry Count	0	0	0	760100000000
196	Reallocation Events Count	0	0	0	65104D000000
68	Unknown attribute	0	0	0	000000000000

Рис.15.10. Результат проверки жесткого диска программой SmartMon

Примечание. Raw Value – фактическое значение, Threshold – допускаемое производителем пороговое значение.

Между **SMART-атрибутами** и состоянием поверхности существует некоторая взаимосвязь. Рассмотрим те из них, которые имеют прямое отношение к bad-блокам.

Raw read error rate (1): количество ошибок чтения. У многих винчестеров (например, у Seagate и Fujitsu) они всегда выше нуля, но если значение Value находится в пределах нормы, опасаться нечего. Это «мягкие» ошибки, успешно скорректированные электроникой накопителя и не приводящие к искажению данных. Опасно, когда этот параметр резко снижается за короткий срок, переходя в желтую зону. Это говорит о серьезных проблемах в накопителе, о возможном появлении bad-секторов в ближайшее время.

Reallocated sector count (5): число переназначенных секторов. Эти атрибуты показывают количество секторов, переназначенных G-list. У новых винчестеров они обязательно должны быть равны нулю. Если их значение отличается от нуля, то это означает, что винчестер уже был в употреблении, на нем появлялись bad-сектора.

Current Pending Sector (197): этот атрибут отражает содержимое «временного» дефект-листа, присутствующего на всех современных накопителях, т.е. текущее количество нестабильных секторов. Эти секторы винчестер не смог прочесть с первого раза. Поле Value этого атрибута показывает общее количество секторов, которые накопитель в данный момент считает претендентами на переназначение в G-list. Если в дальнейшем какой-то из этих секторов будет прочитан (или переписан) успешно, то он исключается из списка претендентов. Постоянное значение этого атрибута выше нуля говорит о неполадках в накопителе.

Uncorrectable Sector (198): показывает количество секторов, ошибки в которых не удалось скорректировать ECC-кодом. Если его значение выше нуля, то это означает, что очень скоро во время записи данных ОС нарвется на этот сектор и в результате какая-нибудь важная информация или системный файл окажутся испорчены.

Посмотреть значения SMART-атрибутов можно также в программе SiSoftware Sandra.

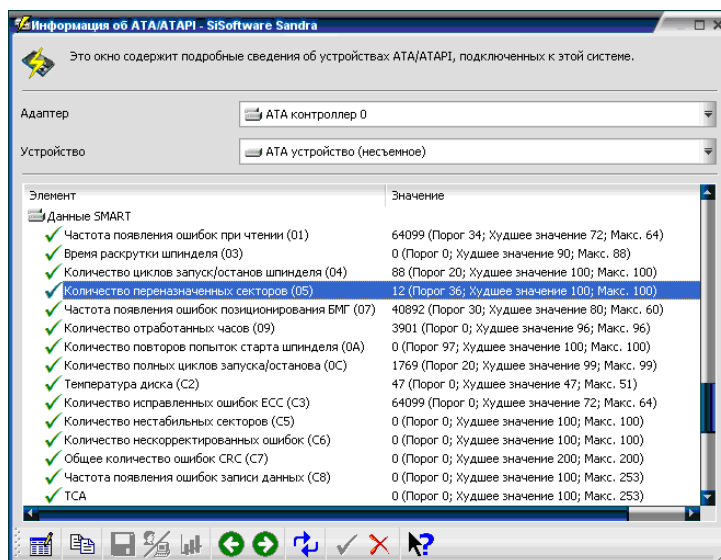


Рис.15.11. Результат проверки жесткого диска программой SiSoftware Sandra

¹Advanced Format (расширенный формат) предложен IDEMA Long Data Sector Committee.

Вопросы для самопроверки

1. Перечислите основные способы контроля целостности.
2. Что такое бит четности и как с помощью него осуществляется контроль целостности?
3. Для чего предназначена технология S.M.A.R.T.?

16. ПРОТОКОЛЫ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

16.1. Сущность и классификация денег

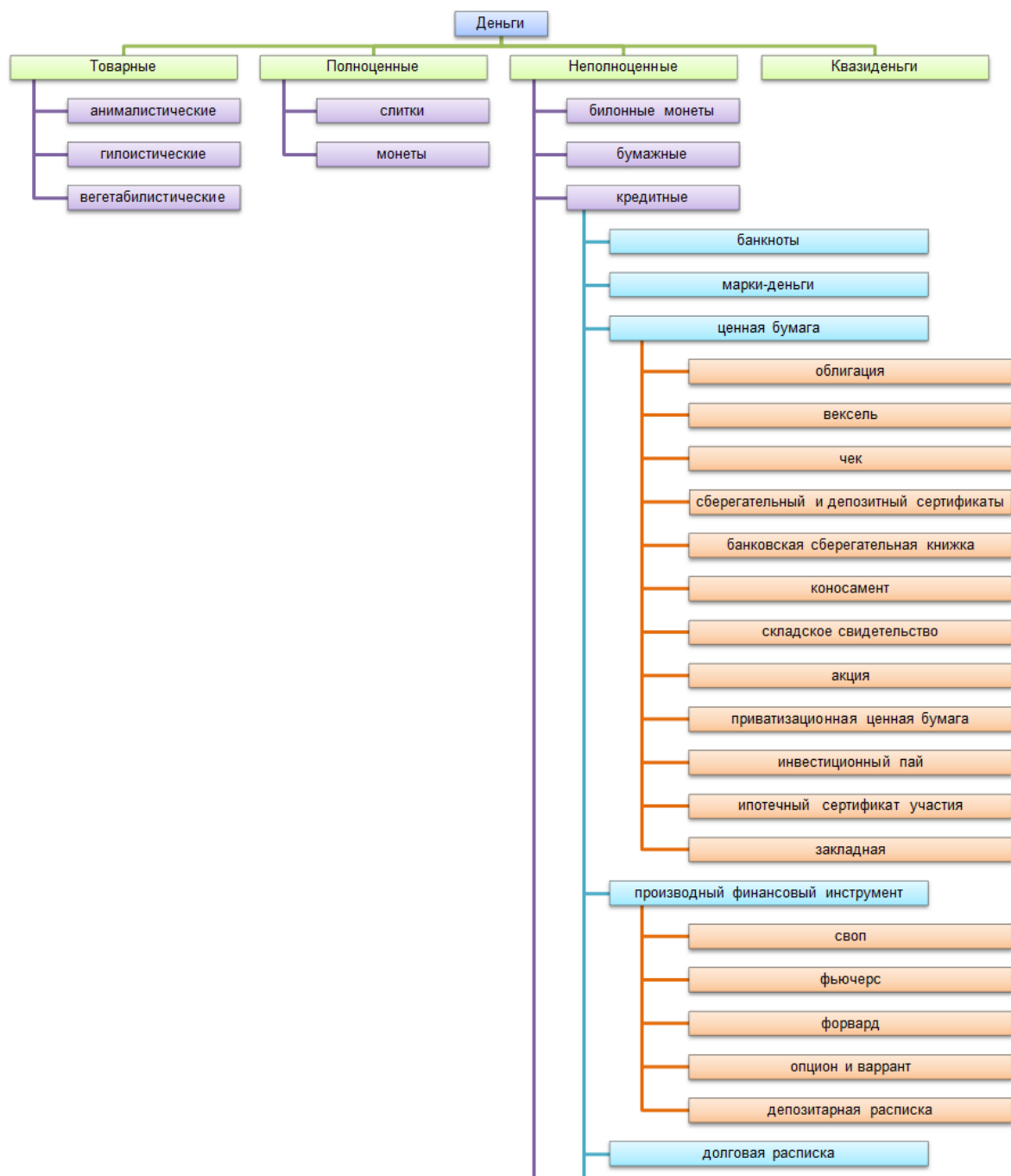
Деньги - специфический товар максимальной ликвидности, который является универсальным эквивалентом стоимости других товаров или услуг.

Деньги выпускаются **эмитентом** (англ. issuer – издатель, выпускающий) - органом исполнительной власти, местного самоуправления или юридическим лицом, которому в установленном порядке и на определенных условиях предоставлено право эмиссии (выпуска в обращение) денег. При этом под деньгами понимаются не только бумажные банкноты и монеты, но другие финансово-платежные средства (см. табл. 16.1).

Существует несколько **классификаций денег**:

- по статусу эмитента:
 - **фиатные** - деньги, номинальная стоимость которых устанавливается, обеспечивается и гарантируется государством посредством его авторитета и власти;
 - **частные** (нефиатные) - деньги, эмитируемые и используемые в обращении частными банками и организациями;
- по возможности идентификации владельца денег при оплате ими товаров и услуг:
 - **персонализированные** - деньги, при оплате которыми устанавливается личность владельца;
 - **анонимные** - деньги, при оплате которыми личность владельца остается неизвестной.

Наиболее распространенными являются классификации денег по видам (возможности преобразования в материальные ценности) и формам (материальному носителю и условиям обращения). На рис.16.1 приведены свернутые классификации видов (первый уровень) и форм (остальные уровни) денег, в табл.16.1 - классификации с определениями, историей и примерами.



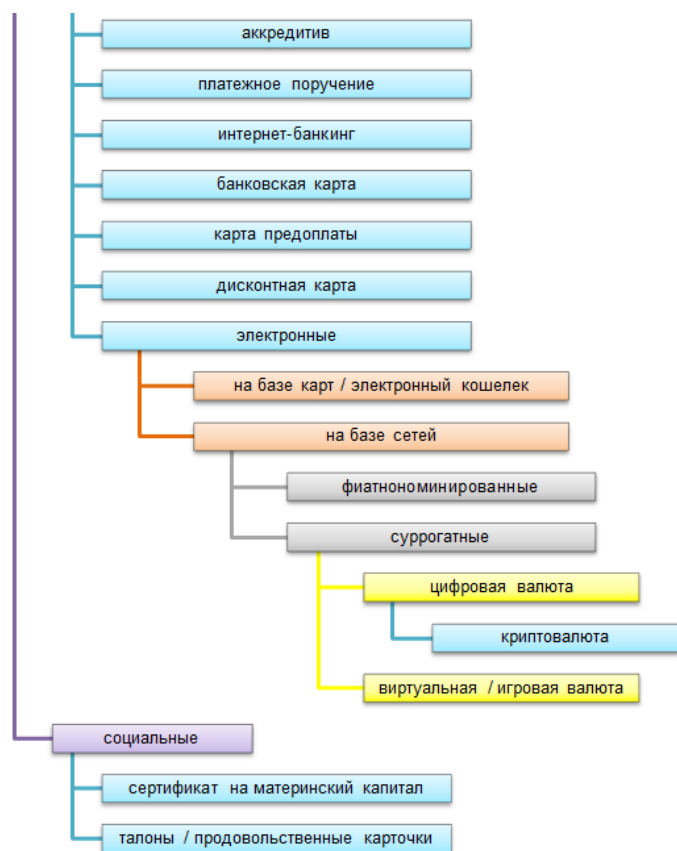


Рис.16.1. Виды и формы денег

Таблица 16.1. Виды и формы денег

Виды денег	Формы денег	История / Определения / Примеры
Товарные деньги - вид денег, представляющих собой реальные товары, которые, наряду с возможностью их потребления (непосредственного использования), могут выступать также в качестве эквивалента стоимости других товаров	анималистические (от лат. animal - животное) - животные и изделия из них, люди	Русское слово «товар» происходит от тюркского слова «скот». В Древней Руси существовала должность «скотника» - человека, взимающего подати. Гомер, говоря о стоимости некоторых видов оружия, оценивал их в быках . В частности, в Германии в I тысячелетии до н. э. имелись так называемые коровьи деньги. У северных народов денежной единицей служил олень, шкурки ценных пушных животных . На Руси долгое время в качестве денег использовалась шкурка белки , которая составляла одну копейку, сто шкурок - 1 рубль, в роли денег использовалась также шкурка куницы . В древности раковины каури были широко распространены в роли денег: их находили в скифских и русских погребальных курганах, в Германии, Англии, Швеции. У североамериканских индейцев из раковин вырезали цилиндры, нанизываемые на нитки («вампук»). В сокровищнице императора Монтесумы II конкистадоры нашли 2.5 тонны какао-бобов - ацтеки платили ими налоги. На островах Фиджи в качестве денег в ходу были зубы акулы . У многих народов единицей ценности и платежа были рабы (Африка, Новая Гвинея).
	гилоистические (от лат. hyle - вещество) - полезные ископаемые и орудия труда из них	Многие народы в качестве денег использовали металлические бруски и пластины определенного веса. Железные пластины были в употреблении у древних бриттов, в Спарте, в Африке. Медные Т-образные полоски (пластинки) шириной 4-5 см были деньгами в древней Мексике. Фароны Египта брали подати с Сирии серебряными кольцами и железными кирпичами . В Древнем Китае в качестве денег стали использовать орудия труда (плуги, ножи, мотыги), сделанные из различных металлов. Адам Смит рассказывал, что в его время (XVIII в.) в некоторых шотландских селениях между рабочими был распространен обычай платить торговцам вместо мелкой монеты железными гвоздями , которые охотно принимались и имели вполне определенную стоимость. То же самое говорит и Шевалье про каменноугольные округа Франции. В конце XIX в. Швейнфурт нашел у племени бонго (Судан) использование в качестве денег железных наконечников копий и лопаты . Другие разновидности: соль, жемчужины, драгоценные камни, янтарь, украшения , а также немаркированные слитки из меди, бронзы, золота, серебра и др. металлов.
	вегеталистические (от лат. vegetabilis - растительные) – растения, их плоды и продукты переработки	У первобытных народов Австралии был простой натуральный обмен. В древней Мексике, Никарагуа, Гондурасе в качестве мелких денег употреблялись бобы какао , а в Перу и Боливии - перец , в других регионах Америки - листья табака , в Монголии - кирпичный чай . Выдающийся русский путешественник Н. М. Пржевальский платил за барана 12-15 кирпичей чая, за верблюда 120-150 кирпичей. В Африке в период колонизации у многих племен деньгами служила бутылка рома . Другие разновидности: зерно, специи, сигареты, спирт, водка и т.д.
		Первые полноценные деньги выпускались в форме слитков (проволоки, пластин и т.д.). Для того чтобы преодолеть неудобства, связанные с определением количества и качества металла, содержащегося в слитке, верховные правители стали клеймить слитки, удостоверяя чистоту металла и его вес. В различных источниках по истории денег можно найти сведения о том, что первые слитки металлов, подтвержденные определенным клеймом, получили широкое хождение в Древнем Вавилоне и Египте. В Древней Руси в XII в. появились серебряные платежные слитки - гривны . В XIII в. для новгородских гривен стало употребляться наименование « рубль », которое постепенно вытеснило название «гривна». За рублем закрепилось название денежной

Полноценные (действительные) деньги – вид денег, номинальная (обозначенная на них) стоимость которых соответствует реальной стоимости металла, из которого они изготовлены

слитки

единицы, за гривной (гривенкой) - весовой (204.75 гр.). Платежные слитки в форме гривен были неразменными, обслуживали лишь крупные оптовые сделки и использовались главным образом для уплаты дани.



гривна

Недостатками металлических полноценных денег в слитках являлись слабая делимость и ограниченная транспортабельность.

монеты

Древние греки приписывали изобретение монеты героям своих мифов, **римляне** - богам Янусу или Сатурну. Согласно их воззрениям, древнейшие монеты с головой двуликого бога и носом корабля (ростром) выбил Янус в честь бога времени Сатурна, который приплыл в Италию с острова Крит на корабле. Само слово «монета» в переводе с латыни означает «предостерегающая» или «советница». Такой титул имела римская богиня Юнона - супруга громовержца Юпитера. Считалось, что она неоднократно предупреждала римлян о землетрясениях и нападениях врагов. На римском Капитолии возле храма Юноны Монеты размещались мастерские, где чеканились и отливались металлические деньги. По месту их изготовления продукция мастерских (монетного двора) также получила название «монета», которое затем попало в большинство европейских языков. Геродот и некоторые другие авторы древности писали о том, что первые монеты были отчеканены в **малоазийском государстве Лидии**. В наше время точно установлено, что древнейшие монеты появились в VII в. до н.э. Изготавливались они из электрума - природного сплава серебра и золота. На одной стороне монеты стояла проба, на другой - голова ассирийского льва. Лидийский царь Крез (561 - 546 до н. э.) установил стандарт чистоты металла (98% золота или серебра) и гербовую царскую печать на лицевой стороне (голова льва и быка). Эта официальная печать гарантировала качество царской монеты.



лидийские монеты

Первым государем, изобразившим свой профиль на монете, был Александр Македонский (Великий).



монеты с профилем Александра Македонского

Самостоятельно монеты были изобретены в **Индии** и **Китае**. Первые монеты в Китае появились: по китайским источникам - почти за 3000 до н.э.; дошедшие до нас древнейшие китайские монеты не восходят, однако, далее VII в. до н.э. Начало монетному обращению на **Руси** было положено в XIV в., в строго определенном количестве монеты стали чеканиться на монетных дворах Москвы, Нижнего Новгорода и Рязани. **Деньга (денга)** - русская монета XIV-XVIII вв. Чеканилась с конца XIV в. в Москве, с начала XV в. - почти во всех других русских княжествах. Изображения на монетах XV в. отличались исключительным разнообразием, причем в Москве наибольшей популярностью пользовалось изображение всадника с соколом или с саблей. Первоначально из гривенки серебра чеканили 200 московских или 100 новгородских монет. Остальные княжества постепенно, по мере образования централизованного государства, лишались права чеканить собственную монету. В результате реформы Елены Глинской (1508-1538 гг., мать Ивана Грозного) из гривенки серебра стали чеканить 300 монет весом 0.68 гр. каждая. На ней, как правило,

изображали всадника с копьем, от чего она получила название копейная денга (**копейка**).



денга 1731 г. и копейка 1715 г.

В соответствии с реформой Петра I серебряная копейка была заменена на медную и был введен серебряный рубль.

биллонные монеты - монеты, в которых содержание благородного металла (золота или серебра) составляет 50% и менее



денарий 238 г.

В **Российской империи** с 1867 по 1917 гг. монеты номиналом в 5, 10, 15 и 20 копеек чеканились из биллона с содержанием серебра 50%.



копейка с содержанием серебра 50%

История появления бумажных денег связана с использованием кожаных денег. В период китайской династии Хань в I в. появились деньги из шкур белых оленей. Поскольку все белые олени принадлежали императору, то только им могло быть принято решение об изготовлении этих денежных знаков. Первые как таковые бумажные деньги, как и бумага, были изготовлены в **Китае**. Первая известная бумажная банкнота была впервые выпущена во времена династии Тан в 7 в. Исторические свидетельства о существовании таких денег представлены в XIII в. итальянским путешественником Марко Поло. Самая древняя известная банкнота мира (Китай): частная - VIII в.; государственная - 812 г.



деньги династии Тан

Первые бумажные деньги в Европе были выпущены центральным банком **Швеции** (Stockholms Banco) в 1661 г.



деньги Stockholms Banco

бумажные деньги – бумажные знаки (заменители) полноценных денег, обмениваемые на них по установленному курсу

В **России** эмиссия бумажных денег (ассигнаций) впервые началась в 1769 г. Ассигнации использовались для выплаты жалования государственным служащим, государственных закупок продовольствия. В целях организации обращения ассигнаций был создан специальный Государственный ассигнационный банк.



ассигнация 1842 г.

Эмиссии бумажных денег государством нередко нарушали главное условие их устойчивости - размен на золото согласно объявленному курсу. Войны и революции требовали больших расходов, покрываемых выпуском бумажных денег, что наряду с потерей доверия населения к правительству приводило к их обесценению и, как следствие, к девальвации денег.

Эпоха золотовалютного стандарта закончилась в 1971 г., когда США отказались от

свободного обмена долларов на золото. Основная причина краха Бреттон-Вудской системы - огромное количество долларов, выпущенных США, которые не были обеспечены золотом.



обеспеченный доллар 1934 г.

банкнота (от англ. bank - банк и note - расписка)
/
банковский билет (от древненем. bille - игральная кость)



миллиард триллион (10^{21}) пенге (Венгрия, 1945-1946 гг.)

марки-деньги

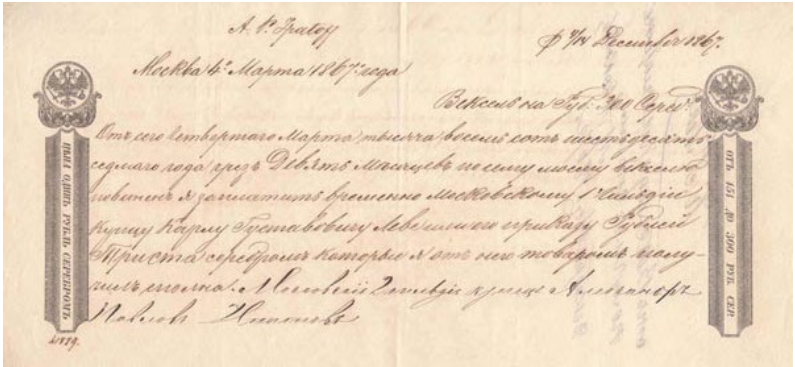
особый вид непочтовых марок, выполняющие функции разменной монеты в связи с ее недостатком.



марки-деньги (1915 – 1916 гг.)

облигация (от лат. obligatio - обязательство)

ценная бумага, удостоверяющая право ее держателя на получение от лица, выпустившего облигацию, в предусмотренный в ней срок номинальной стоимости облигации или иного имущественного эквивалента. Облигация предоставляет ее держателю также право на получение фиксированного в ней процента от номинальной стоимости облигации либо иные имущественные права.

		
вексель (нем. wechsel)	письменное долговое обязательство строго установленной формы, дающее его владельцу (векселедержателю) ничем не обусловленное обязательство векселедателя (простой вексель) либо иного указанного в векселе плательщика (переводной вексель) выплатить по наступлении предусмотренного векселем срока полученные займы денежные средства. 	
чек (фр. cheque; англ. cheque/check)	ценная бумага, содержащая распоряжение чекодателя плательщику произвести платеж указанной в нем суммы чекодержателю. Чекодателем является лицо, имеющее денежные средства в банке, которыми он вправе распоряжаться путем выписывания чеков, чекодержателем - лицо, в пользу которого выдан чек, плательщиком - банк, в котором находятся денежные средства чекодателя. Главным отличием чека от векселя является наличие у покупателя (должника) счета в банке, который производит оплату по письменному обязательству чекодателя. Другое отличие заключается в том, что чек используется в дебетовых операциях, а вексель – в кредитных. 	
сберегательный и депозитный (от лат. depositum - положенное, залог) сертификаты (от лат. certum - верно и facere - делать)	ценная бумага, удостоверяющая сумму вклада, внесенного в банк, и права вкладчика (держателя сертификата) на получение по истечении установленного срока суммы вклада и обусловленных в сертификате процентов в банке, выдавшем сертификат, или в любом филиале этого банка. Депозитные сертификаты выдаются юридическим лицам, сберегательные – физическим.	



ценная бумага, удостоверяющая заключение договора банковского вклада с гражданином и внесение денежных средств на его счет по вкладу.
Аналог сберегательного сертификата, но позволяет в течение действия договора (если это прописано в нем) пополнение или снятие средств с вклада, получение процентов и др.

банковская
сберегательная
книжка



документ, выдаваемый перевозчиком груза грузовладельцу и удостоверяющий право собственности грузовладельца на отгруженный товар.

коносамент (фр.
connaissement,
англ. bill of
lading)

ценная бумага - документ, удостоверяющий с соблюдением установленной формы и обязательных реквизитов имущественные права, осуществление или передача которых возможны только при его предъявлении.

В России рынок ценных бумаг регламентируется: - Гражданским кодексом РФ; - ФЗ «О рынке ценных бумаг»; - ФЗ «Об акционерных обществах»; - ФЗ «Об инвестиционных фондах»; - ФЗ «Об ипотечных ценных бумагах».

складское свидетельство

акция (от лат. actio - движение, действие, поступок)

SHIPPER (Complete Name and Address) SHENSHEN BAITEMAN TECH. COMPANY LIMITED ADDRESS: 4F ZHENG FENG BUILDING FUYONG TOWN BAO AN DISTRICT SHENZHEN GUANG DONG CHINA TEL: 0086-755-27383577 FAX: 0086-755-21580416		JOB NO: SE0904167	BILL OF LADING NO: SSOF090406718
CONSIGNEE (Complete Name and Address) ET: hide client's information ADD: STR, 22, E BULGARIA ATT: hide client's information TEL: 00359 8885 information 3 0002		CHARTER LINK LOGISTICS LIMITED as the Carrier BILL OF LADING	
ACTIVITY PARTY (Complete Name and Address) SAME AS CONSIGNEE		FOR RELEASE OF SHIPMENT, PLEASE CONTACT TEAM TRANS HAMBURG GMBH WENDENSTRASSE 8-12 20097 HAMBURG TEL: 49-40 22 63 05 37 FAX: 49-40 22 63 05 59	
PER: SHEN SHEN / CHINA	PLACE OF RECEIPT: SHEN SHEN / CHINA		
VESSEL / VOYAGE: CSCL LE HAVRE 0029W	PORT OF LOADING: SHEN SHEN / CHINA		
PORT OF DISCHARGE: HAMBURG	PLACE OF DELIVERY: SOFIA		
PARTICULARS FURNISHED BY SHIPPER			
MARKS & NUMBERS	NO. OF PKGS.	DESCRIPTION OF GOODS	GROSS WEIGHT (KGS) MEASUREMENT (CBM)
OCLU6546789 / E842687 / 40'HQ (	650.00 KGS / 2.200 CBM / 31 CTNS)		650.00 2.200
CFS / CFS C/NO.: 1/31-2-31	31 CTNS	S.T.C. PARKING SENSOR CAR ALARM HID KIT *****TELEX RELEASE*****	
"FREIGHT PREPAID" TOTAL: THIRTY ONE (31) CTNS ONLY.		Shipped on board	05-APR-2009
FREIGHT AND CHARGES PAYABLE BY SHIPPER		AT: SHEN SHEN / GUANGDONG	
The above particulars are according to the declaration of the shipper. The Carrier received the above goods in apparent good order and condition, unless otherwise specified, for carriage to the place as agreed above subject to the terms of this Bill of Lading including those on the back page. If required by the Carrier, one original of this Bill of Lading must be surrendered duly endorsed in exchange for the goods or delivery order. In witness whereof the original Bill of Lading has been signed in the number stated below, one of which being accomplished the other(s) to be void. IN ACCEPTING THIS BILL OF LADING, the Shipper, Consignee, Holder hereof, and Owner of the goods, agree to be bound by all of its stipulations, exceptions and conditions, whether written, printed or stamped on the front or back hereof, as well as the provisions of the above Carrier's published Tariff Rules and Regulations.			
OCEAN FREIGHT AS ARRANGED		Number of original (Bill) of Lading issued THREE (3) (If more than one original issued, the others stand void when ONE is accomplished)	
TERMS OF LADING CONTAINED ON REVERSE SIDE		BILL OF LADING NO. SSOF090406718	
Excess value declaration as per Clause 11.4		PLACE AND DATE OF ISSUE SHEN SHEN / CHINA 05-APR-2009	
The contract evidenced by this Bill of Lading is governed by the laws of the Hong Kong Special Administrative Region. Any proceedings against the Carrier must be brought in the courts of the Hong Kong Special Administrative Region and no other court.			

ценная бумага, подтверждающая принятие товара на хранение на товарном складе.

ПРОСТОЕ СКЛАДСКОЕ СВИДЕТЕЛЬСТВО

№ _____ Серия КСД _____

Исходящий № по реестру товарного склада _____
Дата выдачи свидетельства _____
Настоящее складское свидетельство выдано на предъявителя.
Настоящим складским свидетельством подтверждается, что товарный склад _____ (наименование товарного склада)
расположенный по адресу _____ (место нахождения склада)
принял на хранение следующие товары:
а) наименование товара _____
б) единица измерения _____
в) количество товара _____
г) качественные характеристики _____
д) прочие условия _____
Общая стоимостная стоимость товара составляет _____ (сумма цифрами и прописью) рублей
Товарный склад обязуется хранить указанное количество товара _____ (до востребования, указанное количество лет, до указанной даты)
и возратить держателю свидетельства равное количество товара того же наименования и качества, принятые на хранение товары.
Перед востребованием товара со склада направляются внутренним документом товарного склада.
Держатель настоящего складского свидетельства вправе самостоятельно распоряжаться товаром, помещенным на склад, путем передачи этого складского свидетельства.
За хранение товара держатель складского свидетельства уплачивает товарному складу вознаграждение в размере _____ (сумма прописью за каждый день, год и т.д.) рублей.
Вознаграждение за хранение уплачивается _____ (указать кем, когда и способ оплаты)
От лица товарного склада _____ (фамилия, должность, подпись)
Печать товарного склада _____

ценная бумага, закрепляющая права ее владельца (акционера):
- на получение части прибыли акционерного общества в виде дивидендов;
- на участие в управлении акционерным обществом;
- на часть имущества, остающегося после его ликвидации.

	 ПРИВИЛЕГИРОВАННАЯ АКЦИЯ СБЕРЕГАТЕЛЬНОГО БАНКА РОССИИ г. МОСКВА НОМЕР 082429 ОДНА ТЫСЯЧА РУБЛЕЙ 1992 г. 1 000 УСТАВНЫЙ КАПИТАЛ БАНКА ДЕСЯТЬ МИЛЛИАРДОВ РУБЛЕЙ БАНКОМ ВЫПУЩЕНО: 1. 180.000 обыкновенных акций номинальной стоимостью пятьдесят тысяч рублей. 2. 1.000.000 привилегированных акций номинальной стоимостью одна тысяча рублей. Регистратор - Центральный банк России г. Москва ПРЕЗИДЕНТ СБЕРЕГАТЕЛЬНОГО БАНКА РОССИИ ГЛАВНЫЙ БУХГАЛТЕР 1. Владелец акции имеет преимущественное право на получение дивидендов. 2. Владелец акции не имеет права голоса в управлении банком. 3. Владелец акции регистрируется в реестре банка. 4. Факт перепродажи акции отражается записью в книге учета владельцев на оборотной стороне бланка акции и заверяется печатью реестровщика и печатью банка с указанием даты перепродажи. 5. Утрата акции востанавливается за плату. 6. Ставка дивиденда устанавливается собранием акционеров на год вперед.
приватизационная (от лат. privatus - частный) ценная бумага	 РОССИЙСКАЯ ФЕДЕРАЦИЯ ГОСУДАРСТВЕННАЯ ЦЕННАЯ БУМАГА Действителен по 31 декабря 1993 года. Подделка чеков преследуется по закону. 1992 ПРИВАТИЗАЦИОННЫЙ ЧЕК 10 000 РУБЛЕЙ 14 4146958
инвестиционный (от лат. investire – облачать, одевать) пай (тур. payı - доля)	именная ценная бумага, удостоверяющая: - долю ее владельца в праве собственности на имущество, составляющее паевой инвестиционный фонд; - право требовать от управляющей компании надлежащего доверительного управления паевым инвестиционным фондом; - право на получение денежной компенсации при прекращении договора доверительного управления паевым инвестиционным фондом со всеми владельцами инвестиционных паев этого паевого инвестиционного фонда.

(обозначенная на них) стоимость которых не соответствует реальной стоимости материала, из которого они изготовлены, и предназначенные для замещения в обращении полноценных денег

кредитные деньги - специальным образом оформленные права на требование в будущем долга в отношении физических или юридических лиц

закладная



ипотечный (греч. hypotheke - заклад) сертификат участия

именная ценная бумага, удостоверяющая:
- долю ее владельца в праве общей собственности на ипотечное покрытие;
- право требовать от выдавшего ее лица надлежащего доверительного управления ипотечным покрытием;
- право на получение денежных средств, полученных во исполнение обязательств, требования по которым составляют ипотечное покрытие;
- иные права по ФЗ «Об ипотечных ценных бумагах».

именная ценная бумага, которая удостоверяет право ее законного владельца на получение исполнения по денежному обязательству, обеспеченному ипотекой, а также право залога на имущество, обремененное ипотекой (в виде земли, дома, строений и т.п.).

		
производный финансовый инструмент (дериватив - англ. derivative) - договор (контракт), по которому стороны получают право или берут обязательство выполнить	своп (англ. swap – обмен)	договор, по которому продается актив и одновременно принимается обязательство выкупить его обратно через определенный срок на тех же или иных условиях.
	фьючерс (от англ. future - будущее)	срочный биржевой контракт купли-продажи актива, при заключении которого стороны договариваются только о цене и сроке поставки. Остальные параметры актива (количество, качество, упаковка, маркировка и т.п.) оговорены заранее в спецификации биржевого контракта.
	форвард (англ. forward - вперед)	срочный контракт, в соответствии с которым стороны соглашаются о купле-продажи в определенный срок актива оговоренного качества и количества по цене, сформировавшейся на момент реализации контракта. Отличия от фьючерса: - фьючерсы обращаются на бирже, форварды – на межбанковском рынке; - фьючерсы стандартизированы по условиям и срокам поставки, в форвардах эти параметры могут быть произвольными; - в фьючерсах цена покупки актива фиксирована, в форвардах – определяется на момент реализации контракта.
	опцион (от лат. optionis - выбор, желание) и варрант (англ. warrant - полномочие, доверенность)	ценная бумага, дающая держателю право (но не обязанность) купить определенное количество актива (обычно акций) в предусмотренный в ней срок и/или при наступлении указанных в ней обстоятельств по указанной в опционе цене с уплатой за это право определенного вознаграждения (премии, страховки) продавцу.

некоторые действия в отношении базового актива



депозитарная расписка



долговые расписки (обязательства)

документ, оформленный в свободной форме и выдаваемый заемщиком кредитору при получении кредита (или займа).

Расписка

Город
Дата

Я, ФИО заемщика, дата рождения, паспорт серия, номер, кем и когда выдан, место постоянной или временной регистрации, фактическое место проживания, получил по настоящей расписке от ФИО заимодавца, дата рождения, паспорт серия, номер, кем и когда выдан, место постоянной или временной регистрации, фактическое место проживания, денежную сумму в размере (размер полученной суммы чистом и прописью).

На сумму займа начисляются проценты за пользование в размере (сумма процентов чистом и прописью) % годовых.

Сумму займа вместе с процентами обязуюсь вернуть займодавцу не позднее (дата).

Подпись заемщика _____ (ФИО)

условное денежное обязательство, принимаемое банком-эмитентом по поручению плательщика, произвести платежи в пользу получателя средств по предъявлении последним документов, соответствующих условиям аккредитива, или предоставить полномочия исполняющему банку произвести такие платежи.

аккредитив (от лат. ad - к, и credere - верить)

АККРЕДИТИВ N <Номер>		<Дата>		<Видплатежа>		0401063	
Сумма прописью		Дата		Вид платежа			
ИНН <Плательщик>		Сумма		<Сумма>			
Плательщик		Сч. N		<ПлательщикРасчСчет>			
<ПлательщикБанк1>		БИК		<ПлательщикБИК>			
<ПлательщикБанк2>		Сч. N		<ПлательщикКорсчет>			
Банк плательщика		БИК		<получательБИК>			
<ПолучательБанк1>		Сч. N		<получательКорсчет>			
<ПолучательБанк2>		Сч. N		<получательКорсчет>			
Банк получателя		Сч. N		<номерсчетаПоставщика>			
ИНН <Получатель>		Сч. N (40901)		<номерсчетаПоставщика>			
		Вид оп.		<Видоплаты>		Срок дейст. аккредит.	
		Наз. пл.				Срок платежа	
Получатель		Код				Рез. поле	
Вид аккредитива		<ВидАккредитива>					
Условие оплаты		<УсловиеОплаты1> <УсловиеОплаты2> <УсловиеОплаты3>					
наименование товаров (работ, услуг), N и дата договора, срок отгрузки товаров (выполнения работ, оказания услуг), и место назначения <НазначениеПлатежа>							
платеж по представлению (вид документа) <Платежпопредставлению>							
дополнительные условия <Дополнусловия>							
N сч. получателя <ПолучательРасчСчет>							
Подписи				Отметки банка			
М.П.							

платежное поручение

Образец						0401060	
Поступ. в б		Списано со сч. плат.					
ПЛАТЕЖНОЕ ПОРУЧЕНИЕ № 003		01.01.2012					
		Дата		Вид платежа			
Сумма прописью							
ИНН		КПП		Сумма			
				Сч. №			
Плательщик				БИК			
				Сч. №			
Банк плательщика				БИК		046577001	
ГРКЦ ГУ БАНКА РОССИИ ПО СВЕРДЛОВСКОЙ ОБЛ. Г.ЕКАТЕРИНБУРГ				Сч. №			
Банк получателя				Сч. №		40501810100002000002	
ИНН 6660004669		КПП 667001001		Сч. №			
УФК по Свердловской области (ИГД УрО РАН (л/сч 20626Ц19390)				Вид оп.		01	
				Наз. пл.		Срок плат.	
				Код		Очер. плат.	
Получатель						Рез. поле	
48630201010010000130		65401000000					
По сч N от г. за выполненные работы по дог. НИР (номер и дата договора) в т.ч. НДС. П. разрешение.1							
Назначение платежа				Отметки банка			
Подписи							
М.П.							

интернет-банкинг

общее название технологий персонализированного дистанционного банковского обслуживания, а также доступ к банковским счетам и операциям по ним через Интернет.

персонализированная платежная карта, выпущенная банком или иной специализированной организацией, удостоверяющая наличие в соответствующем учреждении счета владельца банковской карты и дающая право на приобретение

		товаров и услуг по безналичному расчету.	
банковская карта			
карта предоплаты / карта с хранимой стоимостью (англ. stored-value card)		карта (сертификат), фиксирующая факт внесения определенной суммы в кассу эмитента и предназначенная для оплаты товаров и услуг эмитента. Представляет собой, как правило, неперсонализированное платежное средство. Стоимость карты может выражаться деньгами, минутами, литрами, поездками и т.д. Данные о неиспользованной сумме средств на пластиковых картах хранятся в зашифрованном виде. Разновидности карт: транспортные, телефонные, топливные, подарочные, накопительные, бонусные, оплаты услуг и т.д. 	
дисконтная карта (купон, ваучер, талон и т.п.)		средство, гарантирующее получение потребителем скидки в торговых точках продавца (-ов) или участников дисконтного клуба при соблюдении правил использования дисконтных карт. 	
электронные деньги - денежные обязательства эмитента, хранение и использование которых осуществляется исключительно электронными средствами.	на базе карт / электронный кошелек (англ. e-Purse или e-Wallet)	смарт-карта или другой электронный носитель со встроенным чипом, позволяющие хранить зашифрованную сумму средств и осуществлять оплату товаров и услуг. По назначению аналогичны картам предоплаты, но позволяют пополнять сумму средств на карте. Термин может употребляться по отношению к информационным системам, позволяющим производить операции пополнения, хранения и перечисления электронных денег на базе сетей. 	
		фиатнономинированные (от лат. fiat - декрет, указание, «да будет так») электронные деньги	электронные деньги, хранимые на персональном счету клиента в базе данных эмитента и номинированные в одну из национальных валют, как правило, с возможностью конвертации в другие национальные валюты. В отличие от интернет-банкинга и банковских карт, эмитенты таких денег не являются банками, хотя и могут получать лицензию на банковскую деятельность на территории некоторых стран. Открытие счета клиента может быть анонимным (т.е. без предоставления персональных данных), но с

	и карты предоплаты.	на базе сетей		обязательным получением клиентом данных для идентификации и аутентификации, необходимых для пользования деньгами на счете. частные электронные деньги, используемые как альтернативная или дополнительная валюта. Номинальная стоимость цифровой валюты может быть привязана к одной или корзине национальных валют, золоту и т.п. разновидность цифровой валюты, эмиссия и учет которой основаны на асимметричном шифровании и применении криптографических методов защиты. частные электронные деньги, используемые для приобретения и продажи виртуальных товаров в различных сетевых сообществах: социальных сетях, виртуальных мирах, онлайн-играх и т.п.
	сертификат на материнский (семейный) капитал		суррогатные (от лат. surrogates - поставленный взамен) электронные деньги	именной документ, подтверждающий право на дополнительные меры государственной поддержки для семей, воспитывающих детей. Выдается с 1 января 2007 г. при рождении или усыновлении второго, третьего или последующего ребенка, имеющего российское гражданство. Материнский капитал может быть потрачен только на следующие цели: - улучшение жилищных условий; - получение образования ребенка; - увеличение пенсионных накоплений матери. 
				Впервые карточки на получение продовольствия использовались еще в Древнем Риме. Во Франции в период якобинской диктатуры вводились карточки на хлеб (1793 – 1797 гг.). Во время Первой мировой войны нормированное карточное распределение существовало в ряде воюющих держав, в частности, в США, Германии и России. В 1916 г. карточная система вводилась даже в нейтральной Швеции. В период Второй мировой войны нормированное карточное распределение основных продовольственных товаров было введено в ряде держав, участвующих в войне: СССР, Германии, Великобритании, США, Канаде, Японии и пр. В СССР карточное распределение введено с июля 1941 г., отменено в декабре 1947 г.

социальные
деньги –
финансовые
обязательства,
выдаваемые
органом
государственной
власти для
поддержки
малоимущих
слоев населения
или обеспечения
приоритетных
социальных
программ

талоны (от лат. talus игральная кость)
/
продовольственные (продуктовые)
карточки

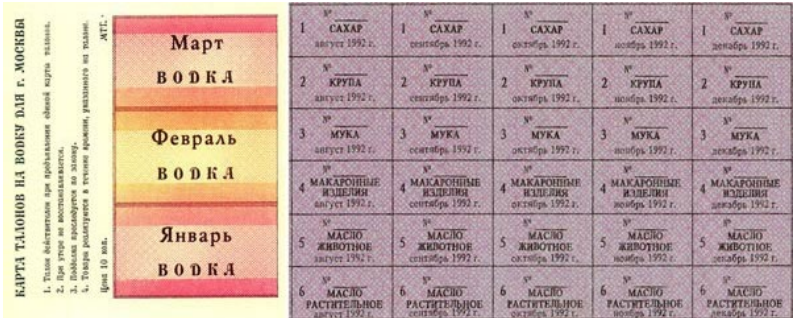


германская продовольственная карта 1940 г.



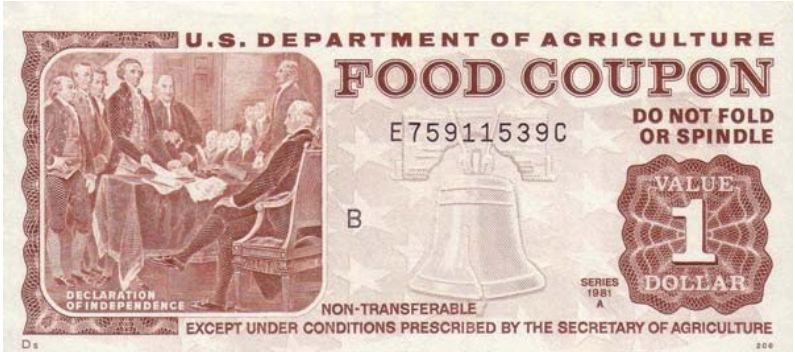
советская продовольственная карта 1942 г.

Наибольшее распространение в современной **России** талонная система получила в 1991-1992 гг. Талоны были введены на табачные изделия, водку, колбасу, мыло, чай, крупы, соль и сахар. В некоторых случаях, в отдаленных местностях талоны вводились на хлеб, майонез, стиральный порошок, женское белье и т.п.



российские талоны на водку (1990 г.) и продукты (1992 г.)

В развитых странах под талонами обычно понимают карточки на товары первой необходимости для социально незащищенных слоев населения. Товары по талонам выдаются либо бесплатно, либо по льготным ценам. Талонная система (Американская программа льготной покупки продуктов - англ. Supplemental Nutrition Assistance Program) для наименее защищенных групп населения давно уже действует в **США** (на постоянной основе с 1964 г.). Современные продуктовые карточки в Америке представляет собой пластиковую карту, ежемесячно пополняемую государством из бюджетных средств. В среднем каждый человек получает продуктовых талонов на \$115 в месяц, а семья - на \$255 месяц. В 2012 г. количество американцев, получающих продуктовые талоны, выросло до рекордных 46,7 млн человек.



		американский талон на еду 1982 г.
Квазиденьги (лат. quasi - как будто, якобы)		денежные средства, находящиеся на срочных и сберегательных банковских счетах, а также наиболее ликвидные финансовые инструменты (ценные бумаги и их производные), обращающиеся на рынке (по методологии МВФ).

Примечание. В таблице предпринята попытка обобщения и систематизации разрозненных (порой противоречивых) сведений о видах и формах денег из различных источников (1. Гражданский кодекс РФ; 2. ФЗ «О рынке ценных бумаг»; 3. Большая советская энциклопедия; 4. Финансовый словарь; 5. Экономический словарь; 6. Энциклопедический словарь Ф.А. Брокгауза и И.А. Ефрона; 7. Деньги, кредит, банки. Под ред. О.И. Лаврушина – М.: КНОРУС, 2010. – 320 с.; 8. ru.wikipedia.org; 9. www.grandars.ru; 10. Другие источники).

Современные платежные системы построены на кредитно-дебетовых операциях, сущностью которых является долговые обязательства одних лиц перед другими. Долговые обязательства, составленные в письменной форме, являются одним из самых старых финансовых инструментов и имеют давнюю историю (дается в кратком изложении по очень интересной книге [46] в [следующем разделе](#)).

).

16.2. Краткая история денег

16.2.1. Месопотамия и Вавилон

В XIX в. до н.э. ассирийские купцы из Месопотамии создали свои коммерческие колонии в Каппадокии (Малая Азия). Поскольку караванные путешествия иногда длились по несколько лет, торговля между Ашшуром и каппадокийскими колониями осуществлялась с помощью кредитных операций. Предоставление ассирийским купцом из Анатолии купцу, идущему с караваном в Ашшур, определенной суммы денег на закупку товаров подтверждалось долговой распиской на глиняной табличке. Если у кредитора возникала потребность вернуть свои деньги, он мог передать долговое обязательство другому кредитору (**тамкару**), который покупал его либо по номинальной стоимости, либо со скидкой.

Долговые надписи на глиняных табличках были достаточно стандартными: «Он (такой-то...) должен уплатить владельцу этой таблички». Позднее частные лица стали использовать подобную формулировку в контрактах, а долговой документ на глиняной табличке давал возможность взыскать долг в указанный срок, при этом имя начального кредитора иногда опускалось. По-видимому, именно ассирийские коммерческие агенты - тамкары впервые в истории применили договорные долговые обязательства среди ограниченного круга лиц, признававших и принимавших их.

Большинство сохранившихся документов на глиняных табличках датируется так называемой старовавилонской эпохой - временем правления царей первой династии, наиболее известным из которых был Хаммурапи (1792-1750 гг. до н.э.). Этим деловым документам был присущ строгий формализм, объединявшийся с лаконизмом и юридической точностью формулировок, что свидетельствует о достаточном развитии правового института долгового обязательства. Типичный договор займа имел обычно следующую форму:

- объект займа (серебро или натуральные продукты);
- величина процента или указание беспроцентного займа;
- обязательная формулировка: должник (имя) взял займы у кредитора (имя);
- время, место и способ погашения займа;
- свидетели и дата.

В этих документах просматривается достаточно сформированная система понятий. Документы в целом назывались duppum; письменный договор - riksatum; документ с печатью - kinnukktum. Беспроцентный заем именовался kirtum (на юге Вавилонии) или hubutatum (на севере); прибыль при обмене монет - tappitatum (на юге) или piplatum (на севере). Документ о займе под проценты назвался kunuk hu-bu-li, а документ о беспроцентном займе - kunuk hu-bu-ta-ti.

Известный исторический памятник «Законы Хаммурапи» свидетельствует не только о существовании долговых документов, но и о попытках регулирования кредитных отношений законодательным путем. В частности, согласно законам Хаммурапи, передача денег без расписки считалась недействительной, а максимальный процент кредита не мог превышать 33% (1/3). В частности одна из сохранившихся до наших табличек гласила:

Минутум одолжил в храме Шамаша 10 гур зерна с вознаграждением в 1/5 гур за один гур и возвратит долг во время сбора урожая.

Подписи трех свидетелей (без даты).

16.2.2. Древняя Греция

Среди прототипов векселя следует отметить синграфы и хирографы, возникшие в Древней Греции ($\approx$ V в. до н.э.). **Синграф** излагался в третьем лице («Такое-то лицо (имя) должен такому-то лицу (имя) такую-то сумму») и составлялся в двух экземплярах в присутствии пяти свидетелей, которые подписывали его вслед за должником. **Хирограф** излагался в первом лице («Я, такой-то лицо (имя) должен такому-то лицу (имя) такую-то сумму»), составлялся в одном экземпляре и подписывался только должником. При выполнении торгово-финансовых операций возникали ситуации, когда в одном и том же городе могли быть и кредиторы, и должники купца, находившегося в другом месте. Во избежание пересылки денег купец мог возратить долги жившим в другом городе кредиторам за счет тех сумм, которые ему должны были третьи лица, проживавшие в одном городе с кредиторами.

В Древней Греции постепенно сформировался особый торговый класс (karēloi), профессионально занимавшийся коммерческой деятельностью. Об этом свидетельствуют труды Аристофана, где упоминаются многие торговые профессии, а также менялы - **трапезиты**. Аристотель четко разграничивал торговлю (emproia) и кредитные операции (tokismos).

Известно, что в эллинистическом Египте, кроме частных банкиров, существовали прототипы государственных финансовых учреждений, и каждая провинция (ном) имела свое учреждение (trapesa basiliki), руководившееся царским чиновником, обязанным осуществлять выплаты в соответствии с контрактам.

Важными новшествами в осуществлении платежей стали письменное платежное поручение и чековый платеж, о чем свидетельствует большое количество банковских документов на папирусе. В I в. до н.э. чековые платежи были широко распространены, и, приблизительно в это же время, стал употребляться греческий

термин **гипограф** (чек или письменное поручение банкиру уплатить деньги).

В 1973 г. библиотека Государственного университета штата Флорида (США) приобрела 24 банковских документа, написанных на папирусе приблизительно между 87 и 84 гг. до н.э. Они имеют стандартную форму и касаются платежных поручений гераклеопольского отделения банка:

*Птолемей, сын Хестиея, приветствует банкира Протарка. Пожалуйста, заплатите Епитеуксу 500 (пятьсот) драхм медью.
26 Фармоута 31 года.*

16.2.3. Древний Рим

Приемы и способы кредитных операций, осуществляемых в Римской империи, были заимствованы в Греции и греческих колониях. Первые свидетельства о существовании финансовых учреждений в Древнем Риме относятся к IV - III в. до н. э., и в большинстве случаев финансово-кредитной деятельностью там занимались греки. В целом же, в Римском государстве товарно-денежный оборот и, соответственно, финансовые инструменты кредита были развиты намного больше, чем в Греции.

В товарообороте Древнего Рима обращались монеты разных денежных систем, а постоянная нехватка наличных денег требовала безналичных форм расчетов, среди которых важное место отводилось кредитным операциям. Как правило, кредитные соглашения заключались на месяц и разрешалось взимать проценты в размере 1%. Со временем этот процент снизился до 4% в год из-за большого объема предложений. Чаще всего займы брали представители аристократии и богатая молодежь.

Большинство богатых римлян охотно принимали участие в кредитных операциях, давая деньги под проценты через подставных лиц. Известно, что этим занимались Брут и Сенека в Британии. Чтобы обойти закон о запрете ростовщичества, долговое обязательство писалось на сумму, превышавшую реально получаемую. Во времена республики ростовщические операции могли стоить репутации гражданам Рима и поэтому Цицерон предостерегал против них. Обычные лица, желающие обогатиться за счет предоставления займов под проценты, поручали эти операции банкиру (аргентарию) или меняле (нуммуларию), которые и осуществляли их на профессиональном уровне. Собственно кредитной деятельностью занимались аргентарии, а деятельность нуммуляриев заключалась в проверке монет на их подлинность (probatio nummorum), отсюда и происходит их название (от лат. nummus - серебряная монета).

16.2.4. Китай

На возникновение в Китае различных финансовых инструментов, служивших безналичной формой оплаты, повлияло много факторов, в т.ч. и немалый вес денег. Ли Гоу в своем трактате «О государственном управлении» (XI в.) писал, что функцию денег сначала выполняли драгоценные камни, золото и серебро. Из-за большой стоимости они были неудобными для мелких расчетов, поэтому были введены монеты (цзянь). Их изготавливали не из драгоценных металлов, а из меди (а позже, во времена династии Сун, - из железа). При этом денежной единицей был не отдельный цзянь весом 3.5 грамма, а связка из 1000 монет, которая, соответственно, имела вес 3.5 кг. Путем изъятия из связки определенного количества монет осуществлялись точные расчеты, особенно при мелких коммерческих операциях. Однако главным неудобством таких связок был их вес, значительно осложнявший транспортировку больших сумм.

Во времена династии Тан (618 - 907 гг.) стали применяться подобные векселю ценные бумаги - **фейцзянь** («летающие деньги»). Чтобы не возить с собой значительные суммы денег, имеющих немалый вес, купцы могли их сдавать в цзиньцзоуянь (представительства местной администрации), получив взамен фейцзянь и уплатив 10% от суммы («плата за перевод денег»). Для получения денежной наличности во время путешествия по Китаю достаточно было предъявить этот документ другому представительству администрации.

Во времена династии Сун (XI в.), наряду с фейцзянь, появились и другие ценные бумаги: **бинцзянь** («удобные деньги»), **цзяоцзы** (синцзянь цзяоцзы – «те, которые можно обменять на деньги») и др. Они постепенно превратились в самостоятельное средство оборота и стали выполнять в Китае функции денег. В 1256 г. было принято решение о выпуске бумажных ассигнаций исключительно центральным правительством. Так завершился процесс преобразования кредитных ценных бумаг в денежные знаки.

В Европе о китайских бумажных деньгах узнали еще в конце XIII в. от Гильома де Рубрука и Марко Поло, видевших их при дворе монгольских правителей. Как отмечал Гильом де Рубрук (1220-1293 гг.), в Китае функцию монет выполняли кусочки бумаги из хлопка шириной и длиной в ладонь. Марко Поло (1254-1324 гг.) в отдельной главе своей книги «Банковские билеты, которые выпускает великий хан» подробно описал внешний вид и способ изготовления бумажных денег на монетном дворе великого хана, а также особенности их оборота. Его свидетельства долго оставались основным источником информации о бумажных деньгах в Китае.

16.2.5. Исламские страны Востока

Исламскому миру давно были известны такие разновидности финансовых инструментов, как **суфтаджа** (вексель на предъявителя, кредитный вексель) и **сакк** (прообраз будущего чека). Развитию кредитных операций и получению прибыли от них способствовало отличие цен на товары в разных частях халифата, а также большое количество наличных денег в виде золотых и серебряных монет, порождавшее естественное стремление к выгодному их вложению. Для этих целей обычно пользовались услугами банкиров. Необходимо учесть и такое обстоятельство, как ухудшение качества монеты на рубеже X-XI вв., что способствовало поиску безналичных форм расчета и кредита.

В частности, в Исфахане в 1052 г., по свидетельству персидского путешественника Насира-и-Хусрау, было не менее 200 банкиров, а в Багдаде они занимали отдельную улицу. Банкирское дело в арабских странах развивалось быстро, и большие суммы денег платились в виде чеков (sakk), гарантировались богами (khatt) и передавалась с помощью аккредитивов - суфтаджи (suftadja) в дальние страны без риска. В Басре - известном портовом городе - банкирское дело приобрело такое развитие, что каждый купец имел свой счет у банкира и расплачивался на базаре лишь чеками, выписанными на имя своего банкира (хатт-и сарраф).

16.2.6. Средневековая Европа

После распада Римской империи в хозяйственной жизни Европы наступил период упадка, что привело к угасанию кредитного дела. В X-XII вв. начинается эпоха экономического подъема. В Европе, где четко выделились два полюса - юг и север (города Италии и немецкие города Ганзейского союза), значительно

активизировалась торговля.

Поскольку вся жизнедеятельность средневековых государств, в том числе и хозяйственная, в значительной мере зависела от церкви, в Европе доминировал канонический подход к любой экономической деятельности, согласно которому источником средств существования может быть только личный труд. Заем под процент был строго запрещен, т.к. «деньги не могут порождать деньги». Эта идея опиралась на евангельское изречение о том, что давая заем, не следует ждать от него вознаграждения (Евангелие от Луки, 6, 35). Церковным запретам кредитной деятельности способствовало и то, что денежными займами пользовались, как правило, люди, находившиеся в затруднительном положении. Поэтому распространенным было мнение, что богатый кредитор в форме процента забирает у бедного должника последние гроши, увеличивая таким образом свое богатство. Церковь беспощадно боролась против кредитной деятельности и, как отмечал М. Вебер, не одного купца заставила возвратить проценты.

Сначала ограничения кредита под проценты касались лишь духовенства, которому Никейским собором в 325 г. было запрещено получать таким образом прибыль. Позднее, в IX в., получение процента от займа было объявлено греховным для всех. Соответствующее постановление канонического законодательства появляется в 1173 г. В нем папа Александр III угрожал ростовщикам отлучением от церкви и запрещал прибыльные коммерческие соглашения. В 1243 г. Григорий X предлагал изгнать ростовщиков из городских общин, а Климент V в 1311 г. объявил недействительным любое светское законодательство, противоречащее церковному запрету на получение процента. Таким образом, ростовщическая деятельность стала рассматриваться как преступление, подобное всем другим преступлениям.

Этим средневековое мировоззрение существенно отличалось от античного - греки и римляне презирали труд как занятие низкое, достойное лишь рабов. Негативное отношение к финансово-кредитной деятельности со стороны канонического церковного права ощутимо сдерживало развитие финансово-кредитных операций. В связи с этим роль ростовщиков была передана евреям как лицам другой веры, хотя это не мешало большим монастырям и аббатствам тоже выполнять роль кредитных учреждений.

По версии некоторых авторов (Дупиуса де ля Серра, Жака Савари, Вернера Зомбарта) изобретателями векселя стали евреи - постоянно гонимая нация не только в Древнем Египте, но во Франции, Испании, Португалии и др. Поселившись в Ломбардии (Италия), евреи нашли способ переводить свои капиталы с помощью специальных тайных писем, составленных в кратких и точных выражениях и передававшихся через иностранных купцов. Первый (по мнению В. Зомбарта) вексель был выдан в 1207 г. Симоном Рубеном, а во многих итальянских городах (в частности Венеции XVI в.) вексельное дело было полностью сосредоточено в руках евреев.

По другой популярной версии происхождение векселя связано с Крестовыми походами. В соответствии с ней вексель возник из-за необходимости пересылки в папскую казну огромных ценностей, захваченных крестоносцам, знакомству с торговыми обычаями стран Востока, а также в связи с деятельностью ордена тамплиеров, возникшего вследствие Крестовых походов. Если сначала финансовая деятельность тамплиеров была направлена на то, чтобы оказывать материальную поддержку паломникам в Палестине, то в XII в. возник обычай предоставлять деньги в долг путешественникам (первый известный случай такого займа датируется 1135 г.). Объемы кредитной деятельности расширились, и во время Крестового похода финансовыми услугами ордена пользовались король Людовик VII (1120-1180 гг.) и папа Александр III (1105-1181 гг.). По количеству и объему кредитных операций орден тамплиеров находился, бесспорно, на первом месте среди других орденов (тевтонского, францисканского, иоаннитского), а в конце XII в. он уже представлял собой крупнейшее банковское учреждение Европы с двумя центральными конторами (так называемыми *templum*) в Париже и в Лондоне, а также с многочисленными отделениями во французских городах и средиземноморских странах.

Первая научная теория происхождения векселя возникла в начале XIX в. и принадлежала Францу-Августу Бинеру (1787-1861 гг.), по которой вексель – изобретение итальянцев. Он обосновывал свою теорию тем, что первые известные к тому времени вексельные документы происходили из Италии. Кроме того, в Италии был изобретен бухгалтерский учет, а камбисты (первые авторы работ о вексельных операциях) также были итальянцами. Наконец, вся вексельная терминология (акцепт, индоссамент, жиро, аваль, трассант, римесса, авизо) имеет итальянское происхождение.

Из первоначальной долговой расписки вексель приобрел популярность при проведении операций по обмену валют. Многочисленные мелкие государства и независимые торговые города в Италии имели право выпускать собственную монету, однако в большинстве случаев правители этих государств и городов стремились к фальсификации монет, уменьшая их вес при чеканке. Именно поэтому необходимо было проверять вес, качество металла и даже достоверность чеканки большинства из этих монет. Первые конторы менял появились в Италии в XI в. Сотрудники этих контор осуществляли свои операции на рынках за специальными столами (**banco**), и поэтому их называли **banchieri**. Отсюда и происходят понятия «банкир» и «банк». Меняла, получив денежные средства, выдавал долговую расписку, платеж по которой можно было получить в другом месте.

Известно, что менял (и евреев, и итальянцев) не очень любили в городах Европы, поскольку они часто занимались ростовщичеством, предоставляя займы под проценты. Такие менялы нередко выгонялись из разных городов, а их имущество подлежало конфискации. При этом евреи преследовались больше, чем другие народы, и поэтому в XIII—XIV вв. обменная деятельность в Европе постепенно сосредоточилась в руках итальянцев. Постепенно ремесло итальянских менял проникло в другие страны Европы, в частности через Фландрию оно попало в Германию.

В XIV-XV вв. итальянские менялы создали первые банкирские компании, контролировавшие финансово-кредитные операции в большинстве государств Европы. Это флорентийские семейные банкирские общества Барди, Перуччи, Медичи, а также известные в то время компании Ачаюоли и Уццано, занимавшиеся депозитными и заемными операциями и предоставлявшие кредиты в валюте любого западноевропейского государства.

Поскольку в обороте находились монеты разного типа, а денежная система итальянских городов была достаточно сложной, упомянутые в контрактах и бухгалтерских записях условные денежные единицы редко соответствовали тем, что реально были в ходу. Поэтому одновременно с развитием торговых отношений возникла потребность упростить платежи и облегчить перевод денег в другие страны, что вызвало объективную необходимость в использовании **lettera di cambio** - векселей. Пример одного из векселей того времени:

1494 год, 9 августа, Венеция.

В соответствии с этим настоящим первым экземпляром векселя уплатите Людвигу де Франческо из Фабриано и Ко 100 унций неаполитанским золотом, которые вы сможете получить в таком же количестве на следующей ярмарке в Фулиньи от уважаемого Донато, сына Приамо. Запишите ту сумму на наш счет.

Пусть бережет вас Бог.

Ниже подписываюсь, ваш Паганино де Паганини из Брекчи.

С помощью векселей кредитные компании находили новые способы избегания церковных запретов. Благодаря своей гибкости и удобству вексель быстро распространился по Европе. Увеличение объемов вексельных операций потребовало законодательного закрепления сложившихся обычаев делового оборота, и в 1569 г. в Болонье был принят первый Вексельный устав.

Наряду с векселями в XVII в. в обращении при совершении сделок стали появляться чеки. Изначально они назывались **drawn note**, т.к. писались от руки, и позволяли клиенту использовать средства, которые он имел на счету в банке. В одном из самых ранних сохранившихся чеков от 16 февраля 1659 г. содержится обращение к банкирам лондонского Сити Моррису и Клейтону об уплате 400 фунтов.

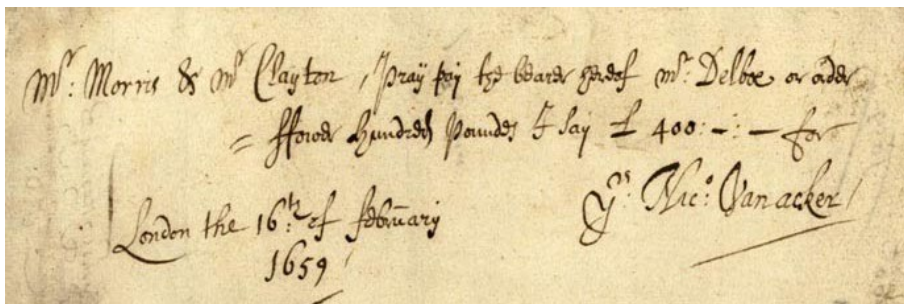


Рис.16.2. Один из первых чеков

В 1717 г. Банк Англии впервые стал использовать заранее напечатанные формы чеков с целью предотвращения мошенничества. В 1811 г. коммерческий банк Шотландии, скорее всего, стал первым банком, который персонализировал чеки своих клиентов, печатая имя владельца счета вертикально вдоль левого края. В 1830 г. Банк Англии стал выдавать клиентам чековые книжки на 50, 100 и 200 бланков.

16.2.7. Древняя Русь и Россия

Первые упоминания о векселях известны еще в XVII в. (хотя это были, скорее всего, иностранные векселя). Они содержатся в Боярском приговоре от 31.08.1697 г., который можно считать первым в России законодательным актом, касавшимся вексельных операций, и приказе купцу Сергею Лабазному «О сборе в Московской большой таможене пошлин», датированном 29.08.1698 г. Оба документа запрещали использовать векселя при сборе таможенных налогов. В именном указе коменданту князю Гагарину от 7.09.1710 г. упоминаются векселя, составленные в России: указом запрещалось переводить с помощью векселей деньги для молодежи, учащейся за границей, поскольку (как отмечалось в приказе) слишком большое количество переведенных денег тратилось на развлечения, что не содействовало успехам в обучении.

Следует отметить, что кредитные операции, оформленные документально, были распространены еще в Древней Руси.

а) При раскопках в Новгороде и Пскове были найдены деревянные «доски» (XII – XV вв.), вероятно покрытые слоем воска, на которых острым предметом фиксировалась долговая зависимость купцов и других «торговых людей».

б) Одним из следствий татаро-монгольского влияния стало появление в Московской Руси института долговой **кабалы**. Первоначально слово «кабала» означало долговую расписку. Оно происходит от арабского слова *ka-bal* - договор купли-продажи, расписка, обязательство. В Московской Руси кабала (кабальный акт) представляла собой документ, которым оформлялось долговое обязательство. Постепенно произошло размежевание двух основных видов кабалы: **заемной** (разновидность долговой расписки) и **служилой**, предусматривающей работу должника на займодателя (с фиксированной заниженной оплатой) в счет долга. Именно второй вид кабалы приобрел наибольшее распространение, став причиной кабального холопства. Так кабала из долгового документа превратилась в соглашение о переходе во временное рабство с удержанием суммы долга.

Се аз Матвей Мартынов с сыном взяли мы у (монастырских) властей ссуды 15 р. А за то за ссуду жить мне во крестьянстве за монастырем.

В XVIII в. (под чутким руководством великого реформатора Петра I) постепенно происходит заимствование приемов вексельных операций. Очевидные преимущества использования векселей состояли в том, что их оформление (по сравнению с обычными долговыми письмами) не требовало ни свидетелей, ни поручителей, ни регистрации. Еще одним преимуществом векселя была лаконичность текста, отличающая его от традиционной формы заемной кабалы, текст которой занимал не меньше одной страницы и перечислял всех участников соглашения, их имена, местожительство и общественное положение.

Приведем пример лаконичного текста вексельного соглашения, составленного на русском языке между голландским купцом А. Розеном и Г. Гребиним из Гамбурга:

Я, нижеподписавшийся, обещаю платить на Москве по получении Гаску Гребину 25 рублей, которые я принял у него в Архангельске.

*22 января 1721 г.
Абрам Розен.*

В начале XVIII в. западноевропейскими купцами постепенно начинает использоваться практика вексельных операций и при кредитных соглашениях с русскими партнерами. Известны отдельные случаи, когда русские купцы обменивались векселями с иностранными купцами при посредничестве западноевропейских банков.

Завершился процесс становления русскоязычной формы векселя принятием первого российского Вексельного устава 1729 г. Согласно этому уставу преимущество векселей состоит в том, что: 1) можно избежать затрат на организацию перевозки денег; 2) этот способ перевода денег наиболее безопасный; 3) лица, торгующие векселями, получают прибыль; 4) даже монархи получают при необходимости денежные средства из других стран с помощью векселей. В целом же, использование векселей признавалось лучшим способом предотвратить вывоз золота и серебра за границу.

Современные платежные системы безналичной оплаты товаров и услуг, ориентированные на частных лиц, в основном, базируются на использовании пластиковых карт (банковских, дисконтных, предоплаты и т.п.) или [электронных денег](#).

16.3. Электронные платежи

16.3.1. Пластиковые карты

В начале XX в. альтернативным (к векселям и чекам) инструментом безналичной формы оплаты товаров и услуг стали **карточки**. В 1888 г. Эдуард Беллами (Edward Bellamy) в своей книге «Оглядываясь назад» (англ. *Looking Backward*) впервые употребляет термин «**кредитная карта**», под которой подразумевалась нечто похожее на карту социального страхования для начисления дивидендов гражданам от государства. В реальности же самая первая кредитная карточка была выпущена

General Petroleum Corporation California (сейчас Mobil Oil) в 1914 г. Владелец картонной карты получал значительные удобства в обслуживании и скидки при покупке товара на любой бензоколонке компании, а компания - постоянных клиентов и стабильные доходы.

В том же году аналогичные карты (потребительская платежная карта – англ. customer charge card) выпустила компания Western Union Telegraph Company. Так, одна из разновидностей таких карт выдавалась только членам правительства США и давала право отправлять телеграммы в кредит за счет правительства. На обратной части карты имеется надпись на этот счет – «Payment not being required from the sender at the time of transmission» («Оплата при передаче от отправителя не требуется»).

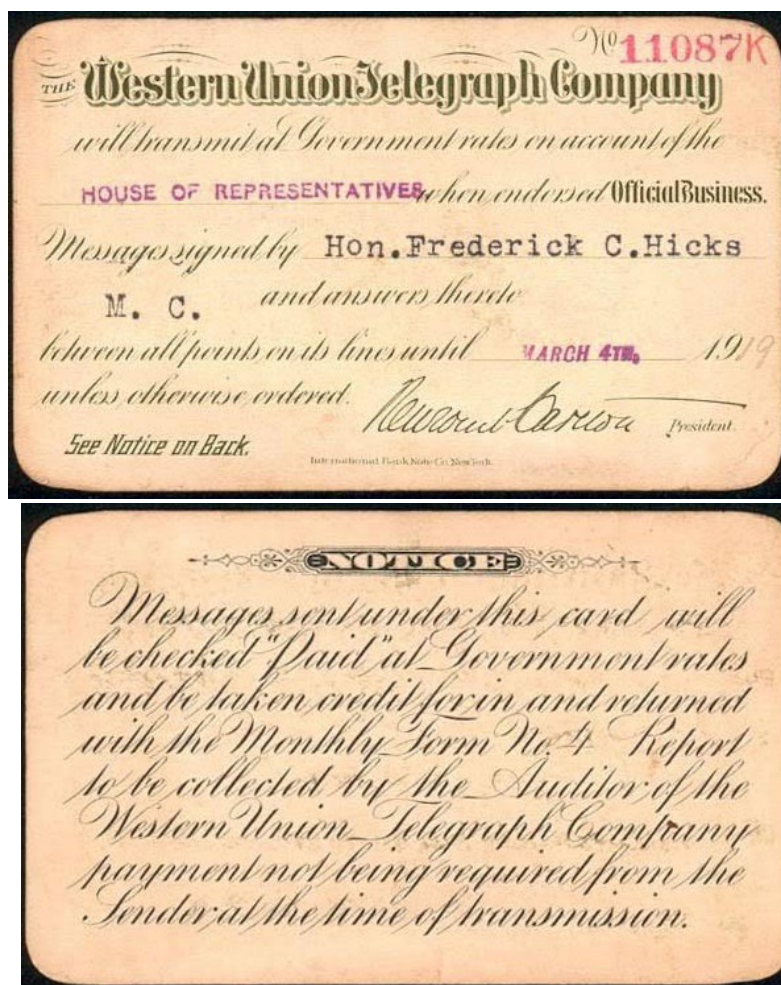


Рис.16.3. Карта Western Union для отправки телеграмм

Недолговечность картонных карточек заставила искать им замену, и через десять лет начали появляться первые металлические карточки с тиснением. Тиснение позволило частично автоматизировать процесс обслуживания этих карт, поскольку с них можно было делать оттиски и переносить информацию о владельце на отпечатанные чеки, что позволило вести учет и регистрацию продаж по каждой из них. В 1928 г. компания Charga-Plate начала выпуск металлических карт, на которых были указаны имя и адрес клиента.





Рис.16.4. Карта Charge-Plate

Первая банковская карта, по мнению многих специалистов, была придумана Джоном С. Биггинсом, который являлся экспертом по потребительскому кредитованию из Национального банка Флэтбуш в Нью-Йорке. В 1946 г. он положил начало работе по кредитной схеме «Charge-it». Эта схема строилась на расписках клиентов, которыми оплачивались покупки в магазинах. После того как покупка состоялась, магазин сдавал расписки в банк, и банк оплачивал их со счетов покупателей. В Флетбуше была впервые опробована классическая цепочка расчетов, которая по сей день используется в банковском карточном бизнесе.

В 1949 г. председатель Hamilton Credit Corporation Фрэнк Макнамара договорился с двумя своими приятелями, Альфредом Блумингдейлом и Ральфом Снайдером, создать компанию, кредитные карты которой принимали бы к оплате более чем в одной торговой сети. На идею создания таких карт Макнамара натолкнула неподобающая его статуса ситуация, когда, поужинав в своем любимом ресторане Major's Cabin Grill (Нью-Йорк), он обнаружил, что забыл бумажник дома. В результате ему пришлось звонить жене и просить, чтобы она привезла деньги в ресторан. Т.о. в 1950 г. появилась первая **универсальная платежная система**, получившая название Diners Club («Ресторанный (обеденный) клуб»).

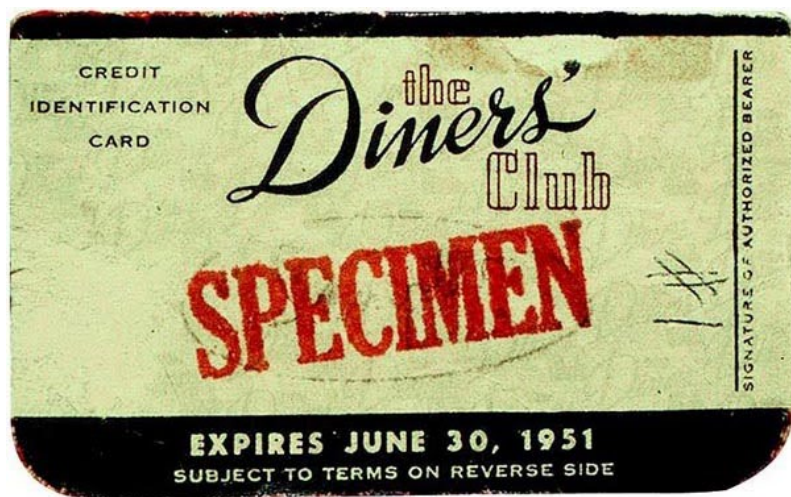


Рис.16.5. Карта Diners Club

Это название объясняется тем, что поначалу кредитные карты Diners Club бесплатно раздавались завсегдатаям 14 нью-йоркских ресторанов, расположенных поблизости от Empire State Building. Карты печатались на прямоугольнике из плотной бумаги со списком ресторанов на оборотной стороне. Держатель карты предъявлял ее в ресторане, тот передавал копии счетов в Diners Club, которая раз в месяц выставляла клиенту общий счет. Клиент расплачивался с Diners Club, а компания - с ресторанами. К концу 1950 г. у компании было около 20 тысяч клиентов, а карточки принимались в 285 ресторанах. В 1953 г. компания начала международную деятельность (Великобритания, Канада, Мексика и Куба), став первой международной платежной системой, работающей с кредитными картами, а в 1969 г. ее карты первыми стали приниматься в СССР. Компания заключила договор с ВАО «Интурист», которое организовывало расчеты по картам в валютных магазинах «Березка», ресторанах и гостиницах Москвы и Ленинграда.

Первая банковская карта была выпущена в 1951 г. (банк Franklin National Bank, Нью-Йорк), **первая пластиковая карта** - в 1959 г. (American Express), **первая пластиковая карта с магнитной полосой** - в 1970 г. (IBM, American Express и American Airlines), **первая смарт-карта** - в 1983 г. (France Telecom).

История создания, стандарты и устройство карт с магнитной полосой и смарт-карт рассмотрено в лекции «Протоколы аутентификации (идентификации)».

Пластиковые карты бывают трех **разновидностей**:

- кредитные;

- дебетовые;
- с разрешенным овердрафтом.

Кредитная карта (лат. credit - «он верит») - персонафицированный платежный инструмент, предназначенный для совершения операций (получения наличных денег в банкоматах, оплаты товаров и услуг), осуществляемых исключительно за счёт денежных средств, предоставленных банком клиенту в пределах установленного лимита в соответствии с условиями кредитного договора. Карта является «персонафицированной», т.к. содержит информацию, включающую номер карты или банковского текущего счета, имя и фамилию владельца, срок годности карты (даты начала и конца срока) и т.д. Кредитная карта может заменять потребительские кредиты и кредиты на неотложные нужды. Главным преимуществом кредитных карт перед кредитами является возможность использования кредита, не отчитываясь перед банком о его целевом использовании, и возможность постоянного возобновления кредитной линии после погашения.

Дебетовая карта (лат. debet - «он должен») – аналогична кредитной, за исключение того, что расчеты по ней выполняются исключительно денежными средствами клиента, имеющимися на депозитном счёте, привязанному к карте.

Карта с разрешённым овердрафтом нечто среднее между кредитной и дебетовой картами. **Овердрафт** (англ. overdraft - сверх планируемого, перерасход) - кредитование банком расчётного счёта клиента (в пределах установленного лимита) для оплаты товаров и услуг при недостаточности или отсутствии на расчётном счёте клиента денежных средств.

Принимающие карту предприятия торговли и сервиса, а также отделения банков образуют **платежную (приемную) сеть**. В настоящее время пластиковые карты являются наиболее распространенной формой безналичной оплаты. О популярности пластиковых карт говорит тот факт, что в Европе в 2003 г. их было в обращении 938 на 1 000 жителей, а по каждой из них было в среднем осуществлено 38,6 операций за год.

Существенным недостатком карт с магнитной полосой является то, что ее достаточно легко подделать, а PIN-код, который должен быть известен только владельцу карты и необходим для получения наличных денег в банкоматах, можно выяснить различными способами.

Другой существенный недостаток - карта при каждом платеже полностью идентифицирует своего владельца. Если владелец карточки использует ее для покупки билетов на транспорт, то можно отследить все его поездки, что в цивилизованном обществе без санкции прокурора недопустимо. Аналогичным образом, для каждого владельца карт можно собрать информацию о том, какие товары и где он покупает, какими услугами пользуется, какие культурно-зрелищные мероприятия посещает и т.д.

Устранить последний недостаток призваны так называемые **электронные кошельки** и **карты предоплаты/карты с хранимой стоимостью** - карты, позволяющие хранить в своей памяти определенную «сумму» (деньги, минуты, литры, поездки), тратить которую можно безо всякой авторизации. Естественно данная «сумма» предварительно должна быть «положена в кошелек». Электронные кошельки также не лишены недостатков – как и для обыкновенного кошелька с настоящими деньгами, если его украли, то деньги, имеющиеся на текущий момент в кошельке, можно считать потерянными.

16.3.2. Суррогатные платежные средства в Internet

На заре электронных платежей через Интернет применялись различные типы суррогатов. Эти средства расчетов предлагались несколькими компаниями, наиболее известные из которых First Virtual Holdings и Software Agents. Электронные деньги в таких системах представлялись в виде **цифровых купонов и жетонов**. Клиент за наличный или безналичный расчет приобретал у «банка» на некоторую сумму последовательности символов (для них «банк» гарантировал **нетривиальность алгоритма генерации и уникальность каждого экземпляра**), которыми расплачивался с торговцем. Торговец возвращал их в «банк» в обмен на ту же сумму, за вычетом комиссионных. При этом на «банке» лежала обязанность контроля наличия жетона в реестре выданных и отсутствия в реестре поступивших обратно. При пересылке жетонов через Internet использовалось шифрование с открытым ключом.

Недостаток – идентификация владельца жетонов.

16.3.3. Расчеты пластиковыми карточками в Internet

В 1994 г. была основана компания CyberCash, первой предложившая технологию, позволяющую использовать пластиковые карточки для расчетов в Сети. Предлагаемое этой компанией программное обеспечение использует криптозащиту с открытым ключом для конфиденциальной передачи данных о пластиковой карточке от покупателя к торговцу. При этом все реальные расчеты и платежи производятся средствами процессинговых компаний¹ без использования Internet. За CyberCash последовали и другие, а кульминацией этого процесса стало соглашение о совместной деятельности по предоставлению расчетных услуг в Internet, заключенное 9 января 1995 г. между MasterCard и производителем коммуникационного программного обеспечения Netscape.

Рассмотрим порядок оплаты товаров и услуг с помощью платежной системы CyberCash. Предварительно покупатель должен загрузить общедоступное программное обеспечение CyberCash Vallet через Интернет – программу, устанавливающую соединение между покупателем, продавцом и их банками.

1. Выбрав товар, покупатель нажимает на кнопку CyberCash «PAY» панели продавца.
2. Продавец посылает покупателю счет, который содержит информацию о покупке, отображаемую на экране дисплея покупателя.
3. Покупатель добавляет или выбирает из списка номер используемой для оплаты кредитной карточки и указывает дополнительные сведения.
4. Вся эта информация снабжается электронной подписью покупателя, реализуемой посредством программы CyberCash, шифруется и передается продавцу вместе с хеш-кодом счета.
5. При получении этого сообщения, продавец добавляет к нему информацию для авторизации банком, которая шифруется, снабжается электронной подписью продавца и пересылается серверу CyberCash.
6. Сервер CyberCash аутентифицирует подписи для подтверждения того, что покупатель и продавец согласились с корректностью счета и правильностью суммы стоимости сделки.
7. Сервер CyberCash переадресует соответствующую информацию в банк, сопровождая ее запросом на производство платежа в пользу продавца, включая его авторизацию.
8. Банк дешифрует и обрабатывает полученную информацию, после чего осуществляет соответствующую операцию с кредитной карточкой.
9. Отклик банка передается серверу CyberCash, который присылает продавцу электронную квитанцию, часть которой продавец переадресует покупателю.

Для генерации ЭЦП используется RSA, сообщения шифруются DES, хеш-коды вычисляются по алгоритму MD5.

Недостаток – идентификация владельца пластиковой карты.

¹**Процессинговая компания** - 1) фирма, координирующая разрозненные процессы; 2) компания, координирующая расчеты по кредитным картам между эмитентом карты (банком, выпустившем карту), эквайером (банком, ведущим расчеты с торговлей), торговой фирмой и пользователем кредитной карты.

16.3.4. Электронные кошелки в Internet

Рассмотрим платежную систему с использованием электронных кошелеков на примере первой такой системы в русскоязычном Интернете – Webmoney (1998 г.).

- 1. Пользователь скачивает с сайта приложение для Windows, мобильного телефона или браузерную версию.
- 2. Пользователь через программу регистрируется (ФИО, дата рождения, адрес, e-mail, номер мобильного телефона) и ему присваивается 12-значный идентификатор (WMID) и высылается файл-ключ, на доступ к которому пользователь назначает пароль. Обмен информации выполняется через SSL².
- 3. Каждый пользователь может получить в качестве удостоверения своей личности перед другими пользователями системы WM-аттестат (в том числе и анонимный). Проверить аттестат любого пользователя системы можно в центре аттестации WMT.
- 4. Пользователь заводит электронные кошелки, каждый из которых предназначен для расчетов в строго определенной валюте. Пополнить кошелек можно несколькими способами: банковским переводом со своего расчетного счета, наличными через кассы коммерческих банков и Сбербанка, через платежные терминалы и автоматы по приему наличных, с помощью купленных WM-карт и др.
- 5. Пользователь может переводить деньги из одного кошелька в другой (как свой, так и другого пользователя системы Webmoney), но в пределах одной валюты и с учетом взимаемой комиссии.
- 6. Обналичить деньги с электронного кошелька можно через открытый счет в банке (например, Сбербанк), специализированные системы (например, Контакт), аттестованные пункты обмена и др.
- 7. При оплате товаров и услуг покупатель сообщает продавцу свой WMID и номер кошелька, для которых продавец выставляет счет. Получив в WM-программе счет, покупатель подтверждает оплату или отказывается от нее.
- 8. Упрощенная процедура оплаты без выписки счета (например, за игры, программы, фильмы) возможна непосредственно на сайте продавца через сервис WM Merchant. В этом случае вся процедура оплаты занимает считанные секунды. Покупатель формирует на сайте свой заказ, после чего его перенаправляют на <http://merchant.webmoney.ru>, где он авторизуется с помощью WM-программы и подтверждает свое желание оплатить указанную сумму в пользу указанного WMID (продавца). Там же покупатель выбирает свой кошелек, с которого совершает платеж.

Для процедур аутентификации, шифрования, проверки целостности и т.д. используются алгоритмы и протоколы RSA, RC5³, MD4, MD5 и SSL.

Недостаток – идентификация покупателя.

²**SSL** - криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером на базе асимметричного шифрования.

³**RC5** - блочный шифр, изобретенный Р.Ривестом.

16.3.5. Цифровые деньги

Преимущества и, в первую очередь, недостатки различных форм безналичной оплаты привели известного голландского математика Дэвида Чома (англ. David Chaum) в 80-х гг. к идее применения цифровых денег, обладающих свойством неотслеживаемости. В 1994 г. возглавляемая им компания DigiCash представила технологию сетевых электронных денег «ecash».

Цифровые деньги - числа, использованные в качестве денежных знаков. Поскольку число как таковое представляется последовательностью битов, которая может существовать в неограниченном количестве неотличимых друг от друга копий, очевидно, ключевую роль в любой технологии обеспечения цифровых платежей является предотвращение копирования «банкнот» и их повторного использования.

В протоколе электронного платежа задействованы три участника, которых будем называть: банк, покупатель (клиент) и продавец. Покупатель и продавец, имеют счет в банке, а покупатель желает заплатить продавцу за товар или услугу. Рассмотрим основные моменты взаимодействия банка, покупателя и продавца.

Этап 1. Снятие наличных со счета.

Таблица 16.2. Снятие наличных со счета

№ п/п	Описание операции	Пример
1	В ходе сеанса связи клиент и банк (точнее, их программы-представители) аутентифицируют друг друга.	
2	Клиент генерирует уникальный номер «монеты» m .	$m = 3$
3	Выбирает случайное число r и отправляет сообщение $m' = (r^e * m) \bmod n$, где e и n – открытый ключ банка. Кроме этого клиент сообщает банку, каким должен быть номинал этой монеты.	$r = 5$ $m' = (5^5 * 3) \bmod 91 = 2$
4	Банк заверяет «монету» $s' = (m')^{d_1} \bmod n$ и отправляет s' клиенту. В данном выражении d₁ – секретный ключ банка, соответствующий запрошенному номиналу «монеты».	$s' = 2^{29} \bmod 91 = 32$
5	Банк уменьшает счет клиента на номинал «монеты».	
	Клиент вычисляет цифровую подпись банка s для исходного номера «монеты» m исходя из уравнения $(s * r) \bmod n = s'$ (в литературе	$(s * 5) \bmod 91 = 32$

В данной схеме r^e – «закрывающий множитель» (англ. blinding factor). За счет применения данного множителя банк не знает номер подписываемой «монеты», но оставляет клиенту цифровую подпись для «монеты» с этим номером. Использование «закрывающего множителя» и составляет основу «слепой (затемненной) подписи», предложенной Чомом. Благодаря использованию этой подписи банк не в состоянии установить клиента, производящего оплату данной монетой, но в то же время сохраняет возможность следить за однократным использованием каждой «монеты».

«Открытая подпись» - $s = m^{di} \bmod n = 3^{29} \bmod 91 = 61$.

Подпись s , полученная в результате открытого подписания сообщения m и слепого подписания сообщения m' , идентична.

Этап 2. Платеж.

1. Для оплаты товаров или услуг покупатель передает продавцу номер «монеты» m и цифровую подпись к ней s .
2. Продавец пересылает эту информацию в банк или на свой страх и риск оставляет ее у себя, чтобы потом переслать.
3. Банк проверяет свою подпись под «монетой» и факт ее использования в первый раз. Если «монета» проходит проверки, то продавцу сообщается номинал монеты, а номер «монеты» заносится в регистр использованных.
4. Продавец считает оплату произведенной, при этом может дать покупателю сдачу наличными.
5. Банк перечисляет сумму, эквивалентную номиналу «монеты», на счет продавца.

Следует подчеркнуть один важный момент - покупатель не может быть идентифицирован даже при сговоре продавца с банком.

Этап 3. Пополнения счета за счет цифровых денег.

Клиент связывается с банком и отправляет ему полученную «монету» (m и s), закрыв ее открытым ключом банка. Банк проверяет, не была ли она уже использована, заносит номер в регистр использованных и зачисляет соответствующую сумму на счет клиента.

Несмотря на все преимущества цифровых денег, отметим все же один недостаток. Т.к. «монеты» (m и s) до использования необходимо где-то хранить (на цифровом носителе), то существует вероятность их кражи.

Первой платежной системой в России на основе технологии «ecash» стала PayCash, реальные финансовые операции с использованием которой начались в декабре 2000 г. В 2002 г. по технологии PayCash была запущена система Яндекс.Деньги, насчитывающая миллионы пользователей в зоне ru. Яндекс.Деньги стала первой системой, которая получила банковское свидетельство на территории Российской Федерации, позволяющее осуществлять Интернет - платежи.

16.3.6. Биткойн [17, 60, 61, 62]

16.3.6.1. Общие сведения

Биткойн (англ. Bitcoin, от bit – бит и coin – монета) – децентрализованная электронная платёжная система (сеть), использующая одноимённую единицу для учёта операций и одноимённый протокол передачи данных. Под словом «децентрализованная» понимается, что сеть Биткойн не имеет каких-либо специализированных центров для выпуска новых монет, обработки транзакций (платежей, операций) или хранения средств. Данные функции может выполнять любой участник платежной системы. Единица учета операций (монета) сокращённо обозначается **BTC**.

16.3.6.2. Краткая история

В 1983 г. Дэвид Чом и Стефан Брэндс (англ. Stefan Brands) предложили первые протоколы «электронной наличности».

В мае 1997 г. Адам Бак (англ. Adam Back) для противодействия отправке спама и DoS-атакам предложил Hashcash, основанную на системе доказательства выполнения работы.

В 2008 г. человеком или группой людей под псевдонимом Сатоши (Сатоши) Накамото (англ. Satoshi Nakamoto) был опубликован файл с описанием протокола и принципа работы платёжной системы в виде одноранговой сети.

Первый блок (первые 50 BTC) был сгенерирован 3 января 2009 г. Первая транзакция по переводу BTC произошла 12 января 2009 г. – Сатоши Накамото отправил Хэлу Финни 10 BTC. Первый обмен BTC на национальные деньги произошёл в сентябре 2009 г. – Марти Малми отправил пользователю с псевдонимом NewLibertyStandard 5050 BTC, за которые получил на свой счёт в PayPal 5.02 \$. Первый обмен BTC на реальный товар произошёл в мае 2010 г. – американец Ласло Ханеч за 10 000 BTC получил две пиццы с доставкой.

16.3.6.3. Блокчейн

Хранение информации в Биткойн организовано по технологии блокчейн. **Блокчейн** (англ. blockchain) – децентрализованная реплицированная база данных¹ в виде непрерывной последовательной цепочки связанных блоков, содержащих информацию определенного рода. В случае с Биткойн – это информация о создании новых BTC и их движении между участниками платежной системы (транзакциях).



Отдельный блок Биткойн состоит из двух частей – заголовка и списка транзакций. На облегченный узлах в блокчейне могут храниться только заголовки.

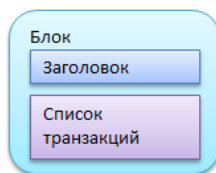


Рис.16.7. Обобщенная структура блока Биткойн

Заголовок блока обеспечивает связность цепочки и эффективную защиту от искажений и подмены данных. Для защиты в Биткойн активно используется асимметричное шифрование (электронная цифровая подпись на эллиптических кривых) и хеширование. Несмотря на использование цифровой подписи, в Биткойн обеспечивается полная анонимность платежей.

¹**Репликация** (англ. replication) – механизм синхронизации (приведения к одинаковому состоянию) содержимого нескольких копий объекта (например, базы данных, блокчейна и т.п.).

Децентрализованная реплицированная база данных (англ. decentralized replicated database) – база данных, копии которой размещаются в различных узлах компьютерной одноранговой сети и имеющие одинаковую силу (достоверность).

16.3.6.4. Сеть

Платежная система Биткойн функционирует на базе **пиринговой** (англ. peer-to-peer, p2p – равный к равному) **сети** – оверлейной² компьютерной сети, основанной на равноправии участников (т.е. каждый узел такой сети может быть как клиентом, так и сервером). **Узлом** сети Биткойн может быть любой компьютер (вычислительное устройство), подключаемый к сети и использующий p2p-протокол, позволяющий узлам общаться между собой и распространять информацию о транзакциях и блоках. Различают полные и облегченные узлы:

- **полный** – узел, который обеспечивает работу сети в соответствии со всеми принятыми правилами Биткойн и хранит полную версию блокчейн. Полная версия блокчейн содержит всю информацию о блоках и транзакциях, включая неподтвержденные. На начало сентября 2018 г. ее объем составлял более 210 Гб [http://bitinfocharts.com/ru/bitcoin]. В режиме реального времени полные узлы загружают каждый блок или транзакцию и проверяют их на соответствие требованиям Биткойн. Если блок или транзакция нарушают требования, то они отвергаются и в течение некоторого времени узел перестанет «замечать» их источник;

- **облегченный, SPV** (англ. Simplified Payment Verification - упрощенная проверка платежей) – узел, используемый клиентами сети для управления собственными Биткойн-кошельками. Облегченные узлы содержат, как правило, усеченную версию блокчейн, состоящую только из заголовков блоков. Объем усеченного блокчейна на начало сентября 2018 г. составлял более 40 Мб.

Помимо описанных функций, узел любого типа может использоваться для генерации блоков блокчейн (майнинга) и собственных транзакций, поддержания связности сети и ретрансляции данных (блоков и транзакций).

Особенности сети Биткойн:

- все узлы равноправны;
- узлы могут подключаться к сети и отключаться от неё в любое время;
- сеть имеет случайную топологию;
- неактивные узлы забываются через 3 часа;
- специальный протокол, работающий через TCP-порт 8333.

При подключении нового узла к сети он обращается на адрес конкретного активного узла с запросом сообщить ему об адресах других активных узлов. После получения списка новый узел повторяет указанную процедуру необходимое ограниченное количество раз, становясь полноправным участником сети Биткойн.

²**Оверлейная сеть** (англ. overlay - наложение) – общий случай логической сети, создаваемой поверх другой сети (в частности Интернет).

16.3.6.5. Адрес

Для выполнения платежей в сети Биткойн узел в определенный момент времени должен обладать определенным Биткойн-адресом.

Биткойн-адрес (англ. Bitcoin address, BTC-address) – идентификатор счета, с помощью которого могут выполняться транзакции (операции по переводу/добыче BTC). С каждым адресом в определенный момент времени связано определенное количество BTC, хранящихся на нем. В настоящий момент наиболее популярными являются два формата адресов:

- **P2PKH** (англ. Pay to Public Key Hash – плата по хешу открытого ключа) - начинается с 1 (например, 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2);
- **P2SH** (англ. Pay to Script Hash – плата по хешу скрипта) – начинается с 3 (например, 3J98t1WpEZ73CNmQviecnyiWrnqRhWNLY).

Биткойн-адреса могут формироваться с помощью программного обеспечения, установленного на компьютере пользователя, или с помощью онлайн-генераторов. В виду того, что в результате формирования адреса генерируется также конфиденциальная информация (закрытый ключ), второй способ с точки зрения приватности считается менее надежным.

Один и тот же человек может создать неограниченное количество адресов, повышая уровень анонимности своих платежей. Более того, рекомендуется для каждой

транзакции создавать новый адрес.

Процедура формирования Биткойн-адреса приведена в следующей таблице.

Таблица 16.3. Формирование Биткойн-адреса в формате P2PKH		
№ п/п	Описание операции	Пример
1	Формирование закрытого d и открытого Q(x_q, y_q) ключей по алгоритму ECDSA с кривой secp256k1 ¹⁾ .	d = 18 E1 4A 7B 6A 30 7F C8 6A 94 F8 11 47 01 E7 C8 E7 74 E7 F9 A4 7E 2C 20 35 DB 29 A2 06 32 17 25 x_q = 50 86 3A D6 4A 87 AE 8A 2F E8 3C 1A F1 A8 40 3C B5 3F 53 E4 86 D8 51 1D AD 8A 04 88 7E 5B 23 52 y_q = 2C D4 70 24 34 53 A2 99 FA 9E 77 23 77 16 10 3A BC 11 A1 DF 38 85 5E D6 F2 EE 18 7E 9C 58 2B A6
2	Формирование открытого ключа адреса в виде строки e = 0x04 + x _q + y _q .	e = 04 50 86 3A D6 4A 87 AE 8A 2F E8 3C 1A F1 A8 40 3C B5 3F 53 E4 86 D8 51 1D AD 8A 04 88 7E 5B 23 52 2C D4 70 24 34 53 A2 99 FA 9E 77 23 77 16 10 3A BC 11 A1 DF 38 85 5E D6 F2 EE 18 7E 9C 58 2B A6
3	Хеширование открытого ключа адреса e по алгоритму SHA-256 ²⁾ .	hash₁ = SHA256(e) = 60 0F FE 42 2B 4E 00 73 1A 59 55 7A 5C CA 46 CC 18 39 44 19 10 06 32 4A 44 7B DB 2D 98 D4 B4 08
4	Хеширование по алгоритму RIPEMD-160 ³⁾ .	hash₂ = RIPEMD160(hash₁) = 01 09 66 77 60 06 95 3D 55 67 43 9E 5E 39 F8 6A 0D 27 3B EE
5	Добавление в начало байта идентификатора сети (0x00 – основная сеть; 0x6F – тестовая сеть).	net_hash₂ = 00 01 09 66 77 60 06 95 3D 55 67 43 9E 5E 39 F8 6A 0D 27 3B EE
6	Двойное хеширование по алгоритму SHA-256 для получения контрольной суммы.	CRC = SHA256(SHA256(net_hash₂)) = D6 19 67 F6 3C 7D D1 83 91 4A 4A E4 52 C9 F6 AD 5D 46 2C E3 D2 77 79 80 75 B1 07 61 5C 1A 8A 30
7	Добавление в конец net_hash₂ первых четырех байтов контрольной суммы CRC .	net_hash₂_crc = 00 01 09 66 77 60 06 95 3D 55 67 43 9E 5E 39 F8 6A 0D 27 3B EE D6 19 67 F6
8	Преобразование net_hash₂_crc в формат Base58 ⁴⁾ .	BTC-address = Base58(net_hash₂_crc) = 16 Uw LL 9R is c3 Qf Pq BU vK of Hm BQ 7w Mt jv M

Примечания.

1) Кривая secp256k1 ECDSA имеет вид $y^2 = x^3 + 7 \pmod p$, где $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF}$ ₁₆ = 115792089237316195423570985008687907853269984665640564039457584007908834671663₁₀.

2) **SHA-256** – алгоритм хеширования с длиной хеш-образа 256 битов.

3) **RIPEMD-160** (от англ. RACE Integrity Primitives Evaluation Message Digest) – алгоритм хеширования с длиной хеш-образа 160 битов, разработанный в Католическом университете Лувена.

4) **Base58** – вариант кодирования цифрового кода в виде буквенно-цифрового текста на основе латинского алфавита. Стандарт похож на Base64, но отличается тем, что в результатах нет не только служебных кодов, но и алфавитно-цифровых символов, которые могут человеком восприниматься неоднозначно. Исключены 0 (ноль), O (заглавная латинская o), I (заглавная латинская i), l (маленькая латинская L). В получаемой строке по формату Base58 важен регистр букв.

5) Создание и проверку Биткойн-адресов можно выполнить по адресу <http://gobittest.appspot.com/Address>.

6) Значение в колонке «Пример» приведены в шестнадцатеричной системе счисления за исключением BTC-address.

Как видно из таблицы, Биткойн-адрес – это модифицированное представление открытого ключа пользователя, полученного по алгоритму асимметричного шифрования (цифровой подписи) ECDSA. Закрытый **d** и открытый **e** ключи в дальнейшем используются для осуществления транзакций. Открытый ключ может быть представлен в несжатой (англ. uncompressed) и сжатой (англ. compressed) форме:

- **несжатый** открытый ключ начинается префикса 0x04, включает в себя координаты x_q и y_q и имеет длину 65 байтов;

- **сжатый** открытый ключ начинается с префикса 0x02 или 0x03, включает в себя только координату x_q и имеет длину 33 байта. Координата y_q может быть вычислена с помощью кривой secp256k1 по координате x_q . Т.к. левая часть уравнения кривой равна y^2 , это означает, что имеется два решения для y (с положительным и отрицательным значением). При хранении в бинарном виде знак числа кодируется первым битом. Соответственно, если y_q положительное число, то первый бит равен 0 (четный – англ. even) и префикс открытого ключа 0x02, иначе первый бит равен 1 (нечетный – англ. odd) и префикс открытого ключа 0x03.

Адреса и соответствующие им ключи хранятся в **Биткойн-кошельках** – специализированном программном обеспечении, располагающемся на компьютере пользователя или в сети. Второй вариант, как и в случае с онлайн-генераторами адресов, снижает приватность.

16.3.6.6. Транзакция

Транзакция – операция по переводу/добыче определенной суммы BTC. У каждой транзакции может быть несколько входов (минимум один) и несколько выходов (минимум один).

Вход – это ссылка на выход другой транзакции. С помощью входа может быть подтверждено, что транзакцию выполняет законный владелец BTC.

Выход – это информация о сумме и адресе, на который необходимо перевести BTC. Каждый выход транзакции может быть использован в качестве входа для следующей транзакции только один раз.

Сумма BTC, полученная со всех входов, должна быть полностью реализована (потрачена) в рамках текущей транзакции. Если сумма входов больше суммы выходов для перевода получателям, то остаток можно вернуть в виде «сдачи» на дополнительный выход, принадлежащий отправителю (владельцу), и/или в виде комиссии для майнера, который включил транзакцию в блок (блокчейн). Вся неизрасходованная на выходах сумма в рамках транзакции считается комиссией майнеру. Комиссия может быть нулевой, но тогда шансы на включение транзакции в блок (подтверждение перевода) значительно снижаются. В большинстве Биткойн-кошельков можно указывать размер комиссии (англ. fee – гонорар). Тогда разница между суммой входов и суммой выходов с комиссией будет возвращаться отправителю (владельцу) в виде «сдачи».

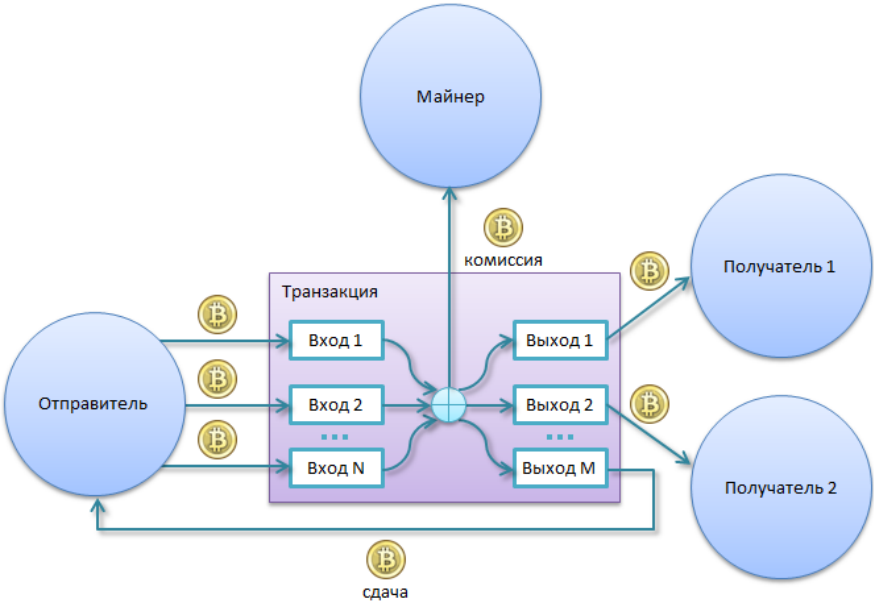


Рис.16.8. Схема перевода BTC в рамках транзакции

В следующих трех таблицах расписана структура транзакции, которая состоит из заголовка, списка входов и списка выходов. В последней колонке таблиц приведен пример пересылаемых/хранимых данных по транзакции в **raw-формате** (англ. raw transaction format – формат необработанных транзакций).

Таблица 16.4. Формат транзакции tx

Имя	Тип	Размер, байт	Назначение	Пример
version	целое, uint32_t*)	фиксированный, 4	Номер версии транзакции. В настоящее время версия 1. Записывается с обратным порядком следования байтов (little-endian).	01 00 00 00
tx_in_count	целое, compactSize uint (uint8_t..uint64_t)	переменный, 1..9	Количество входов в транзакции.	01
tx_in	список, txIn	переменный	Список входов.	см. табл. 16.5
tx_out_count	целое, compactSize uint (uint8_t..uint64_t)	переменный, 1..9	Количество выходов в транзакции.	01
tx_out	список, txOut	переменный	Список выходов.	см. табл. 16.6
lock_time	целое, uint32_t	фиксированный, 4	Время блокировки. Если менее 500 миллионов, время блокировки интерпретируется как высота (порядковый номер) блока. Транзакция может быть добавлена в любой блок с этой высотой или выше. Если значение больше или равно 500 миллионам, время блокировки интерпретируется как время в формате Unix (количество секунд, прошедших с 1970-01-01 00:00 UTC). Транзакция может быть добавлена в любой блок, время блокировки которого превышает время блокировки	00 00 00 00

			транзакции.	
--	--	--	-------------	--

Примечание.

*) Тип данных uint (от англ. unsigned int) предназначен для хранения положительных целых чисел. Число после uint указывает на размер поля в битах.

Таблица 16.5. Формат одного входа txIn

Имя		Тип	Размер, байт	Назначение		Пример
previous_output	outpoint txID	строка, char[32]	фиксированный, 32	Идентификатор выхода предыдущей транзакции, из которой берутся BTC для отправки.	Идентификатор предыдущей транзакции - двойной хеш предыдущей транзакции txID _{prev} =SHA256(SHA256(tx _{prev})). Хеш записывается с обратным порядком следования байтов (little-endian).	F3 A2 7F 48 5F 98 33 C8 31 8C 49 04 03 30 7F EF 13 97 12 1B 5D D8 FE 70 77 72 36 E7 37 1C 4E F3
	outpoint index number	целое, uint32_t	фиксированный, 4		Номер выхода в предыдущей транзакции. Нумерация выходов начинается с 0.	00 00 00 00
script bytes		целое, compactSize uint, (uint8_t..uint64_t)	переменный, 1..9	Количество байтов в скрипте подписи – максимум 10 000 байт.		6A (106 байтов)
signature script (scriptSig)		строка, char[]	переменный	Скрипт для подтверждения авторизации транзакции.		(<Sig> <PubKey>) 47 (71 байт – длина подписи ECDSA) 30 44 02 20 11 1A 48 2A BA 6A FB A1 2A 6F 27 DE 76 7D D4 D0 64 17 DE F6 65 BD 10 0B C6 8C 42 84 5C 75 2A 8F 02 20 5E 86 F5 E0 54 B2 C6 CA C5 D6 63 66 4E 35 77 9F B0 34 38 7C 07 84 8B C7 72 44 42 CA CF 65 93 24 01 (подпись ECDSA двойного хеша SHA-256 текущей транзакции*) с помощью закрытого ключа отправителя d _{отп} – Sig = ECDSA(SHA256(SHA256(tx _{сигт})), d _{отп}) 21 (33 байта – длина открытого ключа ECDSA отправителя) 02 82 00 6E 93 98 A6 98 6E DA 61 FE 91 67 4C 3A 10 8C 39 94 75 BF 1E 73 8F 19 DF C2 DB 11 DB 1D 28 (открытый ключ ECDSA отправителя PubKey = e _{отп})
sequence		целое, uint32_t	фиксированный, 4	Параметр, предназначенный для блокировки неподтвержденной транзакции. В настоящее время не используется. По умолчанию для Bitcoin Core равен 0xFFFFFFFF (блокировка отключена).		FF FF FF FF

Примечание.

*) Предварительно из текущей транзакции удаляются поля scriptSig всех входов и добавляется некоторая дополнительная информация – подробнее см. http://en.bitcoin.it/wiki/OP_CHECKSIG.

Таблица 16.6. Формат одного выхода txOut

Имя	Тип	Размер, байт	Назначение	Пример (для P2PKH-адреса)
value	целое, int64_t	фиксированный, 8	Количество «сатоси» ^{*)} , которое нужно потратить (перевести). Количество записывается с обратным порядком следования байтов (little-endian).	E0 FE 7E 01 00 00 00 00 (0.619 BTC)
pk_script bytes	целое, compactSize uint, (uint8_t..uint64_t)	переменный, 1..9	Количество байтов в скрипте подписи. Максимум – 10 000 байтов.	19 (25 байтов)
pk_script	строка,	переменный	Скрипт, определяющий условия по использованию BTC в последующих	(OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG) 76 (OP_DUP) A9 (OP_HASH160) 14 (20 байтов – длина двойного хеша открытого ключа получателя e _{пол}) 6B F1 9E 55 F9 4D 98 6B

(scriptPubKey)	char[]	транзакциях.	46 40 C1 54 D8 64 69 93 41 91 95 11 (двойной хеш открытого ключа получателя PubKeyHash = RIPEMD160(SHA256(e _{пол})) для подписи ECDSA ≈ Биткойн-адрес получателя если проделать операции с 5 по 8 табл.16.3) 88 (OP_EQUALVERIFY) AC (OP_CHECKSIG)
----------------	--------	--------------	---

Примечание.

*) 1 «сатоси» = 10⁻⁸ BTC = 0.000 000 01 BTC – минимально возможная сумма BTC для осуществления операций в сети Биткойн, названная в честь автора.

Идентификатором транзакции, по которому она отслеживается (хранится в сети Биткойн), является ее двойной хеш txID = SHA256(SHA256(tx)).

В качестве входов указываются выходы предыдущих транзакций, в которых отправитель являлся получателем BTC. В каждом из выходов предыдущих транзакций хранится двойной хеш PubKeyHash = RIPEMD160(SHA256(e_{отп})) открытого ключа отправителя текущей транзакции e_{отп}, где он был получателем BTC – см. scriptPubKey в табл.16.6. Во входе текущей транзакции, связанной с выходом предыдущей, отправитель указывает свой открытый ключ в явном виде e_{отп} = PubKey – см. scriptSig в табл.16.5. Взяв от него двойной хеш PubKeyHash’ = RIPEMD160(SHA256(e_{отп})) и сравнив с PubKeyHash, можно убедиться, что отправитель является законным владельцем BTC. Вторая проверка владения заключается в сравнении хешей транзакций. Вначале дважды хешируется текущая транзакция с учетом примечания к табл.16.5 hash = SHA256(SHA256(tx_{сиг})). Затем с помощью открытого ключа отправителя e_{отп} = PubKey из цифровой подписи Sig входа текущей транзакции – см. scriptSig в табл.16.5 – расшифровывается находящийся в ней двойной хеш текущей транзакции hash’ = ECDSA⁻¹(Sig, e_{отп}) и сравнивается с hash. Равенство PubKeyHash = PubKeyHash’ и hash = hash’ говорит о **законном праве отправителя** распоряжаться BTC. Второе равенство говорит также о том, что данные текущей транзакции не были искажены (подделаны), за исключением полей scriptSig.

Перед формированием транзакции получатели должны передать отправителю двойные хеши своих открытых ключей e_{пол} (≈ Биткойн-адреса, на которые переводятся BTC) PubKeyHash = RIPEMD160(SHA256(e_{пол})), указываемые в выходах текущей транзакции – см. scriptPubKey табл.16.6. Если получатель неправильно укажет двойной хеш своего открытого ключа, то после подтверждения транзакции в блокчейн биткойны с этого выхода будут для отправителя потеряны.

В **скриптах** scriptSig и scriptPubKey используется специальный скриптовый язык Биткойн, включающий в себя около 80 команд, работающих со стековой памятью. В символьном виде команды начинаются с «OP_», а при хранении транзакций – в виде кодов размером один байт. Скрипты позволяют писать довольно сложные программы для сети Биткойн. В транзакциях пара указанных скриптов задают условия, по которым получатель может воспользоваться переведенными BTC. В табл.16.5 и 16.6 указан самый распространенный случай перевода BTC по адресам получателей в формате P2PKH. С помощью скриптов можно:

- выполнять групповое подписание транзакций, чтобы для перевода BTC требовалась подпись более чем одного отправителя (например, для контроля движения денежных средств в крупных организациях);
- выплачивать BTC любому пользователю сети при определенных условиях (например, при розыгрыше конкурсов или лотерей);
- хранить в блокчейн любую информацию, а не только BTC;
- и т.д.

Транзакции по переводу BTC изначально попадают в отдельную распределённую базу данных, называемую **MemPool** (от англ. memory pool – пул памяти), и носят статус **неподтверждённых** (англ. unconfirmed transaction). Клиент, сгенерировавший транзакцию, отправляет ее одному или нескольким полным узлам. Те проверяют ее на корректность и законность, а затем помещают ее в собственный MemPool и осуществляют широковещательную рассылку по другим полным узлам сети Биткойн. Некоторые из транзакций (как правило, с малой комиссией) могут не попасть в MemPool отдельных полных узлов из-за ограничений по объему памяти.

16.3.6.7. Блок

Для того чтобы получатель воспользовался переведенными BTC, транзакция должна быть включена в блок блокчейна Биткойн. Этим занимаются **майнеры** (англ. miner – шахтер). Они создают блок, в который включаются сотни, а, на текущий момент, уже и тысячи разных транзакций. При этом самая первая транзакция в блоке генерируется самим майнером и является для него вознаграждением за создание блока (англ. coinbase / generation transaction). Данное вознаграждение следует понимать как новые BTC (монеты), появляющиеся в сети Биткойн.

Формат транзакции по добыче BTC (создании нового блока) идентичен формату, рассмотренному выше в табл.16.4-16.6. Она имеет строго по одному входу и выходу, а также во входе отсутствует ссылка на предыдущую транзакцию. Особенности указания информации во входе такой транзакции рассмотрены в следующей таблице.

Таблица 16.7. Формат входа первой транзакции в блоке (coinbase)

Имя		Тип	Размер, байт	Назначение		Пример
previous_output	outpoint txID (hash)	строка, char[32]	фиксированный, 32	Идентификатор выхода предыдущей транзакции, из которой берутся BTC для отправки.	Номер предыдущей транзакции. Т.к. она отсутствует, то поле заполняется нулями.	00 00
	outpoint index number (index)	целое, uint32_t	фиксированный, 4		Номер выхода в предыдущей транзакции. Т.к. она отсутствует, то поле заполняется 0xFFFFFFFF.	FF FF FF FF

script bytes	целое, compactSize uint, (uint8_t..uint64_t)	переменный, 1..9	Количество байтов в скрипте coinbase – максимум 100 байт.	29 (41 байтов)
height	строка, char[]	переменный	Скрипт, указывающий номер (высоту) формируемого блока. Высота записывается с обратным порядком следования байтов (little-endian).	(<Height>) 03 (3 байта – размер высоты) 4E 01 05 (328014 ₁₀ – высота блока)
coinbase script	строка, char[]	переменный	Скрипт, указывающий на произвольные данные. Произвольные данные не превышают 100 байтов минус байты высоты. Майнеры обычно помещают в это поле значение попсо (см. табл.16.8), необходимое для правильного формирования хеша заголовка блока.	(<Data>) 06 2F 50 32 53 48 2F 04 72 D3 54 54 08 5F FF ED F2 40 00 00 F9 0F 54 69 6D 65 20 26 20 48 65 61 6C 74 68 20 21
sequence	целое, uint32_t	фиксированный, 4	Параметр, предназначенный для блокировки неподтвержденной транзакции. По умолчанию для Bitcoin Core равен 0x00000000.	00 00 00 00

Для создания блока необходимо решить математическую задачу, требующую больших вычислительных ресурсов для нахождения решения, но малых для проверки правильности решения. Другими словами, необходимо предоставить **доказательство выполнения работы** (англ. Proof-of-work, POW). В основе Биткойн лежит задача поиска блока, двойной хеш заголовка которого меньше заданного целевого порога. Сложность задачи регулируется таким образом, чтобы каждый новый блок создавался участниками сети примерно 1 раз в 10 минут (≈ 210 000 блоков за 4 года).

Изначально, в первое четырехлетие с 2008 по 2012 гг., вознаграждение за создание блока составляло 50 BTC. Каждые 4 года стоимость вознаграждения уменьшается вдвое, ввиду чего итоговая эмиссия не превысит 21 000 000 BTC. К 33 четырехлетию (≈ 2136 – 2140 гг.) стоимость вознаграждения составит минимально возможную для операций сумму – 1 «сатоси». Таким образом, если сейчас стимулом для майнеров являются BTC за создание нового блока и комиссии за транзакции, включенные в этот блок, то в будущем основной доход майнеров будут составлять комиссии за транзакции.

Формат отдельного блока представлен в следующих таблицах.

Таблица 16.8. Формат блока

Имя	Тип	Размер, байт	Назначение
block header	block_header	фиксированный, 80	Заголовок блока. См. табл.16.9.
txn count	целое, compactSize uint, (uint8_t..uint64_t)	переменный, 1..9	Общее количество транзакций в блоке, включая первую транзакцию coinbase.
txns	список, txns	переменный	Список транзакций в блоке в формате необработанных транзакций (raw transaction format – см. табл.16.4-16.6). Транзакции должны следовать в списке в том же порядке, когда их txID появились в первой строке дерева Меркла.

Таблица 16.9. Формат заголовка блока (block header)

Имя	Тип	Размер, байт	Назначение	Пример
version	целое, int32_t	фиксированный, 4	Номер версии блока. Указывает на набор правил проверки блока.	02 00 00 00
previous block header hash	строка, char[32]	фиксированный, 32	Двойной хеш SHA-256 заголовка предыдущего блока. Гарантирует, что предыдущий блок не может быть изменен без изменения заголовка этого блока.	B6 FF 0B 1B 16 80 A2 86 2A 30 CA 44 D3 46 D9 E8 91 0D 33 4B EB 48 CA 0C 00 00 00 00 00 00 00 00
merkle root hash	строка, char[32]	фиксированный, 32	Корень дерева Меркла. Гарантирует, что ни одна из транзакций не может быть изменена без изменения заголовка.	9D 10 AA 52 EE 94 93 86 CA 93 85 69 5F 04 ED E2 70 DD A2 08 10 DE CD 12 BC 9B 04 8A AA B3 14 71
time	целое,	фиксированный,	Время создания блока в формате Unix (количество секунд, прошедших с 1970-01-01 00:00 UTC) – время, когда майнер начал хешировать заголовок (согласно времени, установленному на его компьютере). Оно должно быть	24 D9 5A 54 (Unix time:

	uint32_t	4	строго больше медианного (среднего) времени предыдущих 11 блоков, включенных в блокчейн. Полные узлы не принимают блоки с заголовками, у которых время опережает их собственное более чем на два часа.	1415239972 sec – 2014-11-06 02:12:52)
nBits	целое, uint32_t	фиксированный, 4	Закодированный целевой порог (цель) двойного хеша заголовка блока. Двойной хеш заголовка должен быть меньше или равен порогу.	30 C3 1B 18 (Цель: 0x1BC330 * 256 ^{0x18-3})
nonce	целое, uint32_t	фиксированный, 4	Число, позволяющее изменить двойной хеш заголовка так, чтобы он получился меньше или равным целевому порогу. Если все значения nonce были безрезультативно протестированы, то майнер может изменить время создания блока, обновить транзакцию coinbase или набор включаемых транзакций с обновлением дерева Меркла.	FE 9F 08 64 (1678286846 ₁₀)

Примечание.

*) Значения хешей записываются в прямом порядке байтов (big-endian), другие значения – в обратном (little-endian).

В качестве дополнительной защиты блока и включенных в него транзакций от искажений и подделки в заголовке блока указывается специальная структура, называемая **корнем дерева Меркла**. **Хеш-дерево, дерево Меркла** (англ. Merkle tree) – полное двоичное дерево, в листьях которого помещены хеши от блоков данных, а внутренние узлы содержат хеши от объединения значений в дочерних узлах. Таким образом, корень дерева (корневой узел) содержит хеш от всего набора данных. При формировании блока в нем указывается список включенных транзакций. Как было отмечено выше, первой транзакцией в списке идет транзакция coinbase, а далее транзакции, взятые майнером из MemPool в соответствии с принятым критерием (например, по величине комиссии). Существует ряд дополнительных правил, в соответствии с которыми транзакции должны располагаться в списке. Например, если транзакции взаимосвязаны (выход одной используется в качестве входа другой), то транзакция с выходом должна располагаться в списке раньше транзакции со входом. Для каждой из этих транзакций tx_i вычисляется двойной хеш, он же ее идентификатор $h_i = txID_i = SHA256(SHA256(tx_i))$. Полученные хеши будут являться листьями дерева Меркла (первой строкой, первым уровнем). Если количество транзакций в списке нечетное, то значение хеша последней транзакции дублируется. Для формирования узлов следующего уровня дерева, листья разбиваются на пары и вычисляется двойной хеш их объединения $h_{i, i+1} = SHA256(SHA256(h_i + h_{i+1}))$, где «+» - операция конкатенции. По аналогии с листьями, если будет получено нечетное количество узлов на уровне, то последний узел дублируется. Далее операции по объединению узлов и вычислений двойного хеша продолжаютс, пока на очередном уровне не будет получен единственный узел, называемый корнем дерева.

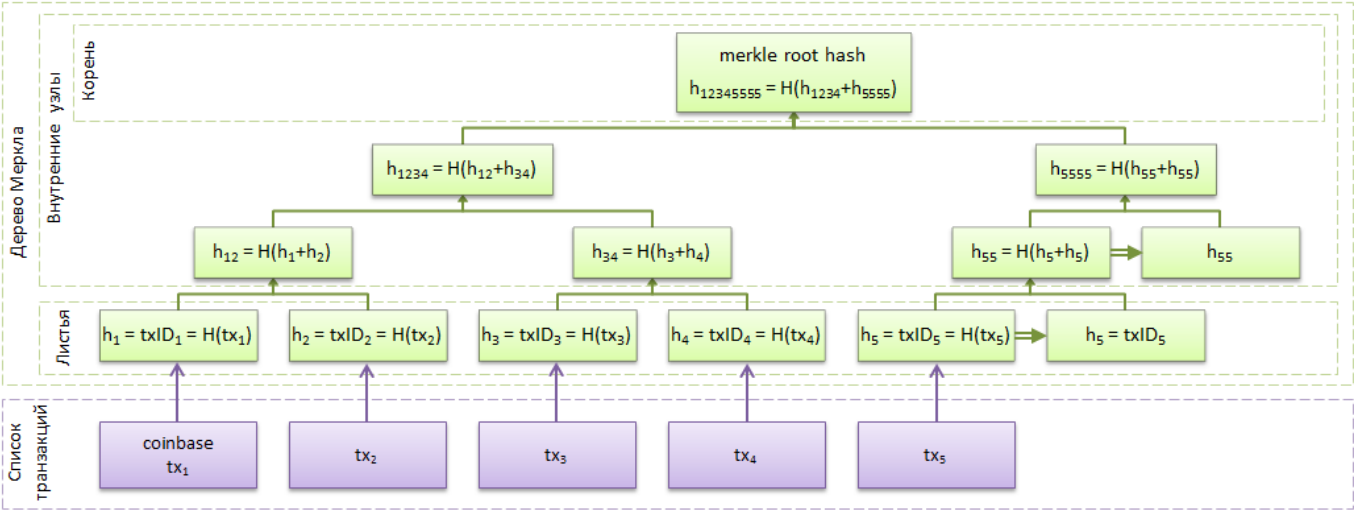
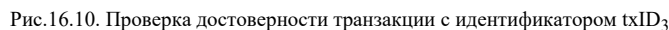


Рис.16.9. Пример схемы определение корня дерева Меркла
($H(M) = SHA256(SHA256(M))$)

Деревья Меркла используются в сети Биткойн для проверки достоверности транзакций. Как отмечалось выше, объем полного блокчейна превысил 200 Гб и неуклонно растет. Хранить такой объем данных на облегченных устройствах (например, смартфонах) крайне затруднительно, а чаще всего невозможно. В связи с этим на таких устройствах хранится усеченная версия блокчейн, состоящая только из заголовков блоков (block header), размер которых всего по 80 байтов. Для проверки достоверности какой-либо транзакции на облегченном SPV-узле используется следующая схема:

- SPV-узел по идентификатору транзакции txID запрашивает у полного узла подтверждающие данные;
- полный узел:
 - о по txID находит блок, в котором она содержится;
 - о вычисляет для этого блока дерево Меркла;
 - о высылает SPV-узлу хеши промежуточных узлов дерева, непосредственно связанных с узлами пути, соединяющему лист транзакции с корнем. При этом сам корень дерева не высылается, а SPV-узлу также сообщается, по какую сторону от пути расположены эти промежуточные узлы;
- SPV-узел самостоятельно вычисляет хеши узлов пути, включая хеш корня дерева, и в своем усеченном блокчейне ищет блок, в заголовке которого имеется вычисленный хеш корня дерева. Если такой блок найден, то транзакция достоверна.

Например, для транзакции с идентификатором txID₃ полному узлу достаточно выслать хеши h₄ (справа), h₁₂ (слева) и h₅₅₅₅ (справа). SPV-узел вычисляет хеши h₃₄, h₁₂₃₄ и h₁₂₃₄₅₅₅₅, после чего в своем блокчейне ищет блок, у которого корень дерева равен h₁₂₃₄₅₅₅₅.



- Вычисление хеша сообщения для современных компьютеров не вызывает никаких проблем. Процессоры или видеокарты обыкновенных компьютеров могут вычислять тысячи и даже миллионы хешей в секунду, а производительность специализированного оборудования в виде ASIC-майнеров (от англ. application-specific integrated circuit - интегральная схема специального назначения) измеряется гига- и терахешами в секунду.



Рис.16.11. ASIC-майнер

Для того чтобы создать блок и получить за него вознаграждение было затруднительно, в системе Биткойн имеется ограничение в виде целевого порога. **Целевой порог** (англ. target threshold), **цель** (англ. target) – это 256-битное целое число без знака, не больше которого должен быть хеш заголовка блока, добавляемого в блокчейн. Поле заголовка nBits содержит только 32 бита (4 байта), в которое порог записывается в так называемом «компактном» формате. Закодированный порог преобразуется по следующим правилам:

[illegible]

Таким образом, майнер, выбрав из MemPool транзакции, определив корень дерева Меркла и другие поля заголовка, начинает последовательно перебирать значения поля **nonce**, считать двойной хеш SHA-256 полученного заголовка и сравнивать его с порогом. Если обратная запись байтов хеша равна или меньше порога, то на этом вычисления прекращаются и полученный блок рассылается по сети Биткойн с целью его добавления в блокчейн. Двойной хеш заголовка блока для примера, приведенного в табл.16.9 – $\text{hash}_{\text{hh}} = \text{SHA256}(\text{SHA256}(\text{block header})) = 0\text{x}2837\text{AF}674\text{E}81436\text{B}09\text{E}0\text{C}937\text{E}94\text{D}96\text{F}32\text{E}5\text{C}872391\text{B}A1090000000000000000$. Сравнив его с целью, можно сделать вывод, что блок удовлетворяет требованиям включения в блокчейн.

Двойной хеш заголовка (little-endian)	00 00 00 00 00 00 00 00 09 A1 1B 39 72 C8 E5 32 FE 96 4D E9 37 C9 E0 09 6B 43 81 4E 67 AF 37 28
Цель (на 32 байта)	00 00 00 00 00 00 00 00 18 1B C3 00

Очевидно, что желающих зарабатывать BTC на создании блоков и получении комиссий много. Тот, кто первым создаст блок, тот и получает все вознаграждения. Для майнинга используются не только ASIC-майнеры, но и специализированные программно-аппаратные комплексы, состоящие из сотен и тысяч единиц оборудования. Среди них выделяются майнинг-фермы и майнинг-пулы. **Майнинг-ферма** – локально расположенный программно-аппаратный комплекс, объединяющий большое количество вычислительных устройств (процессоры, видеокарты и/или ASIC-майнеры) и предназначенный для эффективного майнинга криптовалюты за счет распараллеливания вычислений. Такой комплекс может располагаться в одном помещении, здании или компактно расположенной группе строений.

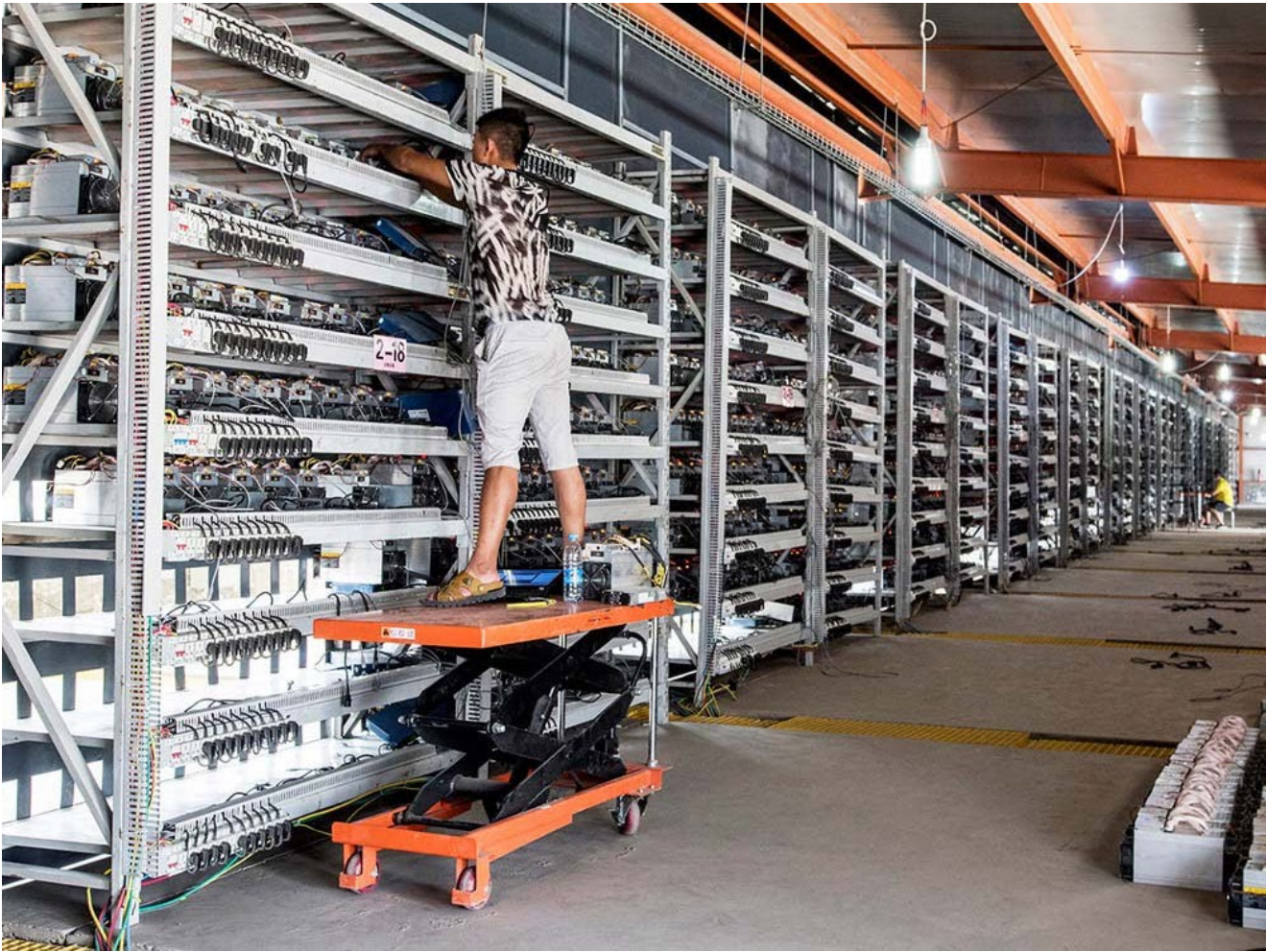


Рис.16.12. Майнинг-ферма

Майнинг-пул в отличие от майнинг-фермы является территориально распределенным программно-аппаратным комплексом. Он объединяет сотни или тысячи различных участников, в т.ч. и майнинг-фермы, для более эффективного майнинга. Доходы в этом случае распределяются между участниками пула, как правило, согласно их вкладу в процесс добычи BTC. В настоящее время основная доля новых блоков создается именно пулами.

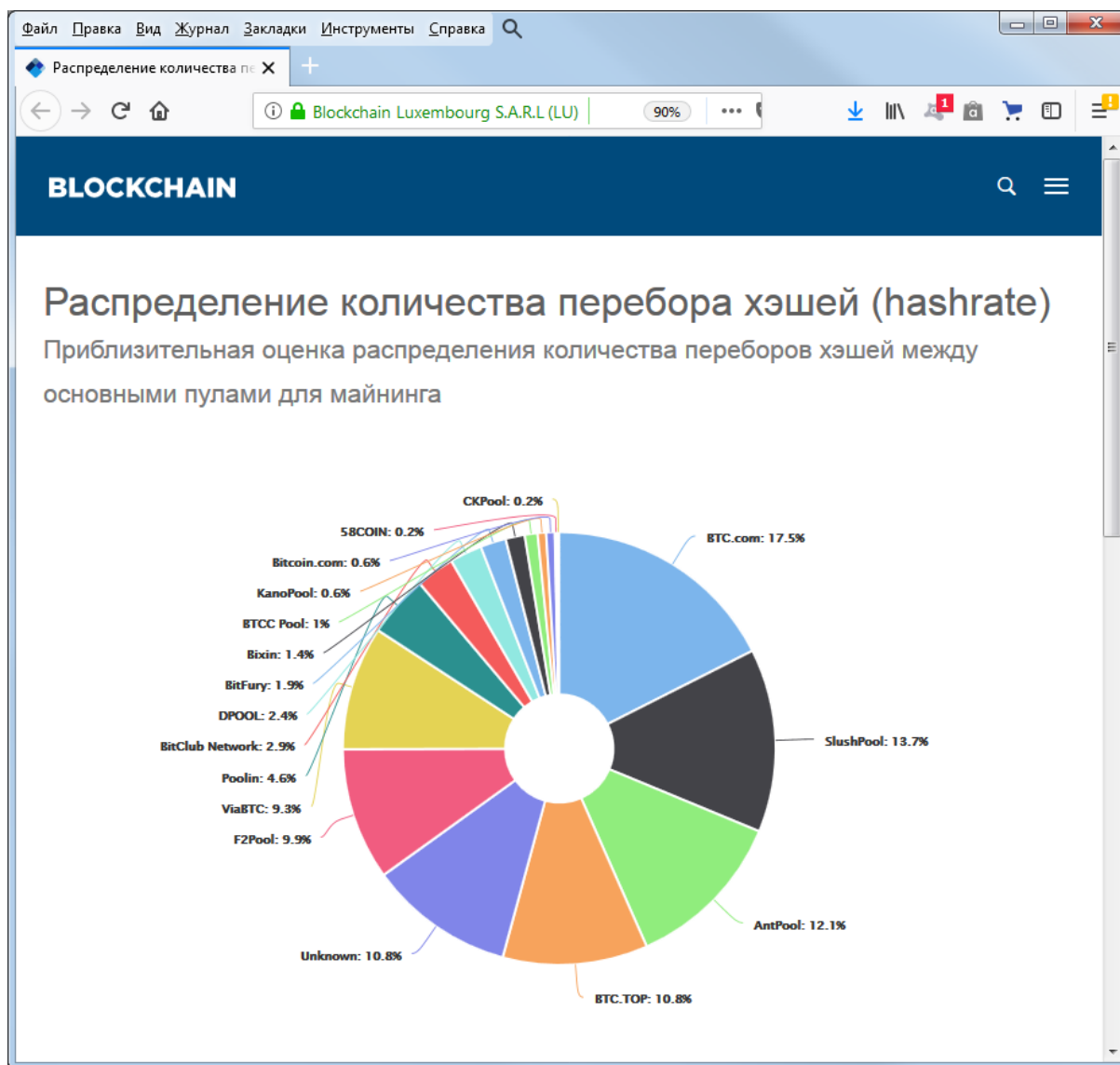


Рис.16.12. Относительная вычислительная мощность майнинг-пулов на начало сентября 2018 г. [<http://www.blockchain.com/ru/pools>]

Учитывая возрастающие вычислительные способности оборудования и распараллеливание вычислений, целевой порог постоянно меняется таким образом, чтобы новый блок добавлялся в блокчейн Биткойн примерно 1 раз в 10 минут. Между участниками майнинга идет постоянное соревнование – кто первым создаст новый блок. В сети постоянно возникают ситуации, когда на добавление в блокчейн претендуют более одного нового блока, созданных разными майнерами – **fork** (русс. ветвление). В этом случае отдельные части сети будут поддерживать (наращивать новыми блоками) свою версию блокчейна, но в итоге одна из ветвей становится длиннее и поддерживается всеми участниками сети Биткойн. За всю историю блокчейн максимальный размер альтернативной аннулированной ветви составил 4 блока. Созданные, но не включенные в блокчейн блоки, называют **брошенными** (англ. orphaned).

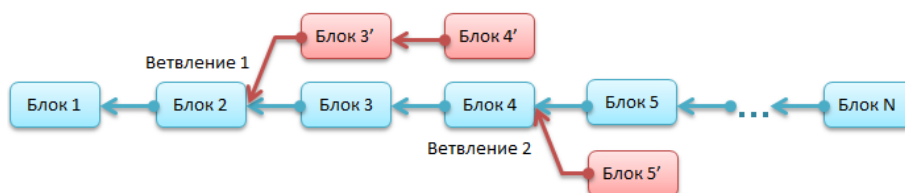


Рис.16.13. Ветвления блокчейна

В связи с возможным появлением ветвлений, награду за создание нового блока можно получить (потратить) только после 120 подтверждений (≈ 20 часов), т.е. когда после этого блока в блокчейн будет добавлено еще 120 блоков. Для транзакций, включенных в новый блок, стандартный (безопасный) период ожидания составляет 6 подтверждений (≈ 1 час). До этого момента транзакция все еще носит статус неподтвержденной. Получатель BTC по такой транзакции может отгрузить товар или оказать услугу, но на свой страх и риск.

Вопросы для самопроверки

1. Перечислите основные разновидности электронных платежей.
2. В чем отличие персонализированных платежных систем от анонимных?
3. В чем отличие дебетовых карт от кредитных?
4. Для чего используется «закрывающий множитель»?
5. Дайте определение понятию «блокчейн».

6. Чем полный узел сети Биткойн отличается от облегченного?
7. Какая связь между ключами ЭЦП ECDSA и Биткойн-адресом?
8. Как подтверждается законность владения BTC?
9. Для чего используется дерево Меркла?
10. Для чего используется целевой порог в Биткойн?

17.1. Общие сведения

17.1.1. Выборы

Выборы - формирование органов власти и/или наделение полномочиями должностного лица посредством волеизъявления голосующих. Различают следующие разновидности выборов.

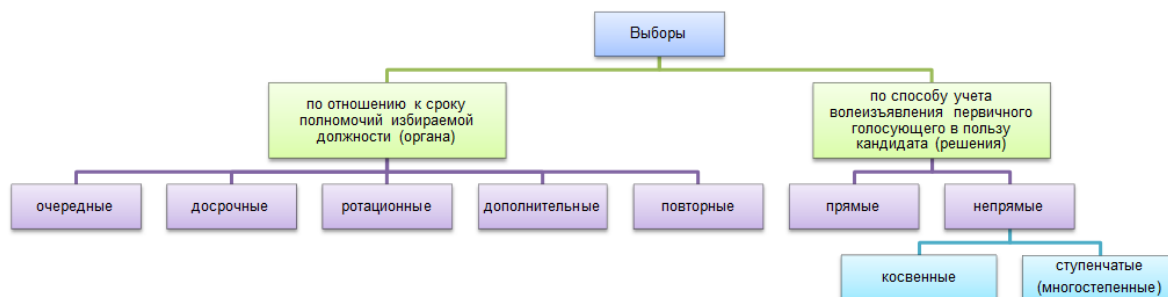


Рис.17.1. Классификация выборов

I. По отношению к сроку полномочий избираемой должности (органа).

Выборы проводятся:

- **очередные** – по истечении установленного срока полномочий;
- **досрочные** – в связи с преждевременным прекращением ранее объявленного срока полномочий;
- **ротационные (частичные)** – в случае одновременного избрания части состава коллегиального органа;
- **дополнительные** – в случае возникновения вакансий (например, по возрастному цензу или болезни) во время срока полномочий коллегиального органа;
- **повторные** – в случае признания по решению суда или избирательной комиссии проведенных выборов несостоятельными или недействительными.

II. По способу учета волеизъявления первичного голосующего в пользу кандидата (решения).

Прямые выборы означают, что орган власти избирается непосредственно голосующими гражданами. Например, в России на основе прямых выборов избираются депутаты местных органов власти, депутаты Государственной Думы Федерального Собрания Российской Федерации, Президент Российской Федерации, в США - сенаторы и члены Палаты представителей Конгресса США, во Франции - Президент Республики, члены Национального собрания и Сената.

Имеются две разновидности **непрямых** выборов: косвенные и ступенчатые.

Косвенные выборы предполагают, что члены коллегиального органа власти или единоличный глава органа избираются выборщиками - лицами, специально избранными для осуществления выборов в соответствующий орган власти. Они перестают быть выборщиками сразу после того, как проголосовали. Принцип косвенных выборов существовал в Пруссии, Румынии и Швеции; применялся на выборах сенаторов во Франции и Испании. В настоящее время на основе косвенных выборов избирается Президент США и сенаторы федерального Конгресса. Как правило, выборщик при голосовании отражает точку зрения большинства своих избирателей.

В ходе **ступенчатых** выборов избирается вначале один орган власти, члены которого избирают другой орган власти, более высокого уровня. Характерны в этом плане выборы во Всекитайское собрание народных представителей (ВСНП). Граждане-невоенные непосредственно, т.е. прямыми выборами, избирают только сельские и поселковые собрания народных представителей. Сельские и поселковые собрания из числа своих депутатов избирают городские и районные. Городские и районные собрания избирают депутатов провинциальных собраний, собраний автономных округов и автономных районов, которые уже из своего состава выбирают депутатов ВСНП. Следует отметить, что представители Народно-освободительной армии Китая в ВСНП избираются косвенными выборами.

В ходе ступенчатых выборов избираются премьер-министры Великобритании, Японии и Италии. Формально они назначаются на должность высшим лицом государства (соответственно, монархом, императором и президентом), но по факту путем одобрения (голосования) в выборном органе законодательной власти - парламенте.

В истории можно найти примеры использования **косвенных ступенчатых** выборов. Например, в России на выборах в Государственную Думу в период 1905 - 1917 гг. рабочие и крестьяне избирали выборщиков, которые на съезде, в свою очередь, избирали других выборщиков и т.д. Только выборщики третьей степени от рабочих и выборщики четвертой степени от крестьян избирали непосредственно депутатов.

17.1.2. Голосование

Выборы осуществляются посредством голосования лиц, имеющих на это право. **Голосование** – способ принятия решения группой лиц, при котором общее мнение формулируется путем определения максимального количества голосов, поданных за один или несколько (строго определенного количества) вариантов из множества альтернативных. Различают следующие разновидности голосования.

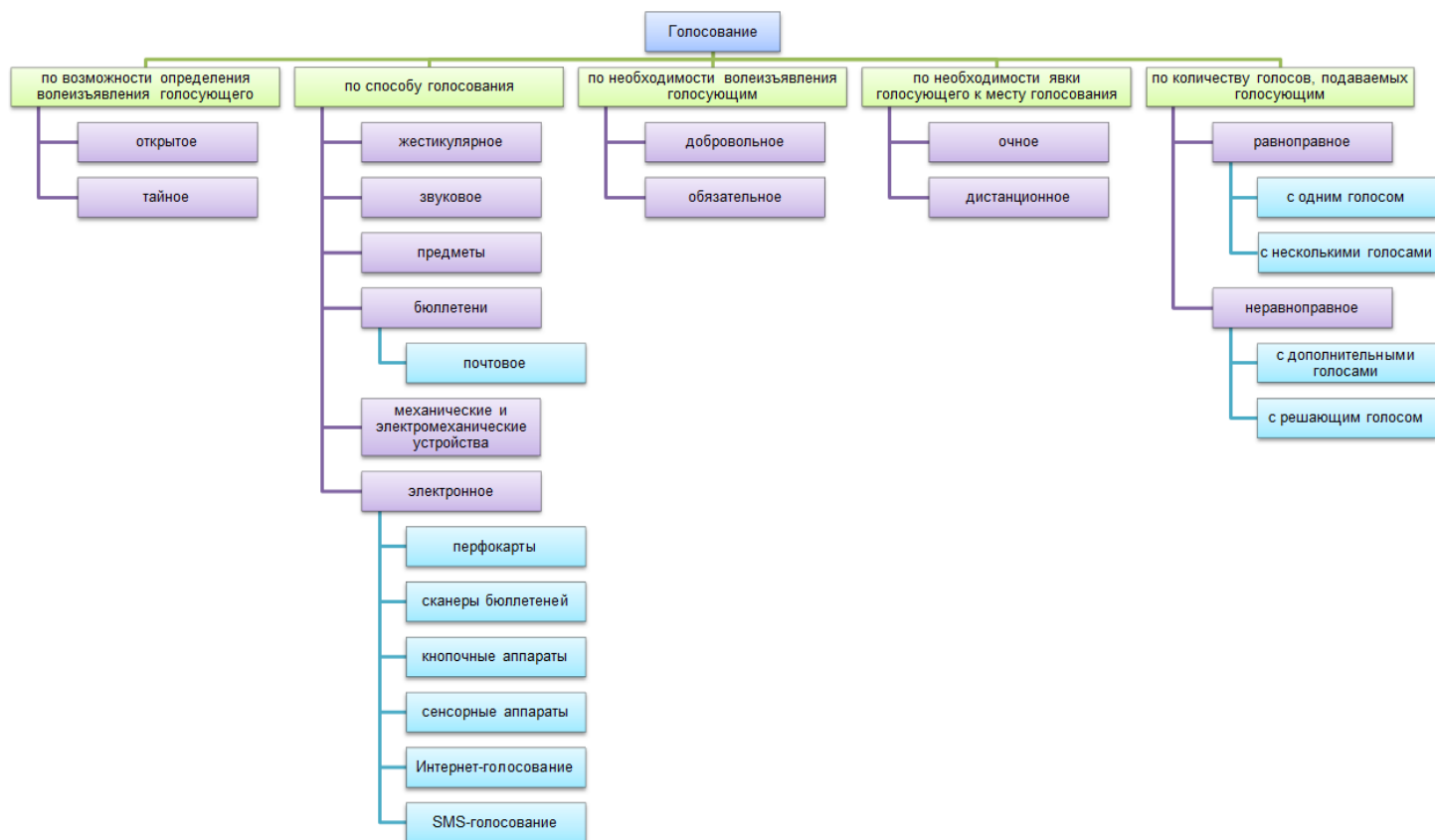


Рис.17.2. Классификация видов голосования

I. По возможности определения волеизъявления голосующего.

Практика тайного голосования имеет давнюю историю. В частности, в **Древних Афинах** подобный способ голосования применялся при принятии различных решений.

В Европе впервые на законодательном уровне процедура тайного голосования была закреплена во **Французской Конституции 1795 г.** По закону 1831 г. при голосовании избиратели по очереди вызывались секретарем собрания, получали от него чистый лист бумаги, и затем, сидя за столом, писали на этом листе имя своего кандидата. По закону 1849 г. анонимные избирательные записки должны быть составлены вне зала голосования на белой бумаге без опознавательных признаков и подаваться в сложенном виде. Урна, в которую председатель комиссии опускал бюллетени, запиралась на два замка. Один ключ находился у председателя, другой - у старшего счетчика. В 1912-1913 гг. во Франции появились изолированные кабины для голосования.

В **Великобритании** требования о введении тайного голосования на парламентских выборах появились еще в 1833 г., но почти сорок лет власти сопротивлялись этому нововведению. Лорд Пальмерстон в свое время отклонил это предложение, т.к. «идти, крадучись, в кабину для голосования» было бы «недостойно для характера прямых и честных англичан». Лишь в конце 1872 г. по инициативе либерального правительства Гладстона парламент принял «Акт о баллотировке», введший систему «тайного» голосования. Слово «тайное» взято в кавычки, т.к. на самом деле секретарь избирательной комиссии находил имя избирателя в списке, отрывал в специальной книге пронумерованный талон-бюллетень, заверял его печатью и вручал избирателю. Т.о. тайна голосования охранялась, главным образом, моральными качествами членов избирательной комиссии.

В 1899 г. в **Германии** начали использоваться специальные ширмы, которые скрывали от окружающих действия избирателей.

Итальянским законом от 1912 г. было введено применение однотипных бюллетеней, отпечатанных типографским способом. В них, помимо фамилий кандидата, следовало, по возможности, изобразить их эмблемы.

В **США** тайное голосование записками применялось еще в XVII в. на выборах должностных лиц в штатах Новой Англии. На федеральном уровне закон 1871 г. предписывал, что выборы в палату представителей должны осуществляться посредством рукописных или печатных бюллетеней. Новый федеральный закон 1891 г. предписывал обнародование (не позднее, чем за 4 дня до выборов) печатных бюллетеней с именами кандидатов. Американский бюллетень имел две части, одинаково пронумерованные. Одна часть отрывалась и вручалась избирателю. Выбрав кандидата, избиратель прокалывал бюллетень в условном месте и опускал в урну. Другая часть хранилась в избирательной комиссии для контроля соответствия числа выданных и использованных бюллетеней. Подобная система позволяла при необходимости определять подлинность бюллетеней при сохранении тайны голосования.

В современной **России** принцип тайного голосования законодательно закреплён в статье 81 Конституции РФ (применительно к выборам Президента РФ), статье 1 ФЗ «О выборах Президента Российской Федерации», статье 1 ФЗ «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации», статье 23 ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации».

II. По способу голосования.

1) Жестикулярное голосование. Один из первых способов голосования. В **Древних Афинах** он назывался «**хейротония**» (от греч. *хэ́рт* – «рука», *та́тис* – «натяжение»), или «поднятие рук». Сегодня мы называем такое голосование открытым. Этот способ применялся при вынесении решения народным собранием. Об этом свидетельствует ряд источников: «Аполлодор, как член Совета, внес проект постановления, и этот проект был вынесен на народное собрание. Он предложил открытым голосованием решить вопрос, использовать ли оставшиеся в казне после расходов на внутренние нужды деньги для военных целей или же, оставить их в качестве зрелищных денег... Когда голосование началось, никто не поднял руки против этого предложения, не выступил против ...» [Демосфен. Против Неэры].

У **германских** племен начала I тысячелетия н.э. на собраниях общины голосование осуществлялось с помощью поднятого вверх **оружия**: «Если их (старейшин) предложения не встречают сочувствия, участники собрания шумно их отвергают; если, напротив, нравятся, - раскачивают поднятые вверх фразы: ведь воздать похвалу оружием, на их взгляд, - самый почетный вид одобрения» [Тацит. О происхождении германцев и местоположении Германии].

В **Древнем Риме** во время гладиаторских боев отогнутый вниз большой **палец**, символизирующий вынутый из ножен меч, означал смерть, сжатый в **кулак** или поднятый вверх - жизнь.

Там же в Сенате среди младших магистратов (сенаторов) был распространен способ «голосования ногами». Т.к. они не имели право голосовать при принятии решений (но имели право выступать), то свое мнение они высказывали путем перемещения по Сенату и присоединения к тем старшим сенаторам, кто разделял их точку зрения. В настоящее время под выражением «**голосование ногами**» подразумевается не участие в голосовании, а, наоборот, отказ от него. Избиратели отказываются от голосования (исполнения своего «гражданского долга») в силу непредсказуемости результата выборов, отсутствия достойных кандидатов, малозначительности вопроса, выносимого на голосование, и т.п.

В популярной молодежной игре «мафия» голосование при выборе очередной «жертвы» осуществляется указанием на нее рукой или пальцем.

В настоящий момент во время открытого голосования, как правило, поднимают руку или **мандат** (лат. *mandatum* - поручение).



Рис.17.3. Пиратская Партия Германии выбирает кандидатов в Европарламент (2014 г.)

2) Звуковое голосование. В наиболее распространенных случаях голосующий должен был назвать имя соискателя из числа претендентов, в пользу которого он подает свой голос, либо высказаться «за» или «против» выдвигаемого предложения или соискателя. Эта разновидность открытого голосования использовалась еще в Древнем Риме во время народных собраний.

3) Голосование с помощью предметов. На протяжении столетия (конец VI-V вв. до н.э.) в Древних Афинах проводилось народное голосование – «остракизм» («остракофория», от др.-греч. τὸ ὀστράκον - «черепок, скорлупа»). По инициативе Клисфена (предположительно, в 506/505 г. до н.э.) община получила право официально изгонять из пределов полиса на десять лет любого общественного деятеля, чья популярность могла привести к узурпации власти и угрожала основам народовластия. Один раз в году народное собрание рассматривало вопрос о том, имеется ли необходимость применения остракизма. В случае положительного ответа на этот вопрос, созывалось специальное собрание. О том, как оно проходило, описано у известного древнегреческого философа.

Каждый, взяв черепок, писал на нем имя гражданина, которого считал нужным изгнать из Афин, а затем нес к определенному месту на площади, обнесенному со всех сторон оградой. Сначала архонты подсчитывали, сколько всего набралось черепков: если их было меньше шести тысяч, остракизм признавали несостоявшимся. Затем все имена раскладывались порознь, и тот, чье имя повторялось наибольшее число раз, объявлялся изгнанным на десять лет без конфискации имущества.

Плутарх. «Аристид»



Рис.17.4. Черепки для голосования (V в. до н.э.)

Подвергнутые «суду черепков» не могли оспорить приговор народа и предоставить доказательства своей лояльности. В разные годы путем остракизма из Афин были изгнаны такие известные политики как Кимон, Аристид, Фемистокл, Дамой (учитель Перикла). Остракизм был свойствен не только Афинам. Он встречался также в Аргосе, Мегаре, Сиракузах, а согласно Аристотелю - во всех греческих городах с демократическим образом правления.

В Афинах существовала еще одна политическая процедура, схожая с остракизмом. Совет пятисот мог исключить из своих рядов лицо, не соответствующее высокому статусу булевта (члена совета). В таком случае применялась «**экфиллофория**» (греч. ἐκφυλλοφορία) - голосование **листьями**, на которых члены Совета писали имя своего коллеги, подлежащего исключению:

Совет приступил к голосованию. И сначала, при подаче голосов масличными листьями, он исключил Тимарха из своих списков, однако затем, при голосовании камешками, вновь принял его в свои ряды.

Эсхин. «Античная демократия»

Для Древних Афин были характерны различные методы голосования и, соответственно, предметы, использовавшиеся для этого. Так, при вынесении вердикта по судебным

разбирательствам присяжные заседатели использовали **металлические диски** (изначально камушки с медным стержнем посередине). Диск с отверстием в центре (на рис.17.5 диск в левом верхнем углу) означал «виновен», без отверстия – «невиновен».



Рис.17.5. Диски для голосования (III в. до н.э.)

В ходе процедуры голосования, каждый из присяжных получал два диска (виновен и невиновен). Диск со своим решением он опускал в бронзовую амфору, второй – в деревянную. На основании подсчета количества просверленных и цельных дисков в бронзовой амфоре выносился вердикт по делу. Если голосов оказывалось поровну, решение выносилось в пользу подсудимого.

На выборах должностных лиц и членов коллегиальных органов управления использовался жребий («**клеросис**»). В один сосуд клали таблички с именами кандидатов, а во второй – **бобы** (впоследствии камешки и шары) двух цветов. Число белых бобов равнялось числу вакантных (выборных) мест, а черных - разнице между числом кандидатов (соискателей) и белых бобов. Далее осуществлялась одновременная выемка имени кандидата из одного сосуда и боба из другого. Белый боб означал, что кандидат избран. Древние греки считали, что таким образом проявляется воля богов. Подобный способ избрания должностных лиц имел и своих критиков. В частности Ксенофонт в труде «Воспоминания о Сократе» приводит слова последнего «...глупо должностных лиц в государстве выбирать посредством бобов, тогда как ни кто не хочет иметь выбранного бобами рулевого, плотника ...».

Для прозрачности и частичной «автоматизации» процесса жеребьевки в Афинах в IV в. до н.э. стали применяться механические устройства – **клеротерии**.



Рис.17.6. Фрагмент клеротерия

Схема полного устройства показана на следующем рисунке.

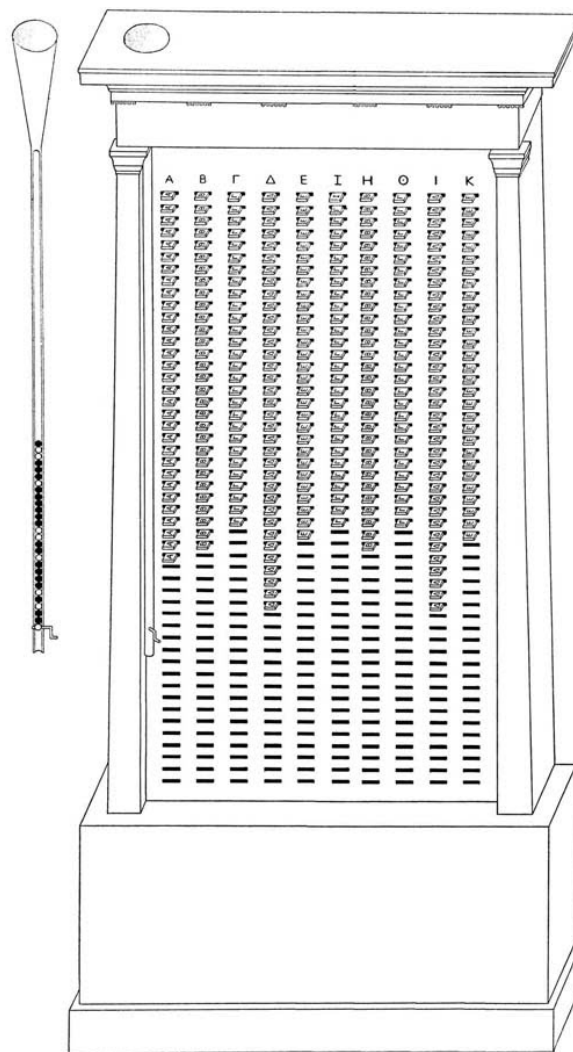


Рис.17.7. Клеротерий

С помощью данного устройства выполнялся выбор присяжных заседателей. В день суда каждая фила (община) предоставляла бронзовые таблички (англ. pinakion) с именами кандидатов в заседатели.



Рис.17.8. Pinakion

Таблички от одной общины вставлялись в соответствующий ей вертикальный ряд. Вдоль левой стороны клеротария располагалась полая бронзовая трубка с воронкой в верхней части и рукояткой в нижней. В воронку засыпалась смесь белых и черных шаров, которые выстраивались в трубке в случайном порядке. При повороте рукоятки из трубки вываливался один шар. Если он был черным, то таблички из первого сверху горизонтального ряда, соответствующие гражданам разных общин, вынимались. Это означало, что они не будут участвовать в заседании суда. Далее процесс повторялся до тех пор, пока из трубки не вываливался белый шар. При этом граждане, чьи таблички оставались в первом сверху заполненном горизонтальном ряду, в этот день становились присяжными.

При тайном голосовании давно (см. ту же Древнюю Грецию) и успешно используются **шары**. Понятие «баллотирование» - т.е. голосование шарами - впервые появилось в **русском** политико-правовом лексиконе при Петре I. 18 февраля 1720 г. им был издан «Образ баллотирования, как во оном поступать надлежит». Это была инструкция, регламентирующая порядок проведения закрытого голосования в государственном учреждении в том случае, когда имелась необходимость получить решение коллегиального органа при сохранении анонимности взглядов отдельных лиц. Согласно «Образу ...» участники «баллотирования» сначала должны были приносить присягу, затем каждый получал небольшой шар, сделанный «из холста или иной мягкой материи, а не деревянные или иной тяжелой материи». При голосовании шары следовало опускать в двойной ящик, имеющий отделения белого («за») и черного («против») цвета.

Своеобразно проходило тайное голосование в **Греции** на рубеже XIX-XX вв., учитывая исторические традиции и значительное число неграмотного населения. Урна состояла из двух отделений - для шаров, поданных «за» и «против». Снаружи отделения окрашивались разным цветом: правая - белым («за»), левая - черным («против»). На лицевой части находилась табличка с именем кандидата. Помимо этого около каждой урны стоял служащий, который неграмотным избирателям называл имя кандидата, которому она соответствовала. Внутри урна была обита сукном и имелись трубки для скатывания шаров с целью скрытия звука падающих шаров. Число урн в помещении для голосования равнялось числу баллотирующихся кандидатов. Избиратели входили в зал группами по пять человек. Рядом с урнами находились баллотировочные шары - пять белых и пять черных. Избирателю следовало держать шар большим и указательным пальцами, демонстрируя, что у него имеется лишь один «голос». Голосующий поочередно опускал руку в каждую урну с зажатым в кулаке шаром. В одной из них избиратель разжимал руку, тем самым, делая свой выбор.

В **Албании** в первые годы после Второй мировой войны по той же причине (неграмотность значительной части населения) практиковалось похожее голосование резиновыми шарами. Избиратель получал шар, прятал его в кулаке, затем опускал руку поочередно в ящики для голосования «за» и «против» кандидата (единственного), после чего поворачивал к избирательной комиссии ладонь этой руки, показывая, что шар опущен в один из ящиков.

В **российских** диссертационных советах при присуждении степени кандидата или доктора наук использовались белые («за») и черные («против») шары, один из которых члены совета при голосовании опускали в урну.

В случае выборов методом жребия могут использоваться **веточки (спички)**, одна или несколько из которых отличаются от стандартной длины. В подобных случаях могут использоваться также **листочки бумаги**, один или несколько из которых помечены особым образом (например, крестиком).

4) **Голосование с помощью бюллетеней.** Появление данного вида голосования связано с необходимостью проведения выборов с большим количеством голосующих. Как правило, на таких выборах предусмотрена процедура тайного голосования.

Изначально при «бумажном» голосовании избиратели писали имя предпочитаемого кандидата на листе чистой бумаги (например, во **Франции** и **Германии** середины XIX в.).

В XIX в. в **США** была широко распространена практика, когда каждая партия печатала собственные бюллетени (англ. party tickets - **партийные билеты**) со своими кандидатами и распространяла их на избирательных участках.

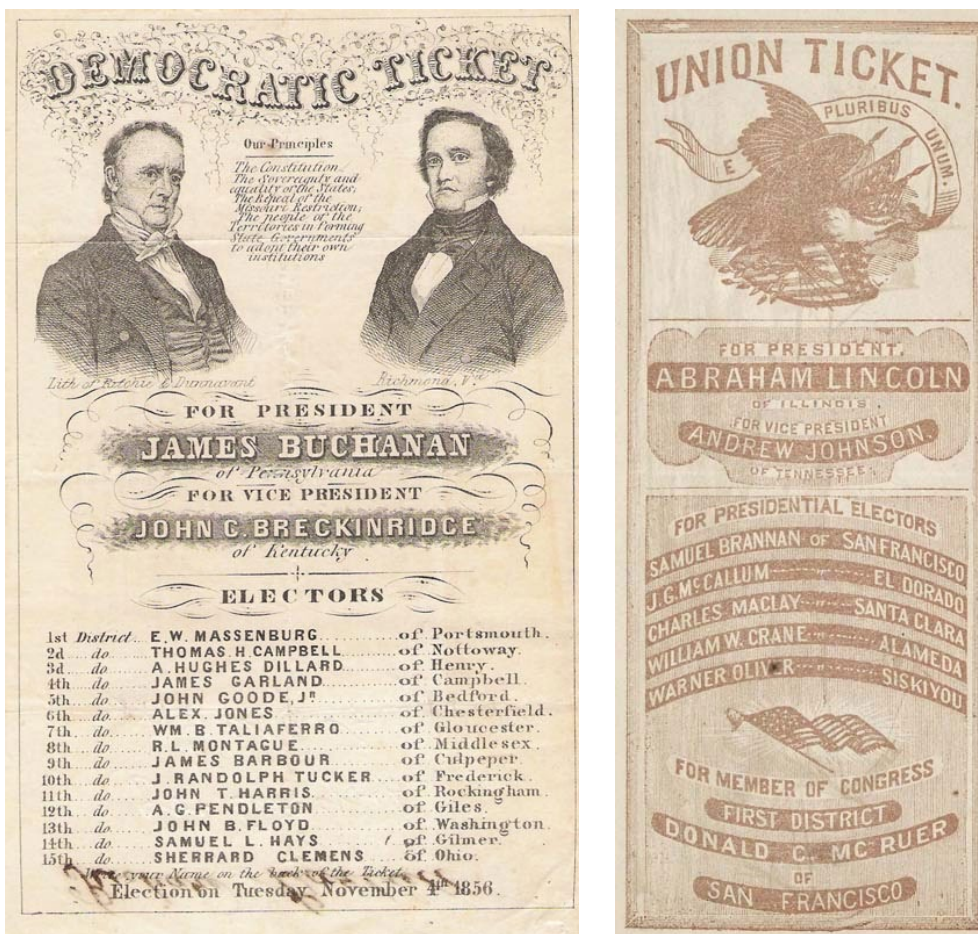


Рис.17.9. Избирательные бюллетени победителей президентских выборов США 1856 г. (Джеймс Бьюкенен – Демократическая партия) и 1964 г. (Авраам Линкольн – Республиканская партия)

Эти бюллетени различались по форме и по цвету, что нарушало тайну голосования. Кроме этого, в бюллетене были кандидаты только от одной партии и, при выборах сразу в несколько органов власти, у избирателя не было возможности отдать свой голос на разные должности за кандидатов от разных партий.

В 1856 г. в штате Виктория на юго-востоке **Австралии** был принят закон о тайном голосовании, по которому за счет средств штата должен был печататься единый бюллетень для всех кандидатов. В нем также было оставлено место для вписывания избирателем фамилии любого другого кандидата. «**Австралийский бюллетень**» стал использоваться в США с 1888 г.

В современных бюллетенях, как правило, свой выбор надо отметить галочкой (крестиком и т.п.).

ИЗБИРАТЕЛЬНЫЙ БЮЛЛЕТЕНЬ
для голосования на выборах депутатов Государственной Думы
Федерального Собрания Российской Федерации пятого созыва
2 декабря 2007 года
Владимирская область

• **РАЗЪЯСНЕНИЕ ПОРЯДКА ЗАПОЛНЕНИЯ ИЗБИРАТЕЛЬНОГО БЮЛЛЕТЕНЯ**
Поставьте любой знак (в пустом квадрате справа от наименования политической партии, зарегистрированной в федеральном списке кандидатов, в пользу которого сделан выбор.
Избирательный бюллетень, в котором любой знак (знаки) проставлен (проставлены) более чем в одном квадрате либо не проставлен ни в одном из них, считается недействительным.
Избирательный бюллетень, не заверенный подписями двух членов участковой избирательной комиссии с правом решающего голоса и печатью участковой избирательной комиссии, без специального знака (марки) признается бюллетенем неустановленной формы и при подсчете голосов не учитывается.

1 Политическая партия «Аграрная партия России» ☐

 Региональная группа № 9 (Владимирская область):
ПЛОТНИКОВ Владимир Николаевич
БРУСНИКОВА Нина Владимировна
ШАНДЫБИН Василий Иванович
ГОРШКОВ Александр Александрович
ЕРШОВА Наталья Ивановна
КУЛЕВ Владимир Евгеньевич

2 Всероссийская политическая партия «Гражданская Сила» ☐

 Региональная группа № 36 (Владимирская область):
БАРЩЕВСКИЙ Михаил Юрьевич
РЯВКИН Александр Юрьевич
ПОХМЕЛКИН Виктор Валерьевич
АБРАМОВ Илья Николаевич
ИЗВЕКОВА Индиана Павловна

Рис.17.10. Фрагмент бюллетеня на выборах депутатов в ГД РФ (2007 г.)

OFFICIAL SAMPLE BALLOT			
GENERAL ELECTION - NOVEMBER 4, 2008			
TANEY COUNTY, MISSOURI			
REPUBLICAN PARTY (REP) DEMOCRATIC PARTY (DEM) LIBERTARIAN PARTY (LIB) CONSTITUTION PARTY (CST) INDEPENDENT (IND) NOTICE OF ELECTION Notice is hereby given that the November General Election will be held in the County of Taney on Tuesday, November 4, 2008 as certified to this office by the participating entities of Taney County. The ballot for the election shall be in substantially the following form:			
A vote for candidates for President and Vice President is a vote for their Electors.		FOR STATE TREASURER Vote for ONE	
FOR PRESIDENT AND VICE PRESIDENT Vote for ONE PAIR		FOR STATE REPRESENTATIVE DISTRICT 142 Vote for ONE	
☐ JOHN MCCAIN SARAH PALIN	REP	☐ BRAD LAGER	REP
☐ BARACK OBAMA JOE BIDEN	DEM	☐ CLINT ZWEIFEL	DEM
☐ BOB BARR WAYNE A. ROOT	LIB	☐ RODNEY D. FARTHING	CST
Write-in		Write-in	
FOR ATTORNEY GENERAL Vote for ONE		FOR STATE REPRESENTATIVE DISTRICT 143 Vote for ONE	
☐ MIKE GIBBONS		☐ MAYNARD WALLACE	
☐ CHRIS KOSTER		☐ CATHY HILLIARD	
Write-in		Write-in	

Рис.17.11. Фрагмент бюллетеня на выборах президента США в штате Миссури (2008 г.)

В отдельных случаях вместо указания кандидата (варианта решения), за которого голосуете, необходимо, наоборот, вычеркнуть остальных. Например, такой порядок голосования регламентировался «Положением о выборах в Верховный Совет СССР» (1937 г.). Согласно «Положения ...» каждый бюллетень содержал надпись: «Оставьте в избирательном бюллетене фамилию ОДНОГО кандидата, за которого Вы голосуете, остальных вычеркните».

ИЗБИРАТЕЛЬНЫЙ БЮЛЛЕТЕНЬ	
по выборам в Верховный Совет СССР	
_____ 1937 года	
округ № _____ по выборам в Совет Национальностей от _____	
(название Автономной республики, области или кнзокруга)	
Оставьте в избирательном бюллетене фамилию ОДНОГО кандидата, за которого Вы голосуете, остальных вычеркните	
Фамилия, имя, отчество кандидата в депутаты	Кем выставлен кандидатом в депутаты
Председатель _____ окружной избирательной комиссии по выборам в Совет Национальностей от _____	

Рис.17.12. Образец избирательного бюллетеня по выборам в Верховный Совет СССР (опубликован в газете «Правда» от 15 октября 1937 г.)

В целях обеспечения конфиденциальности принятого решения избиратель должен лично опустить заполненный бюллетень в урну (ящик) для голосования. В некоторых странах (например, в **Болгарии** и **Польше**) с целью дополнительного обеспечения тайны голосования бюллетени вкладываются в **конверты**.

Во многих странах допускается голосование с помощью бюллетеней по почте. В тех случаях, когда надо обеспечить тайну голосования используются два конверта:

- внешний - с идентификационными данными избирателя (адрес и ФИО). По ним определяется право приславшего конверт на участие в выборах и первичность голосования (т.е. блокируется возможность повторного голосования одним и тем же избирателем);
- внутренний (анонимный) - без данных об избирателе. Его опускают в урну для голосования.

Например, в **Германии** избиратель может заранее получить в избирательной комиссии справку о праве голосования по почте, избирательный бюллетень и отдельный (внутренний) конверт. Помимо бюллетеня, запечатанного во внутренний конверт, во внешний конверт вкладывается также указанная справка с письменным заверением избирателя (или лица, помогавшего ему) на имя руководителя избирательного округа в том, что бюллетень заполнен лично или в полном соответствии с волей избирателя. В ходе выборов в Бундестаг в 1994 г. таким образом проголосовало по разным округам от 7 до 10% избирателей, а на выборах в 1998 г. - от 8 до 16%.

В штате Орегон (**США**) в соответствии с законодательством голосование на президентских выборах осуществляется только по почте.

В бюллетенях надписи, соответствующие разным кандидатам (вариантам решения), как правило, делают однотипными с целью создания равных условий альтернативам. Но, в истории

неоднократно отмечались случаи отступления от этого правила, когда властям необходимо было при внешней демократичности (народном голосовании) легитимизировать выгодное ей решение. Красноречивый пример, бюллетень референдума 1938 г., проведенного в **Австрии** и **Германии**: «Согласны ли вы с Воссоединением Австрии с Немецким Рейхом, которое произошло 13 марта 1938 и поддерживаете ли вы партию нашего фюрера Адольфа Гитлера».



Рис.17.13. Бюллетень с референдума о «воссоединении» Австрии с Германией

Интересна хронология событий перед референдумом и его результаты [17, <http://www.hrono.ru/sobyit/1938avst.html>].

Таблица 17.1. Хронология событий перед референдумом по аншлюсу Австрии 1938 г.

Дата	Событие
12.02.1938	Берхтесгаден. Начались «переговоры» А. Гитлера и министра иностранных дел Германии И. фон Риббентропа с канцлером Австрии К. Шушнигом и австрийским министром иностранных дел Г. Шмидтом. Под угрозой военного вторжения К. Шушниг был вынужден подписать предъявленный ему ультиматум из трёх пунктов: освободить из заключения австрийских нацистов; назначить их лидера А.Зейс-Инкварт министром внутренних дел, главой полиции и службы безопасности; включить австрийскую НСДАП (Национал-социалистическая немецкая рабочая партия) в правительственную коалицию «Отечественный фронт». «Вы не должны обсуждать эти условия. - заявил А. Гитлер, - Вы должны их принять... Если вы будете противиться, вы вынудите меня уничтожить всю вашу систему».
20.02.1938	Берлин. Выступая в рейхстаге, А. Гитлер заявил, что «Германия не может оставаться безучастной к судьбе 10 миллионов немцев, которые живут в двух соседних странах [Австрии и Чехословакии]... Германское правительство будет добиваться объединения всего немецкого народа».
12.03.1938	Утром 8-ая немецкая армия вступила на территорию Австрии, где ее повсюду восторженно приветствовало население. Арестован бывший канцлер Австрии К. Шушниг и принял полномочия новый канцлер Австрии А. Зейс-Инкварт. В Австрию прибыл А. Гитлер, где он посетил свою родину (г. Браунау) и встретился с новым канцлером Австрии А. Зейс-Инквартом (г.Линц).
13.03.1938	Вена. Канцлер А. Зейс-Инкварт подписывает закон «о воссоединении Австрии с Германской империей», согласно которому Австрия объявлялась «одной из земель Германской империи» и отныне стала называться «Остмарк».
10.04.1938	Австрия и Германия. Референдум.

Таблица 17.2. Итоги референдума по аншлюсу Австрии 1938 г.

Выбор	Австрия		Германия	
	Голоса	%	Голоса	%
За	4 453 912	99.73	44 451 092	99.01
Против	11 929	0.27	443 023	0.99
Недействительных бюллетеней	5 777	0.13	69 890	0.16
Зарегистрированных избирателей / явка	4 484 617	99.71	45 149 952	99.59

Для сравнения бюллетень и итоги референдума в **Крыму** в 2014 г.

Приложение 1
к Постановлению Верховной Рады
Автономной Республики Крым
от 6 марта 2014 года № 1702-6/14

Б Ю Л Е Т Е Н Ь
для голосования на общекрымском референдуме 16 марта 2014 года

Б Ю Л Е Т Е Н Ь
для голосування на загальнокрымському референдумі 16 березня 2014 року

2014 сенеси март 16-да умумкырым референдумында рей берильмеси ичюн
БЮЛЛЕТЕНЬ

Отметьте любым знаком в квадрате тот вариант ответа, за который Вы голосуете:

Позначте будь-яким знаком у квадраті той варіант відповіді, за який Ви голосуєте:

Насыл бир вариант ичюн рей бергенинъизни ишаретнен бельгилеъиз:

1) Вы за воссоединение Крыма с Россией на правах субъекта Российской Федерации?

1) Ви за возз'єднання Криму з Росією на правах суб'єкта Російської Федерації?

1) Русие Федерациону субъекти акъларында Кырым Русиеге къошулмасына разысынгыз?

2) Вы за восстановление действия Конституции Республики Крым 1992 года и за статус Крыма как части Украины?

2) Ви за відновлення дії Конституції Республіки Крим 1992 року і за статус Криму як частини України?

2) Сиз Кырым Джумхуриетининъ 1992 сенеси ичюн Анаяасы амельге кечирильмеси ве Кырым Украина къысмы оларакъ статусы ичюн?

Бюллетень, в котором оставлены неотмеченными или отмечены оба варианта ответа, считается недействительным.

Бюллетень, в якому залишено непозначеними або позначено обидва варіанти відповіді, вважається недійсним.

Къайд этильмеген я да эки вариант къайд этильгени заманда бюллетень керчек

Рис.17.14. Образец бюллетеня на референдуме о статусе Крыма в 2014 г.

Таблица 17.3. Итоги референдума в Крыму 2014 г.

Выбор	Автономная республика Крым		Севастополь	
	Голоса	%	Голоса	%
За воссоединение Крыма с Россией	1 233 002	96.77	262 041	95.60
За сохранение статуса Крыма как части Украины	31 997	2.51	9 250	0.99
Недействительных бюллетеней	9 097	0.71	2 810	1.03
Зарегистрированных избирателей / явка	1 534 815	83.01	306 258	89.50

Несмотря на сходства референдумов 1938 г. и 2014 г., от которых у многих в Европе «фантомные боли», справедливости ради, следует отметить их существенные отличия:

- Австрия на момент проведения аншлюса была самостоятельным государством в отличие от Крыма, который в 1954 г. «подарили» Украинской ССР (26 апреля 1954 г. Верховный Совет СССР принял закон «О передаче Крымской области из состава РСФСР в состав УССР»);

- референдум в Австрии проводился после ее оккупации и подписания «официального» закона о воссоединении Австрии с Германией.

5) Механические и электромеханические устройства для голосования. Наибольшее распространение такая практика получила в США. Отчасти это объясняется тем, что в этой стране, как правило, в один день проводилось голосование по многим кандидатам на выборные должности: федеральные и местные (выборщики президента, члены палаты представителей, депутаты легислатур штатов, судьи, шерифы, члены органов местного самоуправления и др.). Подобная практика вызвала естественную необходимость рационализации процесса голосования в целях экономии времени.

Первую попытку предложить обществу машину, с помощью которой могло производиться персональное тайное голосование, предпринял знаменитый ученый и изобретатель Эдисон. В 1869 г. он запатентовал электромеханическое устройство, предназначенное для регистрации голосов (патент № 90646, англ. electric vote-recorder – **электрический регистратор голосов**).

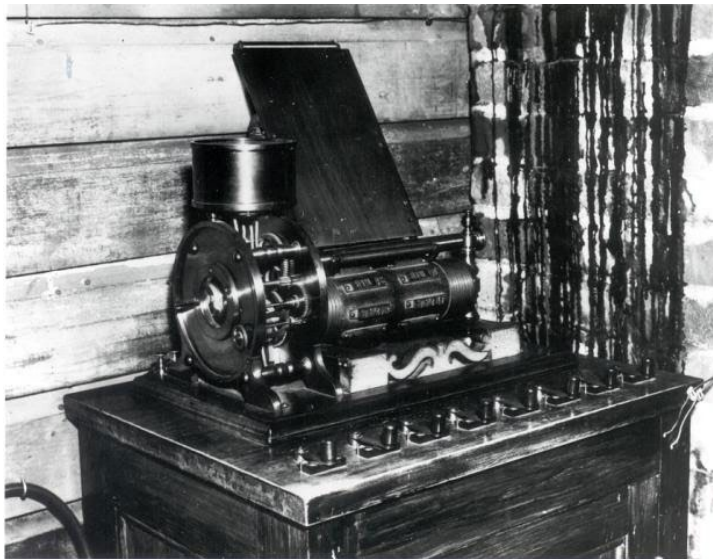


Рис.17.15. Электрический регистратор голосов Эдисона

В конце XIX в. американские изобретатели предложили несколько **рычажно-счетных аппаратов** (РСА) для голосования: А. Беранек (1881 г., патент № 248130, англ. voting apparatus – аппарат для голосования), Дж. Майерс (1889 г., патент № 415549, англ. voting machine – машина для голосования), А. Гиллеспи (1899 г., патент № 628905, англ. voting machine – машина для голосования).

Устройство Майерса впервые было опробовано в г. Локпорте. С 1892 г. голосование с помощью РСА было узаконено в штате Нью-Йорк, а затем и в других штатах. В начале XX в. широкое применение в штатах получило устройство Гиллеспи.

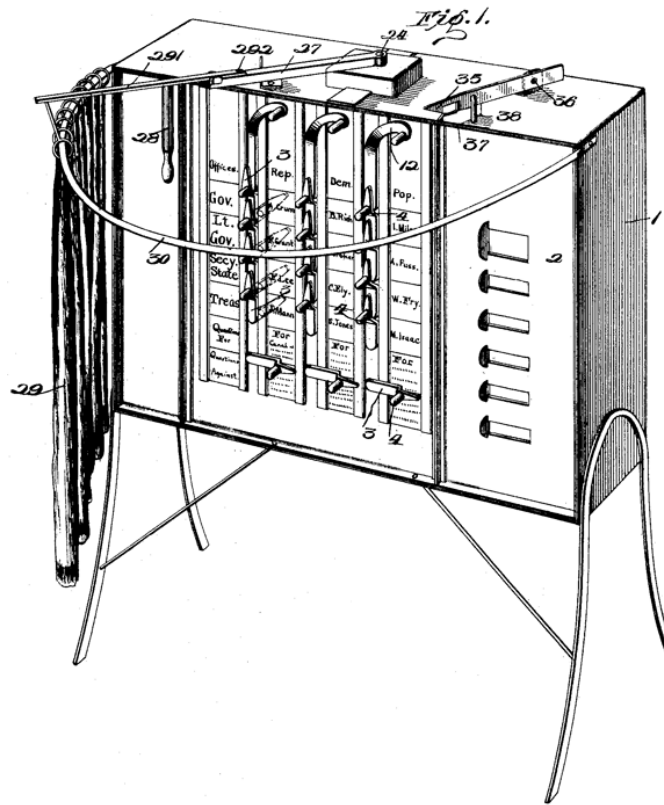


Рис.17.16. Машина для голосования Гиллеспи

При голосовании избиратель должен был повернуть верхний рычаг (28), который с одной стороны закрывал его ширмой, а с другой – инициировал процедуру голосования. Затем избиратель должен был сделать свой выбор, повернуть малые рычажки (3) около своих кандидатов. Возврат верхнего рычага влево приводил к учету сделанного избирателем выбора и возврату малых рычажков в вертикальное положение.

РСА активно используются и в наше время. В частности на всех президентских выборах США начала XXI в.

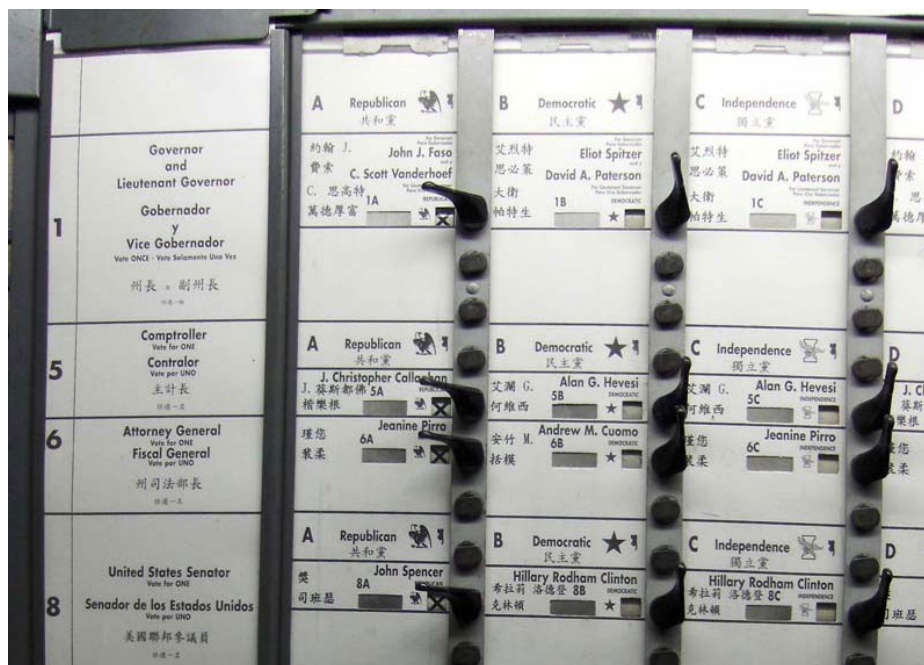


Рис.17.17. РСА на выборах в штате Нью-Йорк (2007 г.)

б) Электронное голосование - голосование, подразумевающее как электронные средства голосования, так и технические электронные средства подсчёта голосов.

Необходимость ускорения процесса подсчета голосов привела к широкому использованию электронных устройств в избирательном процессе. В первых системах электронного голосования вместо бюллетеня использовались **перфокарты** (англ. punchcard). Избирателю вместо указания своего выбора ручкой или маркером необходимо было сделать дырку в бюллетене, а заодно и на перфокарте, подкладываемой под него.

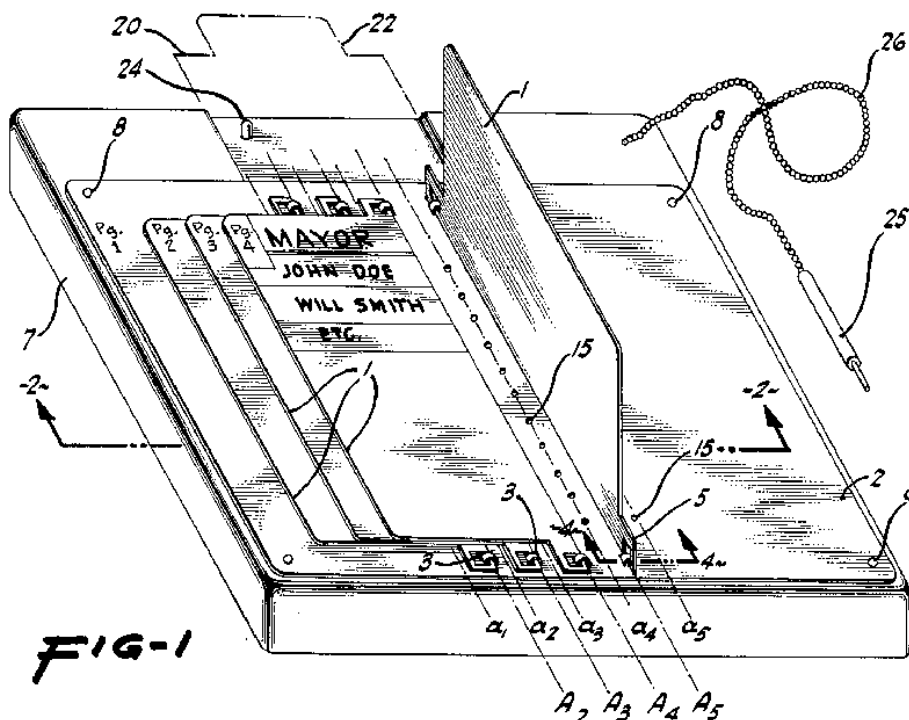


Рис.17.18. Устройство для регистрации голосов на базе перфокарт
(Дж. Харрис, 1965 г., патент № 3201038)

В отверстие сверху по направляющей (20-22) вставлялась перфокарта, после чего в бюллетене (1) с помощью дырокола (25) делалась дырочка в черном кружке (15) напротив своего кандидата. На перфокарте столбцы соответствуют разным видам выборов (президента, губернатора, сенатора и т.д.), а строки – кандидатам (партиям). Сделав выбор кандидата на одну должность (например, президента), избиратель должен перевернуть страницу (1) **бюллетеня-бабочки** (англ. butterfly ballot) и выбрать кандидата на другую должность (например, губернатора). Отмеченные таким образом перфокарты опускались в избирательную урну для последующей автоматической обработки специализированными сканерами.

Первые перфокарты для голосования были использованы в 1964 г. в двух округах штата Джорджия на первичных президентских выборах, а в 1996 г. число проголосовавших таким образом избирателей составило 37%.

На следующем рисунке показано одно из таких устройств «Votomatic», которое использовалось для голосования на выборах президента США в штате Флорида.

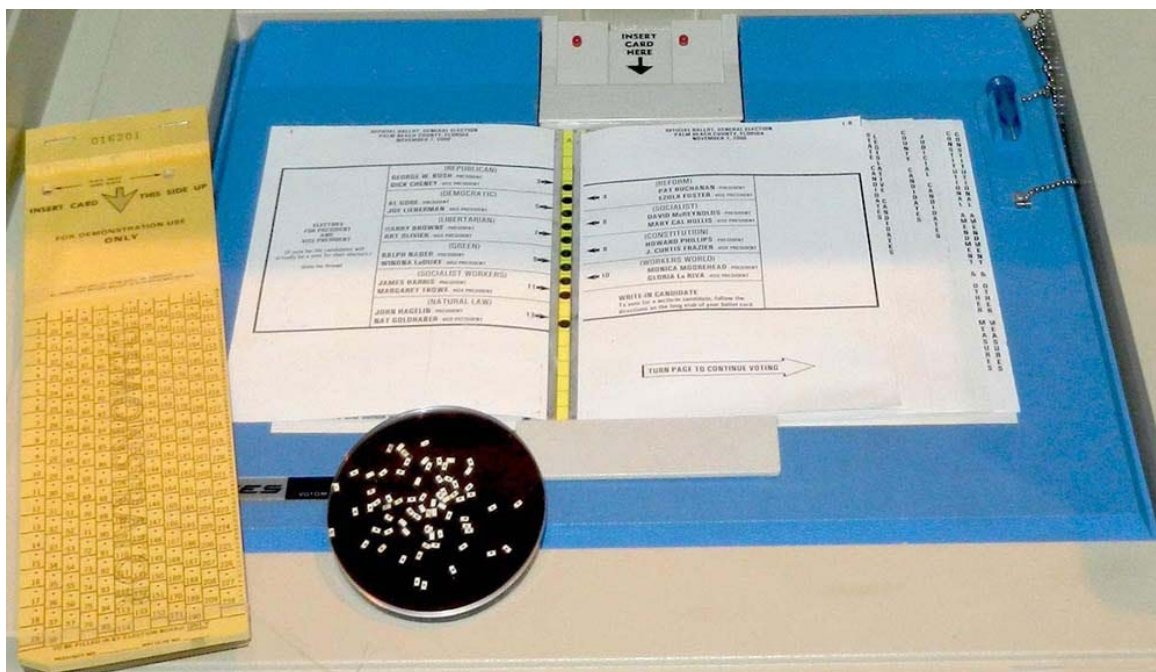


Рис.17.19. Устройство, перфокарта и бюллетень для голосования на выборах президента США (2000 г.)

Практически одновременно с перфокартными системами стали применяться **сканеры** для автоматической обработки традиционных бумажных бюллетеней. Впервые подобные устройства были использованы на избирательных участках в 1962 г. в округе Керн (штат Калифорния).



Рис.17.20. Портативный сканер бюллетеней фирмы «Dominion Voting»

По состоянию на 2011 г. в 41 штате США применяются оптические комплексы для электронного голосования (наряду с сенсорными), а в 17 из них они используются на всех избирательных участках. В мае 2010 г. на выборах Президента и Конгресса **Филиппин** прошли первые в Юго-Восточной Азии выборы с использованием оптических комплексов, количество которых на избирательных участках страны составило 82 200 шт.

В 1975 г. на выборах в штате Иллинойс впервые были использованы **кнопочные** аппараты с прямой электронной записью. В настоящее время подобные аппараты широко используются в **Бразилии** и **Индии**. Так, в Бразилии на выборах муниципалитетов в 2000 г. и Президента в 2002 г. кнопочные аппараты стали применяться по территории всей страны. Процесс голосования на бразильских выборах 2010 г. Президента, губернаторов штатов и парламентариев был полностью компьютеризирован. В том же году в 60 муниципалитетах страны был проведен эксперимент по биометрической идентификации избирателей.



Рис.17.21. Бразильский кнопочный аппарат для голосования и сканер отпечатков пальцев (фирма «Diebold», США)



Рис.17.22. Индийский кнопочный аппарат для голосования

Для обеспечения голосования слепыми гражданами на современных бразильских и индийских кнопочных аппаратах нанесены надписи шрифтом Брайля.



Рис.17.23. Надписи шрифтом Брайля на аппарате для голосования

Другой разновидностью аппаратов с прямой записью являются **сенсорные** устройства для голосования. С начала XXI в. во многих странах стали проводиться эксперименты по голосованию с помощью подобных устройств. Наибольшее распространение они получили в **Венесуэле**, где на референдуме 2004 г. и президентских выборах 2006 г. использовались практически на всех избирательных участках.



Рис.17.24. Венесуэльские сенсорные устройство и планшет для голосования (фирма «Smartmatic», США)

Устройство для голосования, помимо сенсорного экрана, включает в себя также принтер бюллетеней («чеков»), которые следует опускать в избирательную урну. Подсчет голосов на избирательных участках выполняется как автоматически, так «по-старинке» - подсчетом бумажных бюллетеней.

Большинство сканеров бюллетеней и сенсорных устройств подразумевают их использование в составе специализированных комплексов для автоматического подсчета голосов и передачи результатов голосования в центральную избирательную комиссию посредством Интернета. В то же время в мире набирает обороты практика **Интернет-голосования** на специализированных сайтах или с помощью специального программного обеспечения. Избиратели могут сделать свой выбор не только на избирательных участках, оборудованных компьютерами, но и в любом удобном месте: интернет-кафе, дома или со смартфона.

В **США** первым опытом Интернет-голосования стали предварительные выборы Демократической партии в штате Аризона в марте 2000 г. В феврале 2008 г. было организовано Интернет-голосование на первичных выборах для избирателей-демократов, находящихся за границей. Такой вид голосования использовался на парламентских выборах (**Австралия**, 2001 г.), муниципальных выборах в Ливерпуле (**Великобритания**, 2002 г.), выборах главы Новой демократической партии (**Канада**, 2003 г.), выборах депутатов Европейского парламента (**Нидерланды**, 2004 г.), референдуме по Европейской конституции (Баскская автономия **Испании**, 2005 г.).

Наибольшее распространение Интернет-голосование получило в Швейцарии и Эстонии.

В **швейцарском** кантоне Женева для Интернет-голосования на референдумах используются избирательные карточки. Перед голосованием избиратель, предъявив паспорт, может взять в своем почтовом отделении карточку для электронного голосования с уникальным номером и секретным кодом, скрытым под защитным слоем. Далее, на сайте электронного голосования кантона следует ввести номер карточки, поставить галочки напротив нужных вариантов вопросов референдума, затем, убрав с карточки защитный слой, ввести секретный код и получить электронное подтверждение голоса, которое в дальнейшем может быть проверено в администрации кантона. Карточка является одноразовой и перед каждым голосованием за ней надо ходить на почту.

В 2005 г. **Эстония** стала первой страной, предложившей общенациональные выборы местных органов власти через Интернет. Другая статистика по Интернет-голосованию в Эстонии приведена в следующей таблице.

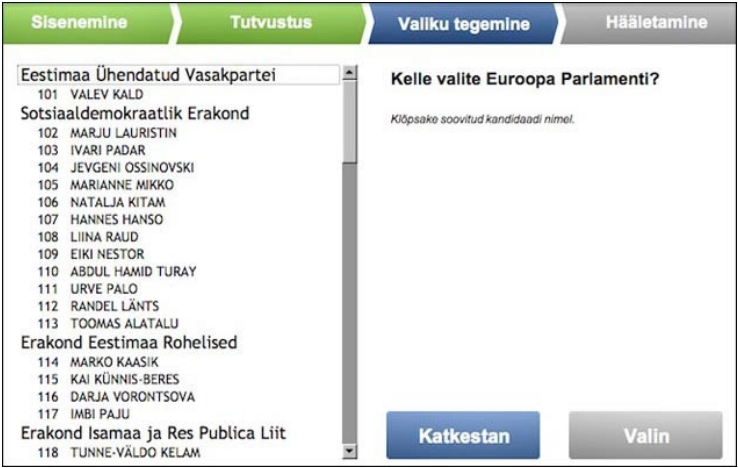
Таблица 17.4. Интернет-выборы в Эстонии

Дата	Тип выборов	Количество проголосовавших через Интернет
Январь 2005 г.	Эксперимент	703
Октябрь 2005 г.	Выборы в органы местного самоуправления	9 317
Февраль 2007 г.	Выборы в Эстонский парламент	30 275
Весна 2009 г.	Выборы в Европейский парламент	58 669
Октябрь 2009 г.	Выборы в органы местного самоуправления	104 413
Март 2011 г.	Выборы в Эстонский парламент	140 846
Май 2014 г.	Выборы в Европейский парламент	103 151

В Эстонии для Интернет-голосования вне избирательных участков необходимо с сайта Республиканской избирательной комиссии www.valimised.ee скачать специальное ПО, а также иметь ID-карту гражданина Эстонии с кардридером, подключаемым к компьютеру, или SIM-карту Mobiil-ID, вставляемую в сотовый телефон. В начале процедуры голосования избиратель проходит двухфакторную аутентификацию (по карте и PIN-коду).



а) выбор способа аутентификации



б) выбор кандидата

Рис.17.25. Копии экранов при Интернет-голосовании в Эстонии

Прием голосов по Интернету выполняется в течение нескольких дней до дня выборов и у избирателя имеется возможность изменить свое мнение (переголосовать). В том случае, если во время предварительного голосования избиратель использовал также бумажный бюллетень, то результаты электронного голосования аннулируются. В день выборов изменить голос, поданный на предварительной стадии, невозможно. Проверить, учтен ли его электронный голос, избиратель может с помощью смартфона или в день выборов на избирательном участке. Разработчики ПО и члены Республиканской избирательной комиссии заверяют, что электронное голосование полностью анонимно и приводят в качестве аналогии голосование по принципу двух конвертов – внешнего идентификационного и внутреннего анонимного [www.valimised.ee/ru/uldkirjeldus]. Даже при аннулировании голоса выбор избирателя остается засекреченным.

SMS-голосование активно используется в различных конкурсах, телевизионных ток-шоу, при опросах общественного мнения и т.п. В 2002-2003 гг. на местных выборах нескольких графств Великобритании были проведены тестовые эксперименты по электронному голосованию, включая голосование посредством Интернет, SMS, телефона и даже интерактивного цифрового телевидения.

III. По необходимости волеизъявления голосующим.

Как правило, голосование является правом гражданина, но на протяжении всей истории встречаются примеры, когда голосование вменялось в обязанность.

В ряде полисов Древней Греции существовал закон: если гражданин уклонялся от участия в выборах, то его лишали гражданства и изгоняли, объясняя это решение тем, что полису не нужен гражданин, которому безразлична судьба его государства.

Первыми странами, которые посредством законодательного регулирования ввели обязательное голосование, были: Бельгия – в 1892 г., Аргентина – в 1914 г. и Австралия – в 1924 г.

По Конституции Эквадора, голосование объявляется обязательным для умеющих читать и писать в возрасте от 18 до 65 лет и факультативным – для остальных. Аналогичное положение есть в Конституции Бразилии, только верхняя возрастная планка поднята до 70 лет.

В статье 31 Конституции Перу указано, что голосование осуществляется лично и является равным, свободным, тайным и обязательным для граждан с 18 до 70 лет. Для граждан старше указанного возраста участие в голосовании оставляется на их усмотрение.

В некоторых странах обязательность голосования закреплена на законодательном уровне. Неучастие в голосовании без уважительных причин влечет за собой определенные санкции.

Таблица 17.5. Санкции к гражданам, не участвующим в голосовании [17, 50]

Санкция	Пример
Объяснение	Предполагает предоставление избирателем информации о законных причинах его неучастия в выборах во избежание дальнейших санкций.
Штраф	Бельгия – 50 евро. В случае повторного нарушения – 125 евро. Швейцария – 3 швейцарских франка. Аргентина – 10–20 аргентинских песо. Перу – 20 перуанских новых соль. Эквадор – 200 долларов США. Египет – 100 египетских фунтов.
Тюремное заключение	Австралия – за неисполнение судебного определения об оплате штрафа за неучастие в выборах грозит тюремное заключение на 1-2 дня. Пакистан – в худшем случае каторжные работы до 5 лет. Греция – от 1 месяца до 1 года с лишением званий и должностей.
Частичное или полное лишение гражданских прав	Бельгия - если гражданин не участвует в голосовании, по крайней мере, на четырех выборах, тогда в течение 15 лет он лишается гражданских прав. Перу - гражданин должен представить карточку голосования с отметкой (печатью) о голосовании на выборах. Этот штамп требуется для того, чтобы получить определенные услуги и товары в некоторых государственных учреждениях. Боливия - гражданин не сможет получить свою зарплату из банка в течение 3 месяцев после выборов, если он не может показать доказательство голосования (карточку со штампом).
Иные санкции	Бельгия – могут быть проблемы с получением работы в государственном секторе. Аргентина – лишение на 3 года права занимать государственные должности. Италия - трудно получить место для своего ребенка в детском саду и т.п. Австралия – неисполнение судебного определения об оплате штрафа за неучастие в выборах может быть наказано общественными работами или арестом имущества.

V. По количеству голосов, подаваемых голосующим.

Равноправное голосование заключается в возможности одинакового (равного) влияния каждого избирателя на исход выборов. В подавляющем большинстве случаев равноправное голосование осуществляется по принципу «один голосующий – один голос» (**система с одним непередаваемым голосом**). При выборе из нескольких кандидатур может возникнуть ситуация, когда избранный кандидат отражает мнение меньшинства избирателей. С целью устранения этой проблемы был предложен ряд выборных методик с **несколькими голосами**, позволяющих более адекватно учитывать мнения всех участников выборного процесса. В них, как правило, избиратель наделен несколькими голосами, но их количество одинаково для всех и строго регламентировано.

В 1831 г., когда в Британии обсуждался билль о реформе, была предложена **блоковая система ограниченного вотума (голоса)**. В 1867 г. она применялась в 12 округах королевства и в Лондоне. Суть системы заключается в том, что в одном округе избирателям дается право проголосовать за число кандидатов, меньшее общего числа подлежащих избранию (например, за двух при трех кандидатурах и т.п.). Такая система применялась в Бразилии (1875 - 1881 гг.), Испании (с 1878 г.), Португалии (с 1884 г.), Италии (1882 г.), а также при выборах членов Совета Федерации Федерального Собрания Российской Федерации (1993 г.).

Другим новшеством являлась **блоковая система неограниченного вотума (кумулятивного голоса)**. Избиратель наделялся числом голосов, равным количеству избираемых депутатов. Но при этом он имел право распределить голоса по своему усмотрению. Например, имея 3 голоса, он мог отдать их трем кандидатам (по одному на каждого), двум или подать все три голоса за одного кандидата. Эта система была предложена в 1853 г. Джеймсом Гартом Маршаллом (Великобритания) для парламентских выборов, но реально применялась при избрании членов школьных советов.

Наиболее показательно применение системы кумулятивного голоса в штате Иллинойс (США), начиная с 1870 г. и до недавнего времени.

Три представителя избираются от каждого округа по выборам в Генеральную ассамблею [штата] сроком на 2 года. В каждом из округов политическими партиями выдвигается не менее двух кандидатов в палату представителей. В голосовании на выборах в палату представителей и при выдвижении кандидатов каждый избиратель имеет три голоса, которые он вправе отдать за одного кандидата либо разделить поровну между тремя кандидатами.

Конституция штата Иллинойс (1970 г.)

Еще одна разновидность голосования с возможностью подачи нескольких голосов практикуется при решении менее значимых вопросов, чем выборы органов власти. Например, при выборе победителей конкурсов, опросе общественного мнения и т.п. Для такого голосования обычно используются телефонные звонки, SMS-сообщения или голосование на сайте. При этом могут устанавливаться различного рода ограничения (например, голосование с одного телефона, IP-адреса или с помощью полученного по электронной почте идентификатора не чаще одного раза в день). Следует отметить, что подобного рода ограничения при электронном голосовании, в случае необходимости, могут быть легко обойдены квалифицированным пользователем.

При **неравноправном голосовании** избиратели изначально находятся в неравных условиях. Часть избирателей оказывается в привилегированном положении по сравнению с другими в силу своего сословного, имущественного, должностного, территориального и т.п. положения.

В системах с **дополнительными голосами** у избирателей имеется разное количество голосов. Показательна в этом плане избирательная система Бельгии XIX – XX вв. В 1848 г. собственникам крупного состояния (свыше 2000 франков) предоставлялось право второго, дополнительного голоса. С 1893 г. в результате очередной избирательной реформы некоторые граждане стали обладать дополнительными голосами на основании семейного и имущественного положения, полученного образования или профессиональной подготовки.

Таблица 17.6. Численность избирателей, голосовавших на выборах в палату депутатов Бельгии в 1900-1901 гг.

Количество избирателей, чел.			Число голосов	
имеющих		Всего		
1 голос	2 голоса			3 голоса
915 673	318 099	239 181	1 472 953	2 269 414

Во Франции с 1820 г. подданные, уплачивающие не менее 1000 франков прямого налога, получали право подачи второго голоса на выборах, после революции 1830 г. - 500 франков.

Согласно Королевского указа 1849 г. и Конституционной хартии Пруссии 1850 г. для выборов депутатов нижней палаты ландтага (главного представительного органа) избиратели Пруссии были поделены на три группы, в зависимости от суммы уплачиваемых ими налогов. К первой, включавшей наиболее состоятельных граждан, относилось примерно 4-5 % всех избирателей, ко второй - менее состоятельные граждане (12-13 %) и к третьей – остальные, кто платил незначительные налоги (81-85 %). Т.к. представительство депутатов от каждой группы в ландтаге было одинаковым, то голос «состоятельного» избирателя равнялся примерно 18 голосам «бедного» избирателя. В 1863 г. Бисмарк (тогда министр-президент Пруссии) издал меморандум, в котором предложил кардинальным образом пересмотреть принципы сосуществования немецких земель. В 1866 г. представителям Пруссии в германских государствах была направлена депеша, в которой Бисмарк так объяснял политику своего правительства:

Искусственная система не прямых и классовых выборов гораздо опаснее тем, что препятствует общению верховной власти с теми здоровыми элементами, которые образуют ядро и массу народа. В стране с монархическими традициями и лояльными чувствами всеобщее избирательное право, устраняя влияние либеральных буржуазных классов, будет приводить и к выборам в монархическом духе ... В Пруссии 9/10 народа верны королю и, лишь благодаря искусственному механизму выборов, лишены возможности проявить свое мнение.

Отто фон Бисмарк [Циркулярная депеша от 24 марта 1866 г.]

Существенное влияние на представительство в выборных органах может оказать неравномерная разбивка на избирательные округа. Например, в 1903 г. округ Берлин-VI насчитывал 696608 жителей, а округ Шаумбург-Липпе – 43132. Указанные округа избирали по одному депутату рейхстага. Т.о. голос избирателя малого округа был примерно в 16 раз значимей голоса избирателя округа столицы.

В ряде штатов США вплоть до 1964 г. практиковалось создание неравных избирательных округов, позволявших избирать больше депутатов от консервативно настроенного сельского населения, чем от того же числа горожан-избирателей (причем в отдельных случаях в сельских избирательных округах проживало почти в два раза меньше избирателей, чем в городских). Только в 1964 г. Верховный Суд США запретил такую практику.

Согласно статье 11 ФЗ «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации» отклонение от равенства избирательных округов по числу избирателей допускается до 10%, в труднодоступных и отдаленных районах – не более 15%. По германскому законодательству численность населения избирательного округа не должна отличаться от средней более чем на 25%.

При выборах на основе куриального (корпоративного) представительства принцип равного избирательного права для всех избирателей не принимается во внимание, хотя он и соблюдается для избирателей внутри курии. Под куриями понимают социальные группы, выделяемые по какому-либо признаку. Для каждой курии выделяется определенное количество мандатов (при этом количество мандатов вовсе не должно быть пропорционально численности группы), которые и получают избранные внутри курии представители. Куриальное представительство было широко распространено в Средние века, но практикуется и в настоящее время, в основном, при формировании консультативных и экспертных коллегиальных органов (например, Государственный совет Словении).

Согласно «Положению о выборах в Государственную думу» 1907 г. 1 выборщик приходился на 230 землевладельцев, 1000 избирателей первой городской курии (состоятельные граждане), 15000 избирателей второй городской курии, 60000 крестьян и 125000 рабочих (по приблизительным подсчетам Ф.М. Калинычева).

В настоящее время во многих странах при формировании представительных органов (в частности, парламентов) действует пропорциональная избирательная система, которая является аналогом куриальной. При проведении выборов по пропорциональной системе депутатские мандаты распределяются между списками кандидатов (партиями, объединениями и т.п.) пропорционально голосам, поданным за списки кандидатов, если они преодолели процентный барьер. В России пропорциональная избирательная система применялась на выборах в Государственную думу с 2007 г. по 2011 г. С 2014 г. в России принята смешанная система выборов в Государственную Думу: 225 депутатов избираются по мажоритарной системе, 225 - по пропорциональной.

Для небольших собраний (до нескольких сотен участников) при принятии решений практикуются системы с правом **решающего голоса**. В том случае, когда по итогам голосования ни одно из предлагаемых решений не набирает необходимого количества голосов (как правило, равное количеству голосов за альтернативные решения), окончательный вердикт выносит председательствующий. В частности:

При решении вопросов на заседании совета директоров (наблюдательного совета) общества каждый член совета директоров общества обладает одним голосом. Уставом общества может быть предусмотрено право решающего голоса председателя совета директоров общества при принятии советом директоров общества решений в случае равенства голосов членов совета директоров общества.

68 статья ФЗ «Об акционерных обществах»

На федеральном уровне право решающего голоса закреплено при голосовании на референдуме:

При принятии решений избирательной комиссией, комиссией референдума в случае равного числа голосов «за» и «против» голос председателя избирательной комиссии, комиссий референдума является решающим.

28 статья ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»

17.1.3. Ограничения избирательных прав

Граждане, участвующие в избирательном процессе, могут обладать **активным** и **пассивным** избирательным правом. Первое подразумевает право избирать, второе – быть избранным. Для обладания этими правами гражданин должен удовлетворять ряду требований, причем для кандидатов на выборное место эти требования более жесткие.

Существовавшие в XIX в. избирательные цензы (в первую очередь имущественный ценз) серьезно ограничивали электорат различных государств. Так, в Англии до избирательной реформы 1832 г. активным избирательным правом обладало 4.4% взрослого населения страны, в результате ее проведения – 7.5%, а после проведения реформы 1867 г. – 16.4%.

- по гражданству;
- по возрасту;
- по оседлости (сроку проживания на территории);
- по состоянию здоровья;
- по решению суда за совершенные преступления;
- по имущественному положению;
- по социальному статусу (сословному или классовому положению);
- по служебному положению;
- по образованию;
- по половому признаку;
- по повторному избранию (для кандидатов);
- иные ограничения.

На выборах органов государственной власти ограничение избирательных прав по гражданству прописано в законодательствах всех стран. Неграждане, как правило, не имеют прав избирать и быть избранными в представительные органы власти.

После распада СССР в странах Прибалтики (Латвия, Литва и Эстония) значительная часть местного населения оказалась пораженной в избирательных правах. В частности, согласно Закона о гражданстве Латвии (от 22 июля 1994 г.), совокупность изначальных граждан составляют лица, бывшие гражданами Латвии до 17 июня 1940 г., а также их потомки, прошедшие регистрацию. К началу 2014 г., по данным Регистра жителей, в Латвии проживало 282 876 неграждан (13,0 % жителей), из них 65,7 % - русские (31,7 % русских Латвии), 13,6 % - белорусы (51,9 % белорусов Латвии), 9,7 % - украинцы (52,3 % украинцев Латвии), латыши – 0,3 % (0,06 % живущих в стране латышей). Парадоксальная ситуация сложилась после вступления Латвии в ЕС. Ряд занятий, по-прежнему недоступных для неграждан, стал доступным для граждан ЕС. В частности, это касается права выставлять свою кандидатуру и голосовать на местных выборах, что разрешено гражданам ЕС с полугодовым сроком проживания в Латвии.



б) паспорт негражданина

Рис.17.26. Латвийские паспорта

В 2006 г. в **российское** законодательство были внесены изменения, запрещающие иметь двойное гражданство лицам, замещающим государственные и муниципальные должности. Двойное гражданство или вид на жительство в другой стране нельзя, в частности, иметь Президенту РФ, секретарю и членам Совбеза, депутатам Госдумы, членам Совета Федерации. Позднее были приняты поправки, запретившие иметь второй паспорт Председателю правительства и вице-преьерам. Скрытие информации о наличии второго паспорта грозит штрафом в размере до 200 000 рублей, либо обязательными работами на срок до 400 часов.

В целом ряде стран иметь двойное гражданство вообще запрещено (например, в США и Германии).

Данное ограничение, как и гражданство, характерно для всех стран.

В **России** возрастной ценз для активного избирательного права (18 лет) был установлен сразу же после Октябрьской революции и закреплён в Конституции РСФСР 1918 г. В большинстве других стран возрастной ценз для активного избирательного права был снижен до 18 лет гораздо позже. В частности, в США - в 1971 г., в Великобритании, ФРГ и Франции - в 1974 г., в Италии - в 1975 г.

Таблица 17.7. Возрастной ценз для активного и пассивного избирательного права

Страна	Избиратель	Президент
Россия	18	35
Франция	18	23
США	18	35
ФРГ	18	40
Италия	18	50
Бразилия	16	35

Китай	18	45 (Председатель КНР)
Куба	16	18 (Председатель Госсовета)

Конституция **Бразилии** 1988 г. предоставляет гражданам право голоса с условием обязательного участия в голосовании с 18 лет, но граждане, достигшие 16 лет и желающие принять участие в голосовании добровольно, согласно этой Конституции могут зарегистрироваться в качестве избирателей. Интересно также, что Конституция Бразилии 1988 г. устанавливает не только нижнюю границу возрастного ценза, но и верхнюю. По этой Конституции граждане старше 70 лет участвуют в голосовании лишь в том случае, если сами по своей инициативе подадут заявку о регистрации в качестве избирателей.

Во многих организация для кандидатов на выборные должности может применяться верхняя возрастная планка.

3) По оседлости (сроку проживания на территории).

Для активного избирательного права он составляет обычно от одного месяца до двух лет. Этот ценз означает, что гражданин, чтобы получить доступ к избирательной урне, должен постоянно прожить на территории данного избирательного округа установленный промежуток времени, предшествующий голосованию. Для пассивного избирательного права могут вводиться и более жесткие требования. Так, в **России** гражданин, чья кандидатура выставляется на пост президента, должен постоянно прожить на территории страны не менее 10 лет, предшествующих выборам, в **США** – 14 лет.

Активным избирательным правом обладают все граждане **Германии**, проживающие в данном избирательном регионе не менее 3 месяцев. Если гражданин ФРГ переселился из данного избирательного региона, где он проживал не менее 3 месяцев, в иную страну ЕС, то он сохраняет активное избирательное право независимо от длительности проживания в этой стране. Если страна, в которую переселился немецкий гражданин, не входит в ЕС, то он сохраняет активное избирательное право лишь в течение 10 лет после выезда из Германии.

Мексиканскими законами предусмотрено, что все граждане, отвечающие требованиям, обязаны зарегистрироваться в Национальном реестре избирателей, для чего необходимо обратиться в местное отделение по месту проживания. При этом гражданин получает постоянное удостоверение, дающее ему право голосовать на выборах. В случае переезда на новое место жительства внесенный в реестр гражданин должен в течение месяца сообщить об этом.



Рис.17.27. Удостоверение избирателя в Мексике

Выдача избирательских удостоверений практикуется во многих странах Южной Америки и Азии. В некоторых странах Азии (в частности в **Индии**) для недопущения повторного голосования дополнительно используется маркировка пальцев избирателей стойкими чернилами.



Рис.17.28. Индийские женщины, принявшие участие в голосовании

4) По состоянию здоровья.

Умалишенные (слабоумные, психически больные) граждане лишены права голосования в силу невозможности сознательного волеизъявления. Является или нет какой-либо человек умалишенным, устанавливается судебными органами на основе результатов специальной экспертизы в строго определенном законодательством порядке.

5) По решению суда за совершенные преступления.

В одних странах избирательное право гражданина приостанавливается (иногда он вообще лишается избирательного права) по решению суда в случае совершения указанных в законе преступлений, а в других - автоматически в силу осуждения гражданина судом за любой вид преступления.

6) По имущественному положению.

В Древних Афинах в VI в. до н.э. по реформе Солона было введено разделение избирателей на 4 класса:

- пентакосиомедимны - получающие со своей земли 500 мер (1 мера = 52.5 л) сухих и жидких продуктов;
- всадники - получающие 300 мер или, по утверждению некоторых, содержащие коня;
- зевгиты - получающие 200 мер;
- феты – остальные. Феты не могли быть избраны на государственную должность.

Во Франции согласно нормам Конституционной Хартии 1814 г., активным избирательным правом обладали лица, платившие в год не менее 300 франков прямых налогов, пассивным - не менее 1000 франков. После Парижского восстания 1830 г. имущественный ценз для избирателей сократился с 300 до 200 франков прямых налогов (для лиц, имеющих образование - до 100 франков).

В результате парламентской реформы 1832 г. в Англии активным избирательным правом обладали:

- сельские жители, имеющие свободное земельное держание (фриголды) и не менее 40 шиллингов годового дохода с недвижимой собственности;
- арендаторы земли (копигольдеры), вносящие в год не менее 5 фунтов арендной платы;
- фермеры, нанимающие землю на срок свыше 40 лет и ежегодно платящие за нее не менее 5 фунтов стерлингов;
- городские домовладельцы или те, кто платил не менее 10 фунтов квартирной платы в год.

В XIX в. избирателям штатов Мэн и Нью-Гэмпшир достаточно было не значиться в списках получающих пособие по бедности.

Согласно «Акта о народном представительстве» 1928 г. в Британии право голоса получили все подданные (мужчины и женщины) достигшие 21 года, прожившие в округе не менее 3 месяцев, владеющие в нем недвижимостью или «помещением для деловых занятий».

В настоящее время имущественный ценз применяется для кандидатов на должность. Например, в Великобритании лицо, баллотирующееся в Парламент, должно внести залог в 500 фунтов, которые не возвращаются, если кандидат получил менее 5% голосов избирателей.

7) По социальному статусу (сословному или классовому положению).

В Англии середины XV в. для того, чтобы войти в Палату общин, нужно было принадлежать к «благородному» сословию, как минимум во втором поколении. По статуту 1445 г. избранию в парламент подлежали только «благородные» лица: «Достойные рыцари, сквайры, джентльмены по рождению» и ни в коем случае не йомены (англ. yomen - в XIV-XVIII вв. крестьянин, ведущий самостоятельное хозяйство). Там же, согласно «Закона о дисквалификации священников из членства в Палате общин» 1801 г. и «Закона об улучшении положения Римской католической церкви» 1829 г.: «любое лицо в сане диакона, кюре, епископа и иных наряду со священнослужителями Шотландской и Римской католической церковей не могут быть избраны в Палату общин».

В средневековой Франции традиционно была распространена идея о делении общества на «три сословия»: «молящихся» (духовенство), «сражающихся» (рыцари, дворяне) и «трудящихся» (крестьянство и прочие). Так, в Генеральных штатах 1789 г. духовенство представляли 291 депутатов, дворянство - 285, третье сословие - 578.

В России половина Государственного совета после реформы этого органа в 1906 г. и вплоть до его ликвидации в 1917 г. избиралась следующим образом: от губернских земских собраний - 34 члена; от съездов землевладельцев в неземских губерниях - 22 члена; от дворянских обществ - 18 членов; от православной церкви - 6 членов; от Академии наук и университетов - 6 членов; от организаций торгового купечества - 6 членов и от организаций предпринимателей-промышленников - 6 членов.

В Китае военнслужашие (к ним относятся также вольнонаемные: повара, машинистки и т.д.) избирают депутатов по специально создаваемым для них избирательным округам. Т.о., часть депутатского корпуса избирается исключительно военными и представляет военнслужаших как определенную социальную группу и обособленный коллектив.

После революции 1917 г. лишение избирательных прав носило довольно широкий характер. Конституция РСФСР 1918 г. определяла 7 категорий граждан, лишенных избирательных прав.

- лица, живущие на нетрудовой доход с целью извлечения прибыли;
- лица, живущие на нетрудовой доход, как то: проценты с капитала, доходы с предприятий, поступления с имущества и т.п.;
- частные торговцы, торговые и коммерческие посредники;
- монахи и духовные служители церковей и религиозных культов;
- служащие и агенты бывшей полиции, особого корпуса жандармов и охранных отделений, а также члены царствовавшего в России дома;
- лица, признанные в установленном порядке душевнобольными или умалишенными, а равно лица, состоящие под опекой;
- лица, осужденные за корыстные и порочащие преступления на срок, установленный законом или судебным приговором.

Общее количество лишенцев в СССР было сравнительно невелико, что видно по данным «Советской исторической энциклопедии» (1971 г.).

Таблица 17.8. Процент лишенных избирательных прав						
Год	1923	1924	1927	1929	1931	1934
В городах	8.2	5.0	7.7	8.5	4.9	2.4
В сельской местности	1.4	0.74	3.5	4.1	3.7	2.6

Позднее, с трибуны VIII Съезда Советов Сталин выступил против сохранения «лишенчества». Он отметил, что практика исключения отдельных лиц из числа избирателей была вызвана обстоятельствами гражданской войны: «Было время, когда эти элементы вели открытую войну против народа и противодействовали советским законам. Советский закон о лишении их избирательного права был ответом Советской власти на это противодействие. С тех пор прошло немало времени. За истекший период мы добились того, что эксплуататорские классы уничтожены, а Советская власть превратилась в непобедимую силу». Там же Сталин прочел отрывок из ленинской рукописи, относящейся к началу 1919 г., где, во-первых, была обоснована необходимость лишения избирательных прав «эксплуататоров», а во-вторых, говорилось об отмене этой вынужденной меры в будущем, «когда пролетарская государственная власть изберет другие способы подавления сопротивления эксплуататоров и введет всеобщее избирательное право без всяких ограничений». Новая Конституция СССР, отменяющая институт «лишенчества», была утверждена Съездом Советов и вступила в силу 5 декабря 1936 г.

В XX в. в странах Латинской Америки, ЮАР, Ираке, посткоммунистических государствах Восточной и Центральной Европы широко применялась люстрация. Люстрация (от лат. lustratio - обряд очищения младенца посредством жертвоприношений в Древней Греции и Древнем Риме) - законодательные меры и практика недопущения на государственную службу, аппарат государственного управления, правоохранительные органы, на иные важные посты и в учреждения системы образования лиц, которые неудобны правящим кругам по политическим мотивам. Предполагается, что осуществление люстрации должно придавать легитимность новой власти путём решительного разрыва с практикой старой власти, воспринимающей как преступная и неправовая.

В настоящее время люстрационные процессы идут в Украине. Президент Украины Петр Порошенко 9 октября 2014 г. подписал закон «Об очищении власти».

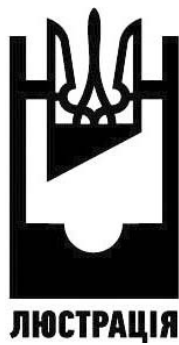


Рис.17.29. Эмблема Люстрационного комитета в виде гильотины

Законом вводится автоматический запрет на занятие определённых должностей в течение 10 лет со дня вступления закона в силу для лиц:

- занимавших определённые государственные должности в течение более чем 1 года (в период с 25 февраля 2010 г. по 22 февраля 2014 г.);
- занимавших указанные в законе должности менее 1 года и не уволившихся по собственному желанию (в период с 21 ноября 2013 г. по 22 февраля 2014 г.);
- занимавших руководящие должности в КПСС или компартиях союзных республик (начиная от секретаря районного комитета и выше), в комсомольских органах, сотрудники КГБ СССР;
- ранее осуждённых государственных служащих и сотрудников правоохранительных органов, которые сотрудничали с иностранными спецслужбами, призывали к нарушению территориальной целостности Украины или допустили нарушения прав и свобод человека, признанные Европейским судом по правам человека;
- государственных служащих, предоставившие недостоверную информацию о собственности в декларациях о доходах, а также те, чья собственность не будет соответствовать уровню зарегистрированных доходов за время их пребывания в должности.

По состоянию на 3 ноября 2014 г., на основании закона «Об очищении власти» было уволено 347 госслужащих.

8) По служебному положению.

Французская конституция 1848 г. установила, что «отправление какой-либо общественной оплачиваемой должности несовместимо с полномочиями представителя народа». По конституции 1852 г. чиновники могли стать депутатами, но с 1875 г. они не могли избираться в тех департаментах, где служили, и это существенно ограничивало их пассивное избирательное право. В начале XX в. лишь представители отдельных категорий должностных лиц могли быть депутатами нижней палаты (министры, послы, высшее духовенство, профессура).

В **Бельгии** с 1848 г. государственные служащие лишились права быть избранными в палату депутатов. В парламент Нидерландов не могли избираться священники, чиновники и военные.

Раздел 3 XIV Поправки к конституции США (1868 г.) лишил права «быть сенатором или представителем в Конгрессе, или выборщиком Президента и Вице-президента ...».

В **Великобритании** членами Палаты общин не могут быть депутаты иностранных парламентов и гражданские служащие, т.е. кадровые служащие министерств, центральных ведомств и дипломаты. Исключаются из числа членов парламента полицейские, кроме состава специальной полиции (к примеру, железнодорожная полиция), и лица, находящиеся на службе в вооружённых силах.

В **Перу** не могут баллотироваться на должности Президента и Вице-президента военнослужащие и лица, занимающие целый ряд должностей (министры, члены Конституционного суда, других судебных органов, избирательных органов, президент Центрального банка и т.д.), если только они не подали в отставку не позже чем за шесть месяцев до дня выборов.

В **Мексике** и **Бразилии** военнослужащие, находящиеся на действительной службе, не имеют пассивного избирательного права.

9) По образованию.

По **итальянскому** законодательству 1859–60 гг. избиратель должен был, как минимум, сдать экзамен по предметам, входящим в курс начальной школы. Главным образом, уметь читать и писать.

В XIX - начале XX вв. в местном законодательстве **американских штатов** активно практиковался образовательный ценз. Критерием грамотности считалось, например: умение читать по-английски конституцию США (Коннектикут); читать по-английски, уметь написать свое имя (Делавэр); читать и говорить по-английски (Вирджиния); умение писать по-английски, читать и толковать содержание конституции США (Миссисипи).

В **Испании** с 1878 г. независимо от уплаты налога, к выборам допускались члены королевских академий и ученые, имеющие университетские дипломы.

10) По половому признаку.

В разных странах женщины получили право голоса в разное время. Во многих странах это произошло до введения всеобщего избирательного права, из-за чего женщины определённых рас и социального положения не имели возможности голосовать.

В средневековой **Франции** и некоторых других европейских странах на городских выборах и собраниях имели право голосовать главы семейств независимо от пола. С 1718 по 1771 гг. во время Эры свободы, в **Швеции** было введено женское избирательное право. Оно распространилось только на женщин, состоящих в гильдиях и платящих налоги.

Проблема женского равноправия приобрела значительную актуальность во второй половине XIX в. Агитация европейской и американской общественности за социальное равноправие неизменно включала и требование о ликвидации гендерной дискриминации избирателей. Это явление получило название «суфражизм» (от франц./англ. suffrage - право голоса, избирательное право).

Первым регионом **США**, в котором женщины добились права избирать и быть избранными, стала в 1869 г. северо-западная территория Вайоминг, с 1890 г. - штат. Вторым штатом, установившим подлинное всеобщее избирательное право стал Колорадо (1893 г.).

Процесс распространения женского равноправия на всей территории США испытывал значительное противодействие консервативных кругов. По словам американского исследователя К. Лайфута, для того, чтобы вычеркнуть из конституции слово «мужчина», женщинам пришлось 52 года без передышки пропагандировать и агитировать. За это время пришлось провести:

- 56 референдумов среди избирателей-мужчин;
- 480 кампаний, чтобы распространить суфражистские поправки среди избирателей;
- 47 кампаний в законодательных собраниях штатов, чтобы включить эту поправку в конституции штатов;
- 227 кампаний, чтобы внести пункт об избирательном праве для женщин в партийные программы на партийных конференциях штатов;
- 30 кампаний, чтобы включить эту поправку в платформы партийных съездов при выдвижении кандидатов в президенты;
- 19 кампаний во время созывов Конгресса.

Усилия суфражистского движения привели к принятию XIX Поправки к конституции США (ратификация завершилась 18 августа 1920 г.), гласящей: «Право голоса граждан Соединённых Штатов не должно опспариваться или ограничиваться Соединёнными Штатами или каким-либо штатом по признаку пола».

В **Англии**, как и в США, борьба женщин за свои избирательные права была долгой и упорной. Не осталась в стороне и королева Виктория (1819 – 1901 гг.), написавшая открытое письмо, в котором резко осудила «эту безумную, злонамеренную и чреватую ужасными последствиями затею с "женскими правами"», добавив, что одна из ее активисток – леди Эмберли –

«заслуживает хорошей порки». Многочисленные акции и демонстрации принесли свои плоды и в 1888 г. женщины получили право голоса на выборах в советы графств, в 1894 г. - в приходские советы, а с 1918 г. – на парламентских выборах, включая право быть избранными. На первых послевоенных парламентских выборах, состоявшихся в декабре 1918 г., свои кандидатуры выставили 16 женщин, хотя избрана была только одна - графиня Маркиевич от Ирландии.

В Венгрии до Второй мировой войны возрастной ценз для женщин равнялся 30 годам. Кроме того, женщина допускалась к участию в выборах лишь в том случае, если у нее было не менее трех законнорожденных детей, причем все трое должны были быть живы, а сама женщина должна была иметь образование не менее шести классов.

В следующей таблице приведены данные по некоторым странам в области предоставления избирательных прав женщинам.

Таблица 17.9. Предоставление избирательных прав женщинам

Страна	Год
Новая Зеландия	1893
Австралия	1902
Финляндия	1906
Норвегия	1913
Дания	1915
Исландия	1915
Россия	1917
Германии	1918
Франции	1944
Италии	1946
Португалии	1945
Индия	1947
КНР	1949
Ливан	1952
Греции	1952
Швейцарии	1971
Катар	1997
Кувейт	2005
ОАЭ	2006
Саудовская Аравия	2011

Несмотря на предоставление избирательных прав женщинам, в некоторых из них существуют дополнительные ограничения для их реализации. В Ливане женщины, в отличие от мужчин, должны представить свидетельство о начальном образовании. В ОАЭ на выборах 2011 г. только примерно 12 % от общего числа граждан (как мужчин, так и женщин) получили право принять участие в голосовании.

11) По повторному избранию (для кандидатов).

В Древних Афинах ни один гражданин не мог состоять в Совете 500 (буле) два срока подряд и более двух сроков за всю свою жизнь; главой буле можно было быть только один раз. В Римской Республике годичные магистраты - народные трибуны, эдил, квестор, претор, и консул не могли переизбираться до истечения определённого количества лет.

В большинстве стран, где выборы президента осуществляются прямым голосованием, одно и то же лицо может избираться только один (Польша, Мексика) или два раза (США, Бразилия). В Конституции РФ в 81 статье прописано «Одно и то же лицо не может занимать должность Президента Российской Федерации более двух сроков подряд», что означает возможность избрания три и более раз, но с перерывами. Аналогичная норма в 2008 г. появилась и в Конституции Франции.

12) Иные ограничения.

В Древних Афинах был закрыт доступ к политической деятельности для уклоняющихся от участия в военных походах или бежавших с поля боя. В Италии с 1912 г. в выборах могли участвовать юноши достигшие совершеннолетия (21 год) и прошедшие воинскую службу.

В Мексике лишение избирательных прав возможно по следующим причинам:

- привлечение к уголовной ответственности, связанное с лишением свободы;
- отбывание наказания в виде лишения свободы;
- пребывание в приютах для наркоманов или душевнобольных;
- бродяжничество или постоянное пьянство, по которым вынесено законное решение;
- уклонение от суда и следствия с момента выдачи ордера на арест;
- вынесение окончательного приговора о приостановлении или лишении политических прав, если впоследствии не произошло восстановление в правах.

17.1.4. Избирательная система

Избирательная система (в широком смысле) - совокупность правовых норм, регулирующих порядок предоставления избирательных прав, проведения выборов в органы государства и местного самоуправления, определения результатов голосования.

Избирательная система (в узком смысле) - порядок определения результатов голосования.

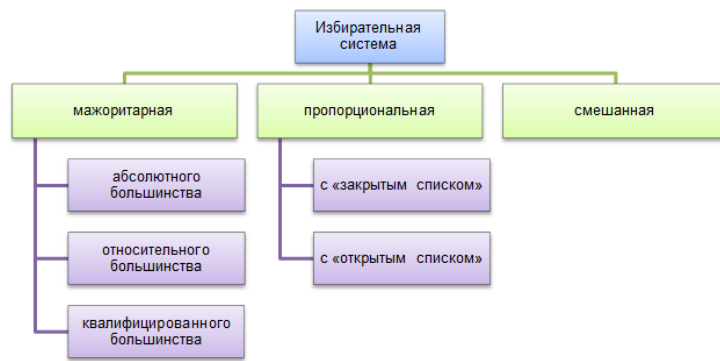


Рис.17.30. Классификация избирательных систем

1) Мажоритарная система (от фр. *majorité* – большинство) – система выборов, при которой для избрания кандидат (кандидаты в коллегиальный орган) должен получить большинство голосов избирателей (страны, избирательного округа, членов правления организации и т.п.).

Существуют три разновидности мажоритарной системы:

- **абсолютного большинства** – избранным считается кандидат, собравший абсолютное большинство голосов (минимум 50 % + 1 голос от проголосовавших избирателей). Обычно таким образом выбирают глав государств, руководителей организаций, филиалов или подразделений организаций и т.д. В соответствии с ФЗ «О выборах Президента Российской Федерации» предусматривается избрание главы государства на основе мажоритарной системы абсолютного большинства. На выборах в представительные органы данный способ применялся при избрании депутатов Верховных советов СССР и РСФСР. В соответствии с законами 1978 г. «О выборах в Верховный Совет СССР» и «О выборах в Верховный Совет РСФСР» предусматривались повторные выборы (а не второй тур голосования) со всей процедурой выдвижения и регистрации кандидатов в депутаты в случае, «если ни один из баллотировавшихся по избирательному округу кандидатов в депутаты не был избран» (не набирал абсолютного большинства). Одной из вариаций данного способа определения победителя является **мажоритарно-преференциальная система голосования (система единого передаваемого голоса)**. При такой системе избиратели расставляют кандидатов в избирательном списке в порядке предпочтения. Если ни один из кандидатов не получает абсолютного большинства первых мест в рейтинге, то кандидат с наименьшим рейтингом исключается из списка, а в бюллетенях, в которых он был указан первым, голос отдается кандидату, указанному на втором месте. Процесс исключения кандидатов и перераспределения голосов продолжается до тех пор, пока кто-то из оставшихся в списке кандидатов не набирает абсолютное большинство голосов. В 1990 г. подобным образом был выбран Президент Ирландии - Мэри Робинсон; используется на выборах в Австралии и Мальте;

- **относительного большинства** – кандидату для победы достаточно набрать больше голосов, чем кому-либо из конкурентов, и необязательно больше половины. Такая система используется в настоящее время на выборах депутатов парламента (конгресса) в Великобритании, Японии, США, Канаде, Индии и др.

- **квалифицированного большинства** – кандидату необходимо набрать заранее установленное большинство, которое выше половины (2/3, 3/4 и т.п.). Обычно применяется при решении конституционных вопросов. В Чили на выборах в Палату Депутатов Национального Конгресса кандидату для победы требуется получить поддержку 2/3 избирателей.

На выборах могут применяться и смешанные схемы. Например, во Франции при выборах депутатов Национальной Ассамблеи (нижней палаты парламента) могут потребоваться два тура. При этом для избрания в первом туре кандидат должен получить абсолютное большинство поданных голосов, которое не менее количества четверти избирателей, вписанных в избирательные списки. В противном случае во второй тур проходят кандидаты, получившие минимум 12,5% от количества зарегистрированных избирателей. Победитель второго тура определяется по относительному большинству. В случае равенства поданных голосов за лидеров второго тура избирается более старший кандидат.

Следует отметить, что мажоритарная система при выборах в представительные органы может давать непредсказуемые результаты. Так, во Франции в результате выборов 1993 г. в Национальное собрание правопоцентристская партийная коалиция набрала в целом по стране 39% голосов, но получила в указанной палате парламента 80% депутатских мест. В том же 1993 г. в Канаде (мажоритарная система относительного большинства) проводились общенациональные выборы в Палату Общин, в ходе которых за кандидатов Либеральной партии было подано 41,6% голосов, но она получила свыше 60% депутатских мандатов (178 из 295); кандидаты Прогрессивно-консервативной партии собрали 16% голосов, однако им досталось лишь 0,7% мест в указанной палате (два депутатских мандата), тогда как кандидаты Реформистской партии, добившись поддержки у 18% избирателей, заняли 16% депутатских мест (46 мандатов). Из вышесказанного следует, что при такой системе очень важное значение приобретает нарезка избирательных округов.

2) Пропорциональная система – система выборов, при которой места в представительном органе распределяются между списками кандидатов в соответствии с количеством набранных голосов. Определяя порядок формирования такого органа, необходимо стремиться, чтобы в нем были представлены все основные политические силы общества. Одним из первых, озвучивших эту идею (в 1789 г.), был видный деятель Великой французской революции Оноре Мирабо. Он отождествил парламент с картой государства. Как на карте, отражающей в уменьшенном масштабе все особенности рельефа страны, в парламенте должны быть представлены неодинаковые взгляды и интересы различных слоев населения в соответствии с их распространением и поддержкой в народе. Практически же эту идею начали воплощать в жизнь столетием позже, когда были разработаны соответствующие правила и проведены первые парламентские выборы на основе новой системы пропорционального представительства.

В 1890 г. пропорциональная система была опробована в швейцарском кантоне Тичино, в 1890 г. впервые использована на парламентских выборах в Бельгии, в 1906 г. - Финляндии (вошедшей в то время в состав Российской Империи), в 1909 г. - Швеции. В настоящее время данная система применяется на парламентских выборах большинства стран мира.

Существуют две основные разновидности пропорциональной системы:

- **с «закрытым (жестким) списком»** – избиратели голосуют за партийный список, а не отдельного кандидата. Каждая партия получает количество мест пропорционально полученным голосам. Эти места занимают представители партии в том порядке, который они занимают в партийном списке. Эта система используется при выборах в Европейский парламент во всех странах Европейского союза, Южной Африке, Израиле и России;

- **с «открытым (свободным) списком»** – избиратели могут голосовать либо за одного кандидата, либо за двоих, либо указать порядок предпочтения кандидатов (пропорционально-преференциальная система голосования) в партийном списке. Полученные партией места в выборном органе распределяются согласно подсчитанному рейтингу кандидатов. Данная система используется при выборах в Финляндии, Нидерландах, Бельгии, Бразилии и Демократической Республике Конго.

Для пропорциональной системы характерно наличие т.н. «процентного барьера» - доли голосов (в процентном выражении), получив которую, список участвует в распределении мест. Обоснованием данной меры выступает недопущение фрагментации представительного органа и обеспечение стабильного большинства. Процентный барьер для разных стран колеблется от 1 до 10%: Нидерланды – 0,67 %; Дания, Израиль – 2 %; Латвия, Украина, Россия (на выборах в Государственную Думу с 2016 г.) – 5 %; Турции – 10 %. В 2007 г. ПАСЕ рекомендовала устанавливать процентный барьер для парламентских выборов на уровне не выше 3 %.

Учитывая, что количество избираемых мест ограничено, существует процентный барьер и другие факторы, используются различные методы определения окончательного распределения мест среди партий в представительном органе: Сент-Лагу (Латвия, Новая Зеландия, Норвегия, Швеция), д'Ондта (Аргентина, Бразилия, Дания, Польша, Финляндия, Чехия, Япония), Хэйра-Нимейера (Германия, Россия) и др.

3) Смешанная система – система выборов, сочетающая в себе элементы мажоритарной и пропорциональной. Её суть заключается в том, что часть депутатских мандатов распределяется по принципам мажоритарной системы, что способствует широкому представительству депутатов от различных регионов, а другая часть - по принципам пропорциональной системы, что способствует более полному учёту голосов избирателей и точнее отражает реальную картину политической ситуации в стране. Такая система имеет определенные преимущества в странах с большим населением, так как позволяет соблюдать баланс между местными или общенациональными интересами. Она используется также в странах, где население неоднородно и живет в разнообразных географических, социальных, культурных и экономических условиях.

До 2007 г. смешанная система применялась при выборах депутатов Государственной Думы Российской Федерации. С 17 февраля 2014 г. в РФ снова применяется данная система: 225 депутатов Государственной Думы избираются по мажоритарной системе относительного большинства, 225 - по пропорциональной.

Смешанная система используется в Боливии, Германии, Лесото, Мексике, Новой Зеландии и Великобритании. В Австралии смешанная система проявляется по-иному: одна палата парламента избирается по мажоритарной системе абсолютного большинства, а другая - по пропорциональной системе. В Мексиканских Соединенных Штатах Палата депутатов Федерального Конгресса состоит из 300 депутатов, избираемых по мажоритарной системе относительного большинства, и 100 депутатов - по системе пропорционального представительства.

Политическая жизнь государств Древней Греции вошла в историю человечества как первый пример демократического правления. Идеи и принципы народовластия, выработанные древнегреческой цивилизацией, показали большое влияние на историю и практику государственного строительства последующих эпох. Именно на земле древней Эллады берут свое начало фундаментальные понятия демократии: равноправие, верховенство закона, выборность органов власти и должностных лиц, активное участие граждан в решении государственных вопросов.

В гомеровский период (XI – IX вв. до н.э.) высшим властным институтом в племенах (филах) Аттики было народное собрание (**эклесия**), на которое созывались все свободные мужчины, имевшие право носить оружие. Царь (**филобасилей**) не мог решать важные вопросы жизни племени, не посоветовавшись с войском и не получив его согласия на те или иные действия: воины должны были поддержать намерения или отклонить их. В действительности возможности собрания были весьма ограничены: его ход и постановления во многом определялись предварительным решением племенной аристократии. Тем не менее, собрание сохранялось в качестве важного элемента политической традиции. Цари имели возможность влиять на эклесию, манипулировать ее участниками, но пренебрегать собранием или ликвидировать этот институт, они не могли.

К VIII в. до н.э. завершился процесс объединения в единое государство отдельных поселений Аттики во главе с Афинами.

Значительные преобразования в политическом устройстве древних Афин связаны с именем Солона (≈ 640 – 559 гг. до н.э.) – одного из архонтов («начальствующих»). Солон строго обозначил обязанности народного собрания, процедуру его созыва и проведения. В круг его важнейших функций входило объявление войны и заключение мира, утверждение законов, избрание должностных лиц афинского государства, принятие специальных постановлений. Воля народа, выраженная путем общего голосования в собрании, приобретала силу закона (**номоса**), обязательного для всех. Постановления народного собрания (**псефисмы**) начинались со слов: «Совет и народ решили».

На собрании очень многое зависело от профессионализма председательствующего. Но поскольку эту должность мог занять любой гражданин, в том числе и недостаточно подготовленный, собрание часто направлялось так называемыми «демагогами» или «вождями народа». Популярные граждане, формально не занимавшие никакой государственной должности, благодаря ораторскому искусству и лести могли убедить народ в необходимости принятия нужных им постановлений.

Известны случаи, когда афиняне, сознавая невозможность повлиять на исход голосования, покидали собрание или совсем не являлись на него. Оратор Лисий, описывая установление в Афинах «тирании тридцати» (404-403 гг. до н.э.) указывал на то, что многие граждане предпочли воздержаться от голосования и уйти (то есть «проголосовать ногами»): «Все порядочные люди, находившиеся в народном собрании, видя такое насилие и понимая, что тут все заранее подстроено, частью остались там пассивными зрителями, частью же ушли, унося с собою, по крайней мере, сознание того, что они не подали своего голоса ко вреду отечества». Но законы принимались и в отсутствие большинства граждан. Лишь в особых случаях требовалось присутствие на собрании значительного числа голосующих - кворума, составлявшего 6000 человек.

Одной из функций народного собрания было избрание **гелизи** - народного суда. В V в. до н.э. его численность достигала шести тысяч человек (пять тысяч действующих судей и одна тысяча запасных). Большое количество судей должно было, по мнению афинян, сделать невозможным их подкуп, а, следовательно, гарантировать справедливость процесса. Для формирования коллегии судей ежегодно составлялся список, куда по жребию попадали афиняне не моложе 30 лет и не замеченные в дурных поступках, независимо от богатства и знатности происхождения.

Гражданская община древних Афин тщательно наблюдала за тем, чтобы только полноправные жители полиса участвовали в политической жизни города-государства. Лишь они могли заседать в народном собрании, быть судьями, занимать выборные должности. Все эти права были достоянием мужчин. Статус гражданина полиса передавался по наследству из поколения в поколение. Номинально афинские юноши достигали совершеннолетия в восемнадцать лет, но для того, чтобы обладать всей полнотой политических прав, они должны были пройти обязательную двухгодичную военную службу. Молодежь не участвовала в избирательных процедурах и не решалась даже посещать народное собрание. Немногочисленные попытки молодых ораторов привлечь к себе внимание вызывали у афинян смех и возмущение. Лишь достигнув 20-летнего возраста, пройдя обряд посвящения, афиняне переходили в категорию полноправных граждан. С лицом, обращенным к небу, они приносили торжественную присягу.

Периодически проводилась проверка гражданских списков: «Имена тех, кто не был рожден от отца-гражданина и матери-гражданки, должны были быть вычеркнуты».

Впрочем, для того, чтобы быть истинным гражданином и членом полиса, афинянину требовалось не только доказать законность своих прав, но и соответствовать определенным моральным требованиям. Законодательство ограничивало права тех, кто отказывался заботиться о своих престарелых родителях. Доступ к политической деятельности был закрыт для не уплативших налогов, уклоняющихся от участия в военных походах (или бежавших с поля боя), а также тех, кто легкомысленно растратил свое имущество. При наличии веских оснований, человек мог быть приговорен судом к **атимии** - лишению гражданских прав. Кандидаты на высокую выборную должность, прошедшие предварительную процедуру жеребьевки или открытого голосования (выдвижения кандидата), подвергались официальной проверке на соответствие родовым и моральным требованиям - **докимасии**.

В правовом отношении граждане полиса были изолированы от других категорий населения: рабов и метеков (лично свободные люди, не обладающие правами афинского гражданства: переселенцы из других полисов и их потомки, отпущенные на волю рабы).

Общая численность населения Афин на протяжении V-IV в. до н.э. оценивается учеными в пределах 120-300 тысяч. Семьи свободных граждан насчитывали соответственно от 60 до 170 тысяч (т.е. примерно половину от общего числа жителей). Что касается граждан, имеющих право участвовать в народном собрании, то их количество оценивается в пределах 30-40 тысяч человек.

Характеризуя афинскую демократию периода V-IV вв. до н.э., исследователи подчеркивают ее существенную особенность: она была прямой и непосредственной. Решение более или менее значимых государственных вопросов принималось всем коллективом (по крайней мере, теми его членами, которые активно участвовали в политической жизни). Любой гражданин имел право внести законопроект, выступить на собрании, выдвинуть свою кандидатуру на выборную должность (с определенными ограничениями). Все это обуславливало своеобразие избирательного процесса в Афинах. Избирательные процедуры имели здесь форму и содержание, отличные от современных. В наши дни путем всенародного голосования формируются представительные органы власти и принимаются важнейшие законы. Афинские граждане не делегировали свои властные полномочия депутатам, как это происходит сегодня в большинстве стран. Государственные институты древних Афин, формируемые путем выборов, не имели самостоятельной власти. Их предназначение было в выполнении решений народного собрания, исполнении законов и подготовка вопросов, выносившихся на очередное заседание собрания (эклесии).

Более того, афинская государственная система стремилась не допускать усиления выборных коллегиальных органов и отдельных должностных лиц. Их полномочия были четко оговорены и ограничены временными рамками, как правило, не более одного года. Даже председатель буле (аналога парламента) и коллегии десять стратегов (аналога кабинета министров) менялись каждый день. Каждый, кто хотя бы в незначительной степени участвовал в управлении государством, должен был, по окончании срока полномочий, отчитаться о своей деятельности. Не выполнив это требование, он не мог покинуть город. Важно отметить, что для античного общества было характерно не разделять понятия «право» и «обязанность», когда речь шла об общественной службе. Гражданин, избранный народом на какую-либо должность, не мог от нее отказаться, даже если ему приходилось выполнять действия, с которыми он лично не был согласен: «Никия избрала стратегом – вопреки его упорным отказам»; «закон не позволяет тем, за кого проголосовал народ, давать в Совете клятву с отказом».

В Афинах последовательно проводился принцип, согласно которому ни одно должностное лицо не могло приступить к исполнению своих обязанностей, минуя сложную избирательную процедуру. Власть могла быть дана ему лишь народом, но не другим должностным лицом. Античные авторы говорят о тождественности понятий «должностное» и «избранное» лицо.

Повседневная жизнь полиса была теснейшим образом связана с голосованием и выборами. Голосование производилось очень часто и по самым разным поводам: в собраниях различного уровня (от мельчайших территориальных единиц - демов, до эклесии), суде, магистратурах, частных сообществах, быту.

17.2.2. Древний Рим

В VIII-VI вв. до н.э. управление осуществлялось посредством нескольких политических институтов - царя, сената и народных собраний. До установления в 509 г. до н.э. республиканского строя **царь** (rex) был пожизненно наделен высшей политической, военной, судебной и административной властью. Должность царя не передавалась по наследству, а была выборной. Им мог стать каждый совершеннолетний римлянин. Кандидатура царя предварительно выдвигалась сенатом, а затем утверждалась народным собранием.

Сенат (senatus) являлся советом родовых старейшин. Его численность с VIII по VI вв. до н.э. постепенно выросла от 100 до 300 человек и соответствовала общему числу римских родов. Сенат был призван сохранять устои римской общины: готовил выборы нового царя, имел право кассировать решения народных собраний, разбирал судебные дела о незначительных преступлениях.

Остальные члены римских родов за исключением женщин, несовершеннолетних и рабов участвовали в жизни общины через **куриатные комиции** - собрания граждан по куриям (территориальным единицам, сложившимся естественным образом; лат. curia – союз мужей). Здесь утверждались законы, решались вопросы войны и мира, выбирались царь и другие должностные лица. Процедура принятия решений комициями в наиболее ранний период римской истории вызывает у исследователей некоторые затруднения. Существует мнение, что внутри курий подача голосов «за» или «против» осуществлялась посредством крика. На общем собрании каждая курия имела один голос и высказывалась по очереди. Если предложение председательствующего (т.е. царя) находило поддержку большинства курий, то голосование прекращалось и глашатай объявлял окончательный результат.

В результате реформ Сервия Туллия (шестой римский царь, правил в 578-535 гг. до н.э.) появился новый вид народных собраний – **центуриатные комиции**. Значение центуриатных комиции постепенно росло. Со временем они стали принимать решения не только о войне или мире, но и избирать должностных лиц, утверждать законы. На центуриатных собраниях

действовала иная процедура голосования, чем на куриатных. По свидетельству Тита Ливия: «Не поголовно, не всем без разбора (как то повелось от Ромула и сохранялось при прочих царях) было дано равное право голоса и не все голоса имели равную силу, но были установлены степени, чтобы и никто не казался исключенным из голосования, и вся сила находилась бы у виднейших людей государства. А именно: первыми приглашали к голосованию всадников, затем восемьдесят пехотных центурий первого разряда; если мнения расходились, что случалось редко, приглашали голосовать центурии второго разряда; но до самых низких не доходило почти никогда». Как правило, все решения принимались первым разрядом, который обладал примерно 51% голосов.

Уничтожив царскую власть (510 г. до н.э.), римляне учредили должности двух высших магистратов, которые первоначально назывались преторами, а затем - консулами, и выбирались из патрицианского сословия на центуриатных комициях. Исполнительную власть в Римской республике олицетворяли **магистраты**. Вместе с народным собранием и сенатом они составляли единую систему высшей власти и управления в государстве. Сами магистраты разделялись на старших (**консулы, преторы и цензоры**) и младших (**эдилы и квесторы**).

Общее количество должностных лиц в Республике постоянно увеличивалось. С конца III до середины I в. до н.э. оно выросло в четыре раза. В правление Юлия Цезаря помимо 2 консулов насчитывалось 16 преторов, 8 эдильов и 40 квесторов. Раздробление исполнительной власти постепенно привело к ослаблению функций магистратов повышению роли сената в государственной жизни, что дало повод некоторым историкам называть Римское государство I в. до н.э. сенатской республикой. Современные исследователи выделяют следующие черты римских магистратур:

- выборность;
- годичность исполнения должности (кроме цензоров, избиравшихся на 18 месяцев);
- коллегиальность;
- последующая ответственность за служебные действия (во время отправления должности магистрат не мог быть привлечен к судебной ответственности);
- безвозмездность (выполнение обязанностей считалось не работой, а почетом).

Вышеперечисленные магистратуры являлись обычными и поэтому назывались **ординарными**. В связи с чрезвычайными обстоятельствами избирались или назначались **экстраординарные** магистратуры, наиболее значимыми из которых были **диктатор** и **интеррекс**. Первый выдвигался из бывших консулов на срок не более шести месяцев для выполнения конкретной задачи. Второй исполнял обязанности консула в течение пяти дней между консульскими выборами.

В республиканский период формируется система ценностей и правовой статус римского гражданина. Служение общественным интересам признается первейшим долгом каждого человека. Наиболее важной обязанностью считалось участие в политической жизни и военных кампаниях. В 17 лет молодой человек принимался в центурию и с момента принесения присяги получал право голосовать в комициях. Для занятия государственных постов предъявлялись дополнительные требования - достижение необходимого возраста и участие в нескольких военных кампаниях. В частности, в 180 г. до н.э. были определены условия, открывавшие кандидатам доступ к отдельным магистратурам. Для занятия должности квестора требовалась десятилетняя служба в армии. Претором мог стать только бывший квестор, а консулом - бывший претор, при условии, что между двумя разными ступенями проходило не менее двух лет. Таким образом, минимальный возраст, с которого начинались эдилитет и квестура равнялся 28 годам, претура - 40, консулат - 43. Такое выдвижение называлось избранием в «свой год».

Большая группа законов (не менее 13) получила название **leges de ambitu** (от «ambitus» - хождение вокруг, домогательство почетных должностей) и была направлена против предвыборных интриг кандидатов в магистраты. Уже в середине IV в. до н.э. злоупотребления при соискании должностей, допущенные честолюбцами незнатного происхождения, сравнивали с организацией мятежей. Осуждению подвергались кандидаты, агитировавшие за себя на рынках и в селах. В I в. до н.э. **leges de ambitu** запретили претендентам устраивать бесплатные пиры и зрелища для граждан, дарить подарки и раздавать деньги. Для всех нарушителей устанавливались суровые наказания. По закону 70 г. до н.э. им преграждался доступ в магистратуры на 10 лет, по закону 61 г. до н.э. с них взымался пожизненный ежегодный штраф. В дальнейшем ответственность за подкуп избирателей еще больше ужесточалась. Провинившихся ждал крупный штраф и окончательный запрет занимать магистратуры, а в последние годы I в. до н.э. - лишение римского гражданства и имущества с последующим изгнанием.

Кандидат на должность заранее уведомлял соответствующие магистраты о своем желании баллотироваться. От должностных лиц требовалось проверить, насколько отвечает требованиям закона заявленный соискатель, и принять решение о внесении его имени в список для голосования.

Официальная регистрация считалась началом избирательной борьбы и проходила до дня выборов. Претенденты облачались в белоснежную тогу, которая символизировала чистую совесть будущего магистрата, и направлялись в наиболее людные места - площади и базары для «обхода» избирателей. Встречая сограждан, соискатели обращались к ним по имени и почтительно просили поддержки. Большую помощь оказывал раб-номенклатор: он помнил имена избирателей и вовремя подсказывал их кандидату. В соответствии с **leges de ambitu** «обход» считался одним из немногих дозволенных способов агитации. В Помпеях в ходе избирательной кампании разрешалось использовать «агитационные плакаты» - на стенах домов поверх белой штукатурки красной краской писались имена кандидатов и их обращения к избирателям, бранные слова и карикатуры на кандидатов, призывы к активному участию в избирательной кампании.



Рис.17.31. Агитационные надписи в Помпеях

Примеры некоторых «агиток»:

- «Лорей, соседки просят тебя, выбери в эдилы Амплиата»;
- «Прокул, выбери Сабина эдилом, и он тебя выберет»;
- «М. Казеллий Марцелл будет хорошим эдилом и устроит великолепные игры»;
- «Выбирайте в дуумвиры Бруттия Бальба – этот не расхитит казны».

Количество обнаруженных «плакатов» говорит об ожесточенности и размахе предвыборной борьбы в Помпеях. Из 1400 предвыборных надписей, найденных к 1871 г., около 600 были датированы 79 г. н.э. (год гибели Помпеев). Если учесть, что население города не превышало 30000 человек, а размеры 2.5 километров по окружности, то становится очевидным высокий интерес местных жителей к выборам.

В день голосования перед заседанием комиции старшие магистраты проводили ауспиции (auspicia) - ритуальные процедуры определения воли богов по полету и крику птиц. За их правильностью и результатом следил авгур-жрец. Если он находил предзнаменования дурными, то произносилась формула: «В другой день!» и комиции распускались.

Процедура голосования на народных собраниях нашла отражение в большой группе законов, принятых в III-II вв. до н.э. В 139 г. до н.э. было введено тайное голосование при выборах магистратов, а в 137-107 гг. до н.э. – при обсуждении законопроектов и дел о государственной измене.

Непосредственную подачу голосов осуществляли при помощи деревянных перегородок, напоминавших загон для овец. Римляне называли их «**ovile**» (от «ovis» - овца) или «**saepta**» (от «sacres» - изгородь, забор). На входе в ovile избиратели получали дощечки, на которых писали имя своего кандидата, а на выходе клали их в урну. При открытом голосовании, применявшемся до 139 г. до н.э., на выходах стояли счетчики, которые спрашивали у избирателей мнение по кандидатуре соискателя. Голоса «за» и «против» фиксировали еще одни служащие - контролеры. На табличках они делали соответствующие отметки и по окончании голосования подсчитывали результаты.

Своеобразно принимали решения сенаторы: обутое в башмаки из красной кожи (знаки отличия тех, кто избирался в старшие магистраты) высказывали свое мнение вслух, обутое в башмаки из черной кожи (младшие магистраты) - «голосовали ногами».

С сенатом связаны и другие интересные факты. Так, во времена консульства Калигулы (37, 39-41 гг. н.э.), он сделал сенатором своего любимого коня Инцитата (лат. incitatus - быстроногий, борзой) и даже занес его в списки кандидатов на пост консула. Другой широко известный факт связан с убийством Гая Юлия Цезаря в стенах сената 15 марта 44 г. до н.э. Среди заговорщиков оказался и опекаемый Цезарем Марк Юний Брут (Цезарь был любовником матери Брута). Увидев его среди заговорщиков, он произнес знаменитую фразу «И ты, Брут!» (по другой версии - «И ты, дитя мое!»).



Рис.17.32. Убийство Юлия Цезаря (Винченцо Камуччини)

В ходе судебных разбирательств в Риме применялось тайное голосование. При вынесении приговора члены судебных коллегий писали на табличках одно из мнений - A («absolvo» - оправдываю), C («condemno» - обвиняю) или NL («non liquet» - не ясно). Решения выносились большинством голосов и объявлялись претором. В случае равенства обвинительных и оправдательных мнений подсудимый считался оправданным.

С середины I в. до н.э. - начала I в. н.э. существенно изменяются роль, значение и порядок формирования римских государственных институтов. При Юлии Цезаре консулы избирались не на один год, а на много лет вперед; количество членов сената возросло до 1000 человек; часть магистратов назначается без участия народных собраний. Известный историк Светоний отметил: «Выборы он поделил с народом: за исключением соискателей консульства, половина кандидатов избиралась по желанию народа, половина - по назначению Цезаря. Назначал он их в коротких записках, рассылаемых по трибам (административно-территориальным единицам – «избирательным округам»): «Диктатор Цезарь - такой-то трибе. Предлагаю вашему вниманию такого-то, дабы он по вашему выбору получил искомое им звание».

В начале I в. н.э. император Тиберий отнимает у центурнатных и трибутных комиций последние выборные полномочия, часть которых передает сенату, а часть присваивает себе. Комиции собирают только для оглашения имен избранных, а в III в. окончательно упраздняют.

17.2.3. Новгородское вече (XII – XV вв.)

Со второй половины X - начала XI в. на территории древнерусского государства начинается быстрый рост городских поселений. По данным археологических исследований, уже к середине XIII в. таких поселений насчитывается более 150. В X-XII в. окончательную форму принимает высший орган власти городов и подконтрольных им земель - народное собрание (вече).

Столицы княжеств имели свои атрибуты вечевой деятельности – особый колокол и специальную трибуну (степень), которая возвышалась над площадью. Если в спокойное время на таких собраниях соблюдался определенный порядок, то в экстраординарных случаях (в моменты бедствий и возмущений) они представляли собой неуправляемую толпу, кричащую на разный лад. По мнению историков, обычное вече выглядело как «вполне упорядоченное совещание», проходящее с соблюдением следующих правил: инициатива созыва принадлежала князю или главе городского самоуправления, сбор общинников проходил на главной площади, а его участники размещались в определенном порядке - ближе к князю и другим правителям города «именитые люди», за ними - все остальные. Исследователи высказывают даже предположение о существовании предварительной записи для выступавших (если повестка собрания была известна заранее) и протокольным ведении принятых решений.

В столице Древней Руси - **Киеве**, где прочно утвердилась монархическая форма правления, в X-XII вв. собрание горожан имело столь широкие полномочия, что изгоняло одного правителя и возводило на княжеский стол другого, назначало судей, вершило вопросы войны и мира, ведало финансовыми и земельными ресурсами волостей, отправляло посольства в другие земли.

Аналогичными полномочиями обладало и **новгородское вече**. В столице Северо-Западной Руси к XIII в. устанавливается особая процедура приглашения (выбора) князя. «Совет господь» (боярский совет) предварительно рассматривал кандидатуру **князя**, затем ее рекомендовали вечу, которое и принимало окончательное решение. При согласии вече за новым

князем отправлялась специальная делегация горожан. Выбранный «на всей воли новгородской», он заключал с городом договор - «**ряд**», в котором определялись права и обязанности князя, а также принципы его взаимоотношений с городом по вопросам суда, торговли и финансов. Таким образом, юридически оформлялся статус избранного правителя и одновременно закреплялись полномочия республиканских органов власти. Процедура выборов завершалась **крестоцелованием** - особой присягой «на грамотах Ярославлих», в которых издавна были зафиксированы политические и экономические привилегии новгородского самоуправления. Присягая, князь обязывался соблюдать условия «ряда» и не нарушать права городской общины.

В ведении новгородского вече входило и избрание **посадника** (своего рода «вице-президента»). Посадник председательствовал на вече, контролировал деятельность князя и делил с ним судебно-административную власть. Он участвовал в военных походах и вел дипломатические переговоры, следил за правильностью взывания податей с населения. К началу XIV в. посадника сменила коллегия из 6 человек, пожизненно избранных от всех новгородских концов (административных районов Новгорода). Из их числа вече ежегодно стало избирать главного - «степенного» посадника. Во второй половине XV в. количество членов коллегии посадников достигает 36 человек, а смена степенного - каждые 6 месяцев. Отличительной чертой выборов посадника стала их многоступенчатость: от выдвижения на кончанском вече до избрания на общегородском. Всего, по подсчетам историков, с 1126 по 1400 гг. эту должность занимали 275 человек, представлявших 30-40 наиболее авторитетных боярских семей.

Особое положение в Новгородской республике занимал **архиепископ**. Он возглавлял одну из самых крупных и богатых епархий. Владыка не только распоряжался огромной церковной казной и большими земельными ресурсами, но и организовывал работу «Совета господ», скреплял своей печатью городские грамоты и договоры, активно участвовал в разборе межтерриториальных тяжб и распрей. Недаром иностранные путешественники называли его «сеньором города». Выборный статус архиепископа сформировался в ходе борьбы Новгорода за политическую самостоятельность. Первое такое избрание состоялось в 1156 г. после смерти очередного владыки. С тех пор новгородские архиепископы выбирались горожанами на вечевых собраниях, а киевский митрополит утверждал этот выбор.

С 1193 г. сложилась оригинальная процедура избрания архиепископа, по замечанию одного из исследователей, сочетавшая в себе «принципы всенародного вечевого избрания с некоей видимостью проявления воли Божьей». Вначале на вече выдвигали трех кандидатов. Их имена записывали на пергаменте и приносили в Софийский собор во время церковной службы. Здесь запечатанные листы раскладывали на трапезе собора и по окончании службы посылали с веча слепца или ребенка для выноса одного из листов - «которого Бог даст». Поименованный в выбранном листе кандидат и становился владыкой Новгорода.

Одним из принципов новгородской «демократической» республики был строгий контроль за действиями выборных лиц. По требованию одного из концов, вече могло принять решение о немедленном смещении того или иного должностного лица и его наказании в случае грубого нарушения общинных прав и обычаев.

17.2.4. Английский парламент (XIII – XVI вв.)

В 1215 г. крупные землевладельцы добились от Иоанна Безземельного подписания «Великой хартии вольностей», согласно которой король не мог назначать новых налогов (кроме некоторых старых феодальных налогов) без согласия королевского совета (англ. royal court), который постепенно эволюционировал в парламент. В 1265 г. Симон де Монфор собрал первый выборный Парламент, а в 1295 г. был созван т.н. «Образцовый парламент». Этот год стал начальной точкой отсчета регулярных и упорядоченных парламентских сессий.

В первые века существования парламент не имел постоянного места заседаний. Король мог созвать его в любом городе. Как правило, он собирался в том месте, где в данное время располагался король и его двор. В частности, места дислокации некоторых парламентов конца XIII - начала XIV в.: Йорк - 1283 г., 1298 г., Шрусбери - 1283 г., Вестминстер - 1295 г., Линкольн - 1301 г., Карлейль - 1307 г., Лондон 1300 г., 1305 г., 1306 г. В XV в. постоянной резиденцией, местом, где проходят заседания палат парламента, стал комплекс зданий Вестминстерского аббатства.

К середине XIV в. намечилось разделение парламента на две палаты - верхнюю и нижнюю. В XVI в. стали употреблять названия палат: для верхней - **палата лордов** (англ. the House of Lords), для нижней - **палата общин** (англ. the House of Commons).

Верхняя палата включала представителей светской и церковной знати, входивших в королевский совет. Это были пэры (крупные феодалы) королевства, «великие бароны» и высшие официалы короля, церковные иерархи (архиепископы, епископы, аббаты и приоры монастырей). Все члены верхней палаты получали именные вызовы на сессии за подписью короля. Сложившаяся в Англии система прецедентного права давала лорду, получившему однажды такое приглашение, основание считать себя постоянным членом верхней палаты. Число лиц, причастных, в силу своего социально-правового статуса, к деятельности палаты, было невелико. Количество лордов в XIII-XIV вв. колебалось от 54 в парламенте 1297 г. до 206 человек в парламенте 1306 г. В XIV-XV вв. численность лордов стабилизируется; в этот период она не превышала 100 человек.

Любопытен документ – приглашение родственника короля Эдуарда I (1272 – 1307 гг.) на заседания парламента 1295 г.

Король возлюбленному родственнику и верному своему Эдмунду графу Корнуолл, привет. Так как необходимо позаботиться о мерах против опасностей, которые в эти дни угрожают всему королевству нашему, и мы желаем иметь с вами и прочими королевства нашего магнатами совещание и рассуждение, то мы повелеваем вам именем верности и любви, которые вы имеете к нам, крепко наказывая, чтобы в воскресенье, ближайшее после праздника святого Мартина зимнего, вы лично присутствовали в Уэстминстере для того, чтобы обсудить, постановить и исполнить вместе с нами и с прелатами и прочими магнатами и другими жителями королевства нашего то, с помощью чего следует устранить эти опасности.

Засвидетельствовано королем в Кентербери в первый день октября.

Уже в первом парламенте Монфора, помимо группы магнатов (лордов), присутствовали представители графств (по два «рыцаря» от каждого графства), городов (по два представителя от наиболее значимых населенных пунктов), а также церковных округов (по два «проктора» - депутата-священника). Впоследствии эта группа представителей общества трансформировалась в палату общин. В середине XIV в. количество членов палаты общин составляло примерно двести человек, к началу XVIII в. - более пятисот. Термин «палата общин» происходит от понятия «commons» - общины. В XIV в. оно обозначало особую социальную группу, некое «среднее» сословие, включающее рыцарство и горожан. «Общинами» стала называться та часть свободного населения, которая обладала полнотой прав, определенным достатком и добрым именем. Представители этого «среднего» сословия постепенно приобрели право избирать и быть избранными в нижнюю палату парламента.

Выборы в палату общин от графств проводились перед каждой сессией парламента, примерно за два-три месяца до ее открытия. Королевская канцелярия рассылала шерифам графств письма-приказы (англ. returns). Эти документы надлежало возвратить ведомству канцлера с вписанными в них именами избранных лиц. В XIII-XIV вв. процедура выборов производилась на собрании графства, а с 1407 г. на ближайшей сессии суда графства. Согласно статуту 1429 г., для участников выборных собраний в графствах был установлен сословно-имущественный ценз судебных присяжных заседателей, равный 40 шиллингам годового дохода. Помимо имущественного ценза, статут устанавливал и обязательность постоянного проживания избирателя в соответствующем графстве. Голосование по выборам парламентариев из кандидатов выполнялось поднятием рук (англ. show of hands).

В начале XV в. парламентом был издан ряд законов, призванных упорядочить и усовершенствовать выборный процесс в графствах. Статут 1407 г. впервые ввел понятие протокола избирательного собрания (англ. indenture) и списка избирателей. К письму, свидетельствующему об избрании «рыцарей», шериф должен был приложить и список избирателей, причем каждое имя подтверждалось личной печатью и подписью.

Выборы в палату общин от городов, носивших статус «парламентских», выполнялся по схожей с графствами процедуре. В городе, имевшем право представительства в парламенте, должно было проживать значительное количество граждан. Кроме этого, такие города облагались повышенным налогом и несли расходы за работу парламентариев во время сессии. Не каждый город мог позволить себе такие расходы. Так, при Эдуарде I в парламенте было представлено 58 из 177 городов.

Состав палаты общин формировался при активном, заинтересованном участии королевской администрации. Характер парламентских выборов в средневековой Англии существенно отличался от того, что наблюдается в новейшее время. Об этом говорит выдержка из свидетельства религиозного деятеля XVI в. Р. Холла, сообщавшего об особенностях формирования так называемого «Парламента реформации» (1529-1536 гг.):

Наряду с традиционным предписанием выбрать от каждого города двух честных, достойных и способных членов парламента, следовало частное послание от наиболее влиятельных лиц в том графстве, где расположен какой-либо город - от королевских советников или даже от самого короля, с настойчивой просьбой выбрать того, кто указан в письме. Многие склонялись перед авторитетом ходатаев и поступали именно так ... В результате в нижней палате оказалось множество королевских блюдолиз, прихлебателей, паразитов и негодяев всех мастей, имевших самые жалкие представления о чести ...

Несмотря на это, значительное количество парламентариев открыто выражали свое мнение на заседаниях. Этому способствовали шаги, предпринятые в области обеспечения «депутатской неприкосновенности». Так, в 1523 г. спикер палаты общин Томас Мор создал прецедент, испросив у короля Генриха VIII (1491 - 1547 гг.) право высказываться в парламенте, без опасений преследования за свои слова, и при Елизавете I (1533 – 1603 гг.) эта привилегия была узаконена (хотя нередко нарушалась на практике). Другой случай, приведший к расширению прав парламентариев, произошел в 1543 г. с депутатом Дж. Феррерсом. Он был арестован за долги во время следования на сессию. Палата просила шерифов Лондона об

освобождении Феррера, но получила грубый отказ. Тогда по приговору палаты общин были арестованы должностные лица, заключившие под стражу депутата. В сложившейся правовой коллизии король Генрих VIII издал распоряжение о привилегии членов палаты общин: их личность и имущество признавались свободными от ареста во время парламентской сессии.

Значительных успехов парламент добился в области законодательства. Задолго до его возникновения в Англии сложилась практика подачи королю и его совету частных петиций - индивидуальных или коллективных прошений. С возникновением парламента петиции стали адресовать и этому представительному собранию. В парламент поступали многочисленные письма, отражавшие самые разные нужды как частных лиц, так и городов, графств, торговых и ремесленных корпораций и т.д. На основании этих запросов, парламент в целом или отдельные группы его членов, вырабатывали собственные обращения к королю - «парламентские петиции».

Развитие института «парламентских петиций» привело к появлению нового порядка принятия законодательства. При Генрихе VI (1366 – 1413 гг.) сложилась практика рассмотрения в парламенте законопроекта - билля. После трех чтений и редактирования в каждой палате, билль, одобренный обеими палатами, направлялся на утверждение короля; после его подписи он становился статутом (закон, принятый королем и парламентом). Со временем формулировки принятия или отклонения билля приобрели строго определенный вид. Положительная резолюция гласила: «Королю это угодно», отрицательная: «Король об этом подумает».

В конце XVI в. наблюдаются попытки парламента расширить свои административные полномочия применительно к электоральному процессу. В 1581 г. палата общин обсуждала вопрос о порядке производства **дополнительных выборов** в случае досрочного прекращения депутатом своих полномочий (вследствие болезни, смерти). Группой парламентариев было предложено принять решение о том, что «дополнительные» выборы следует производить с санкции палаты общин. В 1586 г. палата общин добилась права проверять законность выборов в тех случаях, когда имелись веские основания подозревать, что закон был нарушен. Ранее подобное расследование производили королевские чиновники.

17.2.5. Президент и Конгресс США (конец XVIII - начало XX в.)

До войны за независимость США (1775 – 1783 гг.) все колонии имели систему органов местного управления, включавшую институты исполнительной, представительной и судебной власти. Исполнительная власть осуществлялась губернаторами. В «коронных колониях» они назначались Лондоном и подчинялись королевской администрации. В собственнических и корпоративных колониях порядок формирования администрации был зафиксирован в юридических документах (хартиях), определяющих основы взаимоотношений американских территорий и правительства Великобритании. В корпоративных колониях губернаторы, как правило, являлись местными гражданами и избирались «пайщиками» компании.

Победа Севера в Гражданской войне и принятие «Декларации независимости» (4 июля 1776 г.) сыграли важную роль в процессе демократического развития Западной цивилизации, становления «гражданского общества». Именно в «Декларации ...» была провозглашена идея социального и политического равноправия всех членов общества.

С провозглашением независимости, многие штаты-участники конфедерации разработали и приняли собственные конституционные акты, в которых были юридически закреплены основы внутреннего устройства этих новых государственных образований и, в том числе, важнейшие черты местных избирательных систем.

Формально, в штатах сохранялась старая, колониальная система организации власти. Однако в новых условиях способ формирования властных структур изменился.

Практически во всех штатах губернаторы избирались законодательными собраниями (как правило, на годичный срок). Избирая губернаторов, ассамблеи штатов стремились подчеркнуть приоритет законодательной власти над исполнительной и одновременно осуществляли более жесткий контроль за деятельностью региональных правительств.

Законодательные собрания (ассамблеи) штатов, как правило, состояли из двух палат: верхней (чаще всего она называлась «сенат») и нижней. В большинстве регионов, где законодательная ассамблея состояла из двух палат, ее состав переизбирался ежегодно, но в некоторых штатах законодательство устанавливало более длительный срок полномочий: в штате Мэриленд - 5 лет, в Вирджинии и Нью-Йорке - 4 года (с ежегодной ротацией 1/4 состава). В большинстве штатов выборы были прямыми: избиратели голосовали непосредственно за кандидатов в депутаты соответствующей палаты.

Необходимо отметить такой важный элемент избирательного процесса, как тайный способ подачи голосов с использованием записок – бюллетеней (англ. ballots). Он был зафиксирован в конституциях штатов Делавэр, Джорджия, Северная и Южная Каролина, Пенсильвания и других.

Реформа государственного устройства США была обсуждена в 1787 г. на конвенте в Филадельфии. Участники этого собрания обсудили несколько проектов государственного устройства и в качестве базового приняли проект, разработанный Джеймсом Мэдисоном. В его основу был положен принцип разделения властей на законодательную, исполнительную и судебную. Предполагалось создание сильного федерального центра с большим объемом полномочий, двухпалатного парламента, независимых судебных органов.

Высшим законодательным органом согласно проекту конституции становился двухпалатный парламент – **конгресс**. Он состоял из **сената** (верхней палаты) и **палаты представителей** (нижней палаты). Каждый штат избирал на своем собрании (легислатуре) двух представителей в сенат независимо от численности проживающего населения. Члены палаты представителей избирались прямым народным голосованием пропорционально количеству избирателей в штате, но не менее одного. Срок полномочий члена палаты представителей – 2 года с возможностью неограниченного количества переизбраний. Сенаторы избирались на 6 лет с возможностью неограниченного переизбрания, но каждые 2 года должна была выполняться ротация трети состава сената.

Высшим органом исполнительной власти должен был стать **президент**. Кандидатам в президенты предъявлялось только три требования:

- гражданство (быть гражданином США по праву рождения или принять гражданство);
- оседлость (проживать на территории США не менее 14 лет);
- возраст (быть не моложе 35 лет).

При обсуждении способа его избрания остановились на следующей процедуре.

1. Вначале в каждом штате выбираются их представители (выборщики), число которых равно числу конгрессменов от штата. Порядок избрания выборщиков в штатах регламентируется местными конституциями. Можно выделить три принципа, по которым создавались коллегии (коллегии) выборщиков в штатах: избрание законодательным собранием, избрание всеобщим голосованием избирателей, выборы по избирательным округам внутри штатов.

2. Собрания выборщиков проходили исключительно на территории своего штата. Была предусмотрена ситуация, когда выборщики будут голосовать лишь за представителя своего региона. Для ее предупреждения вводилось правило, по которому каждый выборщик должен был подать два голоса, причем второй голос обязательно за кандидата от другого штата: «Выборщики собираются в своих штатах и голосуют посредством бюллетеней за двух лиц, которые не должны быть жителями одного штата». По окончании процедуры голосования составлялся протокол, в котором указывались все кандидаты, названные выборщиками и количество голосов, поданных за каждого из них. Протоколы решений собраний выборщиков в запечатанных конвертах направлялись председателю сената Конгресса. Они распечатывались и оглашались на совместном заседании палат. Для победы на выборах кандидат в президенты должен был получить простое большинство голосов выборщиков. Лицо, занявшее второе место по итогам голосования, становилось вице-президентом.

3. В случае, когда равное большинство получит несколько кандидатов, право избрания президента передавалось нижней палате конгресса. Конституция США предписывала следующее: «Если ... более чем одно лицо получило ... большинство и равное число голосов, тогда незамедлительно Палата представителей, голосуя посредством бюллетеней, избирает одного из них Президентом ...».

Интересно мнение одного из влиятельных американских политиков, участника конвента Александра Гамильтона по поводу практически двухступенчатой процедуры избрания президента (народ – выборщиков, выборщики – президента) и отдельного заседания коллегий выборщиков.

... Особенно желательно максимально сузить возможности для буйства и беспорядков. Это зло отнюдь не последнее, которого следует опасаться при выборах должностного лица, которому надлежит играть столь важную роль в правительстве, как президент Соединенных Штатов. ... Выбор нескольких для создания промежуточной коллегии выборщиков потрясет куда меньше сообщество необычными или бурными конвульсиями, чем выбор одного ... А когда избранные в каждом штате соберутся и проведут голосование в выбравшем их штате, находясь далеко и порознь друг от друга, на них окажут значительно меньшее влияние чувства и страсти, которые могли бы передаваться от них народу, чем если бы они собирались одновременно в одном месте. Самое главное, чего следует желать, - нужно возвести все практически возможные препятствия против заговоров, интриг и коррупции. Можно, естественно, ожидать, что эти самые смертельные враги республиканского образа правления проявятся более чем с одной стороны, но их главный источник - желание иностранных держав достичь ничем не оправданного влияния в нашем руководстве ...

А. Гамильтон. К народу штата Нью-Йорк [Федералист № 68 от 12 марта 1788 г.]

Разработанный на конвенте проект конституции на протяжении 1787-1788 гг. был ратифицирован в девяти штатах, и 2 июля 1788 г. было объявлено о том, что конституция вступила в

Обычно на первичных выборах представлена целая обойма кандидатов на многочисленные посты - не только политические, но и административные и юридические. Праймериз официально организуются публичными властями и проводятся обычно в таких же пунктах для голосования, что и основные выборы. Они бывают **открытыми**, когда голосовать может любой, и **закрытыми**, когда право голоса имеют только члены партии, проводящей предварительные выборы. При открытых праймериз у входа в пункт для голосования избиратели получают несколько бюллетеней, по одному от каждой партии, или один общий бюллетень с разделением списков по партиям. Далее избиратель делает выбор кандидатов только в одном бюллетене (в одном списке).

Composite Sample Ballot - Guilford County, NC – May 6th, 2008, Primary Election

Democrat Composite Sample Ballot

PRESIDENTIAL PREFERENCE

(You may vote for ONE)

☐ Hillary Clinton

☐ Mike Gravel

☐ Barack Obama

☐ No Preference

US SENATE

(You may vote for ONE)

☐ Kay Hagan

☐ Dusk C. Lassiter

☐ Jim Neal

☐ Howard Staley

☐ Marcus W. Williams

Precincts: G16, G18, G19, G20, G21, G22, G27, G30, G31, G32, G33, G34, G35, G40A1, G40A2, G40B, G41A, G41B, G42A, G42B, G43, G63, G64*, H04, H14, H15, H16, H20A, H20B, H21, H22, H23, H24, H25, H26, H27, C01, C02, FEN2, FR1, FR2, FR3, FR4, FRS4, FR5B, GIB, GR, JAM1, JAM5, JEF1, JEF2*, JEF4, MON1, MON3, NCGR1, NCGR2, NCLAY1, NCLAY2, NDRI, NWSH, OR1, OR2, PG1, PG2, RC1, RC2, SCLAY, SDRI, SFI, SF2, SF3, SF4, SMAD, STOK, SUM3, SUM4, SWASH

US CONGRESS

DISTRICT 6
(You may vote for ONE)

☐ Johnny J. Carter

☐ Jay Ovitore

☐ Teresa Sue Bratton

Precincts: G01, G02, G03, G05, G06, G07, G08, G09, G10, G11, G12, G13, G14, G15, G17, G23, G24, G25, G26, G28, G29, G36, G37, G38, G39, G44, G45, G47, G48, G49, G50, G51, G56, G58, G59*, G60, G72, G73A, CG3B, JEF2*, MON2, NMAD

US CONGRESS

DISTRICT 13
(You may vote for ONE)

☐ Derald Hafner

☐ Brad Miller

GOVERNOR

(You may vote for ONE)

☐ Richard H. Moore

☐ Dennis Nielsen

☐ Bev Perdue

LIUTENANT GOVERNOR

(You may vote for ONE)

☐ Walter H. Dalton

☐ Hampton Dellinger

☐ Pat Smathers

☐ Dan Besse

AUDITOR

(You may vote for ONE)

☐ Beth A. Wood

☐ Fred Alkens

COMMISSIONER OF INSURANCE

(You may vote for ONE)

☐ Wayne Goodwin

☐ David C. Smith

COMMISSIONER OF LABOR

(You may vote for ONE)

☐ Mary Fant Donnan

☐ Ty Richardson

☐ Robin Anderson

☐ John C. Brooks

SUPERINTENDENT OF PUBLIC INSTRUCTION

(You may vote for ONE)

☐ Eddie Davis

☐ June St. Clair Atkinson

TREASURER

(You may vote for ONE)

☐ Janet Covell

☐ Michael Welsel

☐ David Young

Precincts: FEN1, FR1, FR2, G03, G04, G05, G06, G46, G52*, G53, G64*, G65, G66, G67, G68, G69, G70, G71, G72, G73, G74, G75, H01, H02, H03, H04, H05, H06, H07, H08, H09, H10, H11, H12, H17, H18, H19A, H19B, H20A, H20B, H26, H27A, H27B, H28, H29, JAM1, JAM2, JAM3, JAM4, JAM5, JEF1*, JEF2*, JEF3, JEF4, PG1, PG2, SDRI*, SUM1, SUM2, SUM3, SUM4

STATE SENATE

DISTRICT 28
(You may vote for ONE)

☐ Bruce Davis

☐ Katie O. Dorsett

Precincts: G01, G02, G07, G46, G47, G52, G54, G56, G57, G58, G59, G60, G67, G68, G69, G70

COUNTY COMMISSIONER

DISTRICT 8
(You may vote for ONE)

☐ Greg Woodard

☐ Skip Alston

На основании полученных результатов определялся рейтинг кандидатов и формировались группы поддержки каждого претендента на президентский пост. Затем участники национальных партийных съездов (конвентов) избирали одного кандидата в президенты и одного - в вице-президенты, за который в дальнейшем рекомендовалось голосовать сторонникам партии на основных выборах. Первые праймериз состоялся в 1904 г. в штате Флорида; к 1916 г. они практиковались в 20 штатах. С 1952 г. институт «первичных выборов» становится неотъемлемой частью кампании по выборам президента США.

- (1) Избирательная комиссия формирует списки голосующих и готовит (получает) бюллетени.
- (2) В день выборов голосующий приходит на избирательный участок, предъявляет паспорт (или другой документ, удостоверяющий личность), его регистрируют в списке избирателей, он получает бюллетень, расписывается в его получении, голосует (например, ставит галочку в бюллетене напротив ФИО кандидата, за которого он голосует) и опускает бюллетень в урну.
- (3) После окончания голосования избирательная комиссия подсчитывает результаты голосования и отправляет результаты в центральную избирательную комиссию (ЦИК).

1. Члены избирательной комиссии могут проголосовать вместо не пришедших на выборы избирателей (-2, -4).

2. В кабинках для голосования могут быть установлены скрытые камеры (-3).

3. Члены избирательной комиссии могут сделать недействительными некоторые бюллетени (например, поставив вторую галочку в бюллетене) или поставить галочку напротив «нужного» кандидата, если в бюллетене нет никаких пометок (-5).

4. Итоги голосования могут быть неправильно подсчитаны (непреднамеренные ошибки).

5. Итоги голосования могут быть преднамеренного искажены.

6. Избиратель не может проверить, что его голос учтен и, тем более, учтен ли правильно.

7. Простой избиратель не знает кто голосовал, а кто нет.

8. Результаты голосования обрабатываются относительно долго (в частности окончательные результаты голосования, как правило, становятся известны через несколько дней).

Чтобы устранить последний недостаток во многих странах (США, Европа, Бразилия, Россия и др.) стали внедрять системы электронного голосования (СЭГ). К достоинствам последних стоит отнести и возможность дистанционного голосования, что положительно сказывается на увеличении числа голосующих избирателей.

Электронное голосование - термин, определяющий различные виды голосования, охватывающий как электронные средства голосования (электронная демократия), так и электронные средства подсчета голосов. Разновидностью электронного голосования являются Интернет-выборы [17].

Интернет-выборы - один из способов электронного голосования, представляющий собой проведение части или полностью голосования на выборах и референдумах с использованием сети Интернет. Одним из первых экспериментов по внедрению Интернет-голосования был проведён Избирательной комиссией Волгоградской области на голосовании в Урюпинске в 2009 г.

Системы электронного голосования применяются на выборах с 1960х годов, с тех пор, как появились перфокарты. Более новая система оптического сканирования может считывать отметку, поставленную избирателем, с бюллетеня. Системы прямой записи голосов на базе устройств с кнопками или сенсорными экранами, накапливающие голоса, повсеместно используются в Бразилии. Они довольно сильно распространены в Индии, Нидерландах, Венесуэле и США. Системы телефонного и Интернет-голосования завоевали популярность и используются на правительственных выборах и референдумах в Великобритании, Эстонии и Швейцарии, а также муниципальных выборах в Канаде и партийных выборах в США и Франции.

Известные проблемы использования первых систем электронного голосования:

- отсутствие анонимности во многих системах при голосовании с помощью ID-cards, телефонном и Интернет-голосовании;

- возможность продажи голосов;

- 30 октября 2006г., Нидерланды. Была отозвана лицензия на 1187 устройств из-за того, что они позволяли следить за процессом голосования с расстояния до 40 метров;

- 2 марта 2004г., Калифорния. Устройства PES TSx не позволили большому количеству избирателей исполнить свой долг из-за неисправных считывателей электронных карт для голосования;

- октябрь 2006г., Майами. Из-за неправильной калибровки сенсорного экрана три голоса были учтены как голоса за демократов, хотя отображались как голоса за республиканцев;

- устройства AccuVote-TSx были изучены группой учёных из университета Принстона. Они показали, что на эти машины может быть установлено мошенническое ПО менее чем за минуту. Кроме того, эти устройства могли передавать друг другу компьютерные вирусы во время сеансов связи;

- одна из лабораторий, занимающихся компьютерной безопасностью, продемонстрировала способ изготовить и внедрить в оборудование компании Diebold Electronic System жучок, который позволит вводить в аппарат, в т.ч. и дистанционно, любую информацию. Цена «проекта» - 25\$, уровень технологии – школьный радиокружок [32].

Несмотря на приведенные выше проблемы, характерные для первых попыток разработки и использования электронного оборудования на выборах, электронное голосование приобретает в мире всё более широкое распространение.

По мнению одного из крупнейших специалистов в области информационной безопасности Брюса Шнайера **идеальный протокол электронного голосования** должен обладать следующими свойствами [8].

1. Голосовать могут только те, кто имеет право.

2. При подсчете результатов голосования для каждого избирателя учитывается не более одного голоса.

3. Никто не может узнать, за кого проголосовал конкретный избиратель (т.е. должна обеспечиваться анонимность голосования).

4. Никто не может проголосовать за другого.

5. Никто не может тайно изменить чей-то голос.

6. Избиратель может проверить, что его голос учтен при подведении итогов голосования.

7. Каждый знает кто голосовал, а кто нет.

Желательны также два дополнительных свойства.

8. Избиратель может изменить свое мнение (т.е., аннулировать свой бюллетень и проголосовать заново) в течение заданного периода времени.

9. Если избиратель обнаруживает, что его голос засчитан неправильно, он может подать протест.

Ниче рассматривается ряд протоколов электронного голосования на базе симметричного и асимметричного шифрования, удовлетворяющие тем или иным перечисленным свойствам.

Используемые в протоколах обозначения:

• **ЦИК** – центральная избирательная комиссия;

• **ЦСК** – центр сертификации ключей. Сертифицирует, хранит, распространяет и удостоверяет подлинность открытых ключей участников протокола;

• **В** – бюллетень;

• **ID** – уникальный номер (идентификатор), однозначно связанный (ассоциируемый) с конкретным избирателем. В качестве **ID** может использоваться идентификатор электронного удостоверения личности, как это делается в Эстонии. В РФ может быть использован идентификатор Универсальной электронной карты или будущего электронного паспорта;

• **М** – уникальный номер (метка), который нельзя сопоставить с конкретным избирателем (по крайней мере, для комиссии, выполняющей подсчет голосов и публикацию результатов голосования). Генерируется разово, специально для процедуры голосования;

• **k_{pub}**, **k_{priv}** – открытый и закрытый ключи для асимметричного шифрования. Открытый ключ доступен всем желающим и однозначно связан (ассоциирован) с **ID**;

• **k_{en}**, **k_{dec}** – асимметричные ключи шифрования и расшифрования. В отличие от предыдущей пары ключей, **k_{en}** (аналог открытого ключа **k_{pub}**) хранится в тайне;

• **k_{secr}** – секретный ключ для симметричного или асимметричного шифрования. Для симметричного шифрования рекомендуется использовать блочные комбинированные шифры;

• **DS** (англ. digital signature) – электронная цифровая подпись, ЭЦП;

• **h(X)** – процедура хеширования сообщения **X**;

• **encrypt(k, X)** – процедура шифрования ключом **k** сообщения **X**;

- $\text{decrypt}(k, X)$ – процедура расшифрования ключом k сообщения X ;
- $\text{sign}(k, X) = \text{encrypt}(k, X)$ – процедура создания ЭЦП ключом k для сообщения X ;
- $\text{unsign}(k, X) = \text{decrypt}(k, X)$ – процедура проверки ЭЦП ключом k для сообщения X ;
- $\text{blind}(\{r, k\}, X) = \text{encrypt}(\{r, k\}, X)$ – процедура зашифрования с помощью «закрывающего множителя» r и ключа k сообщения X ;
- $\text{unblind}(\{r^{-1}, k\}, X) = \text{encrypt}(\{r^{-1}, k\}, X)$ – процедура расшифрования с помощью «раскрывающего множителя» r^{-1} и ключа k сообщения X ;
- $\{\}$ – набор данных;
- $*$ – множество однотипных данных;
- $=$ – определение (расчет) значения по определенному алгоритму;
- $==$ – сравнение значений;
- **защищенный канал** – канал связи, который не прослушивается злоумышленниками или по которому информация передается в зашифрованном виде;
- **анонимно** – передача информации таким образом, чтобы получатель не мог определить отправителя.

17.3.2. Упрощенный протокол голосования №1 [8]

Схема голосования.

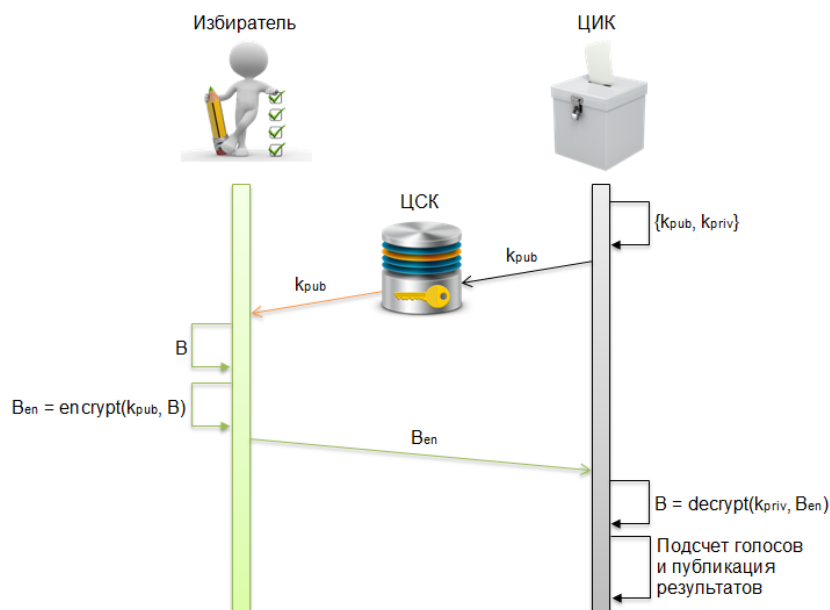


Рис.17.34. Схема упрощенного протокола голосования №1

(1) ЦИК:

- создает пару ключей для асимметричного шифрования $\{k_{pub}, k_{priv}\}$;
- публикует открытый ключ k_{pub} в ЦСКИ. ЦСКИ может быть независимой организацией или подчиняться ЦИК.

(2) Избиратель:

- делает свой выбор в бюллетене B ;
- с помощью открытого ключа ЦИК k_{pub} шифрует бюллетень $B_{en} = \text{encrypt}(k_{pub}, B)$;
- посылает зашифрованный бюллетень B_{en} в ЦИК.

(3) ЦИК:

- с помощью своего закрытого ключа k_{priv} расшифровывает бюллетень $B = \text{decrypt}(k_{priv}, B_{en})$;
- подводит подсчет голосов;
- публикует результаты голосования.

Достоинства и недостатки. Этот протокол приводит к массе проблем. ЦИК не может узнать, откуда получены бюллетени, и даже, принадлежат ли присланные бюллетени правомочным избирателям. У нее нет ни малейшего представления о том, голосовали ли избиратели больше одного раза. Положительной стороной является невозможность изменить бюллетень другого человека (для этого и используется шифрование), но никто и не будет пытаться это сделать, потому что гораздо проще голосовать повторно, добиваясь нужных результатов выборов.

17.3.3. Упрощенный протокол голосования №2 [8]

Схема голосования.

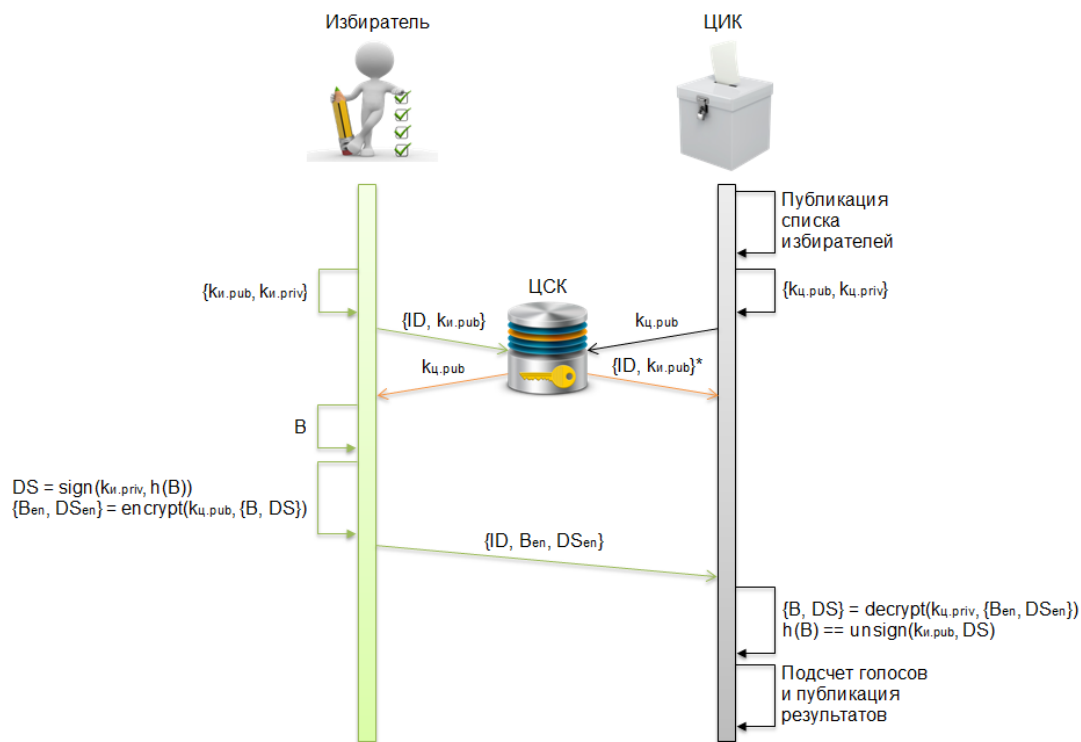


Рис.17.35. Схема упрощенного протокола голосования №2

(1) ЦИК:

- публикует список всех правомочных избирателей;
- создает пару ключей для асимметричного шифрования $\{k_{ц, pub}, k_{ц, priv}\}$;
- публикует открытый ключ $k_{ц, pub}$ в ЦСК. ЦСК может быть независимой организацией или подчиняться ЦИК.

(2) Избиратель:

- создает пару ключей для асимметричного шифрования $\{k_{и, pub}, k_{и, priv}\}$ и публикует открытый ключ $k_{и, pub}$ в ЦСК. Публикация ключа подразумевает его регистрацию на конкретного избирателя с присвоенным ему ID;
- делает свой выбор в бюллетене B;
- с помощью своего закрытого ключа $k_{и, priv}$ подписывает бюллетень $DS = \text{sign}(k_{и, priv}, h(B))$;
- с помощью открытого ключа ЦИК $k_{ц, pub}$ шифрует бюллетень и ЭЦП к нему $\{B_{en}, DS_{en}\} = \text{encrypt}(k_{ц, pub}, \{B, DS\})$;
- посылает в ЦИК свой идентификатор ID, зашифрованный бюллетень B_{en} и ЭЦП к нему DS_{en} .

(3) ЦИК:

- с помощью своего закрытого ключа $k_{ц, priv}$ расшифровывает бюллетень и ЭЦП $\{B, DS\} = \text{decrypt}(k_{ц, priv}, \{B_{en}, DS_{en}\})$;
- с помощью открытого ключа избирателя $k_{и, pub}$ проверяет ЭЦП к бюллетеню $h(B) = \text{decrypt}(k_{и, pub}, DS)$;
- подводит подсчет голосов;
- публикует результаты голосования.

Достоинства и недостатки. Протокол обладает свойствами 1 и 2 идеального протокола (только правомочные избиратели могут голосовать и никто не может голосовать более одного раза). Каждый бюллетень подписан закрытым ключом избирателя, поэтому ЦИК знает, кто и как голосовал. Если получен бюллетень, который не подписан правомочным избирателем, или бюллетень, подписанный избирателем, который уже проголосовал, то такой бюллетень игнорируется комиссией. Шифрование бюллетеней и ЭЦП к нему открытым ключом ЦИК мешает посторонним узнать, кто за кого голосовал.

На этапе (2) шифрование бюллетеня выглядит бессмысленным. Т.к. бюллетень имеет определенную структуру, то нетрудно сгенерировать все возможные варианты бюллетеней $\{B'\}^*$ и по известному открытому ключу комиссии $k_{ц, pub}$ получить зашифрованные их варианты $\{B'_{en}\}^* = \text{encrypt}(k_{ц, pub}, \{B'\}^*)$. Сравнивая перехваченный зашифрованный бюллетень B_{en} с бюллетенями из множества $\{B'_{en}\}^*$, можно сделать о выборе избирателя с идентификатором ID. По отношению к ЦИК также отсутствует анонимность, т.к. комиссия знает ID и выбор избирателя (бюллетень B).

17.3.4. Протокол двух агентств Нурми-Саломая-Сантин

Протокол был предложен Ханну Нурми (Hannu Nurmi), Арто Саломая (Arto Salomaa) и Лилой Сантин (Lila Santean). Функции ЦИК согласно протокола распределены между двумя агентствами:

- регистратор (англ. validator, administrator) – агентство, выполняющее регистрацию избирателей;
- счетчик (англ. tallier, counter) – агентство, выполняющее прием и подсчет бюллетеней.

Схема голосования.

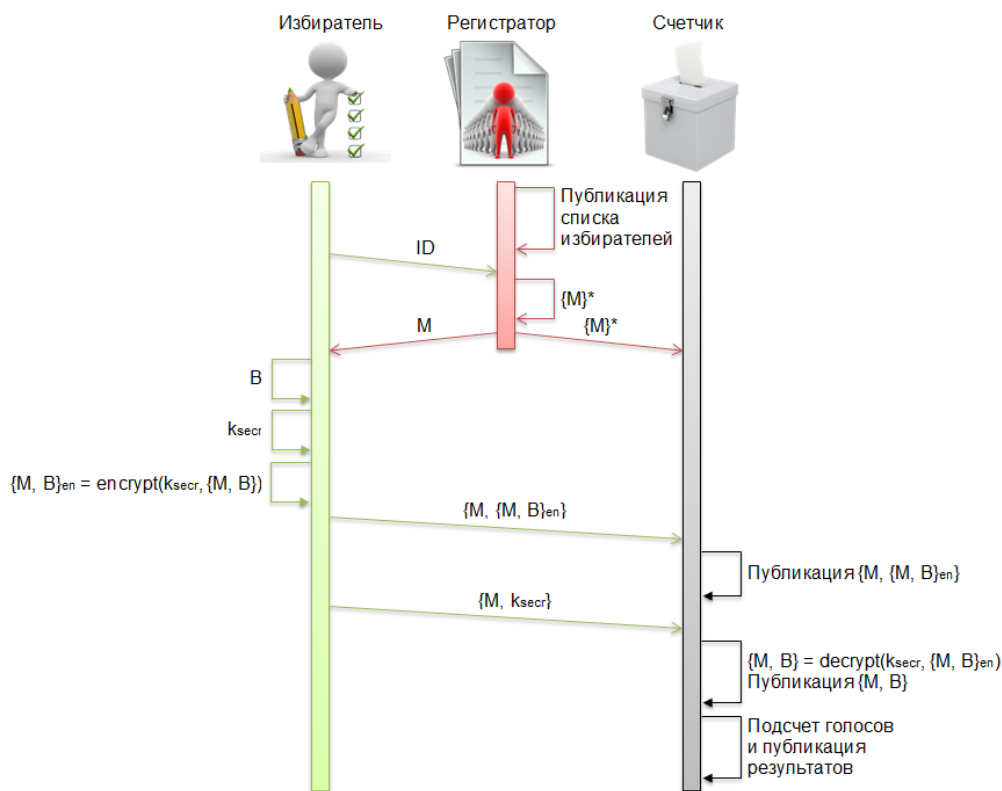


Рис.17.36. Схема протокола двух агентств Нурми-Саломая-Сантин

(1) Регистратор:

- публикует список всех правомочных избирателей.

(2) Избиратель:

- регистрируется для голосования (высылает регистратору по защищенному каналу свой уникальный идентификатор **ID**).

(3) Регистратор:

- высылает по защищенному каналу каждому правомочному избирателю уникальную метку **M**;
- высылает счетчику список уникальных меток $\{M\}^*$, но без указания, какому избирателю, какая метка принадлежит.

(4) Избиратель:

- делает свой выбор в бюллетене **B**;
- создает секретный ключ для симметричного шифрования k_{secr} ;
- с помощью секретного ключа k_{secr} шифрует уникальную метку и бюллетень в виде единого файла $\{M, B\}_{en} = \text{encrypt}(k_{secr}, \{M, B\})$;
- анонимно посылает свою метку **M** и зашифрованный файл $\{M, B\}_{en}$ счетчику.

(5) Счетчик:

- по истечении времени, отведенного на голосование, публикует все метки **M** и зашифрованные файлы $\{M, B\}_{en}$ в доказательство избирателю, что его голос принят и без искажений (подмены).

(6) Избиратель:

- анонимно высылает счетчику секретный ключ k_{secr} для метки **M**.

(7) Счетчик:

- с помощью секретного ключа k_{secr} расшифровывает файл $\{M, B\} = \text{decrypt}(k_{secr}, \{M, B\}_{en})$;
- в дополнение к $\{M, \{M, B\}_{en}\}$ публикует $\{M, B\}$ для того, чтобы избиратель убедился в правильности учета его голоса;
- подводит подсчет голосов;
- публикует результаты голосования.

Достоинства и недостатки. Протокол обладает практически всеми свойствами идеального протокола, за исключением свойства 3. Регистратор знает, какие метки принадлежат каким избирателям и, соответственно, их выбор. В связи с этим избирателям приходится надеяться на честность регистратора, отсутствие сговора между регистратором и счетчиком, взлома БД регистратора злоумышленниками и т.п.

Для обеспечения свойства 7 по окончании голосования регистратор, зная опубликованный счетчиком список принятых меток, может опубликовать списки проголосовавших избирателей, но без указания их меток.

Протокол обладает также дополнительными свойствами.

Избиратель может изменить свое мнение (свойство 8). Для этого он высылает метку **M**, секретный ключ k_{secr} и новый зашифрованный файл $\{M, B'\}_{en}$. Счетчик расшифровывает ранее посланный бюллетень $\{M, B\}_{en}$ и сравнивает метки, высланную в открытом виде и содержащуюся в зашифрованном файле. В случае их совпадения $\{M, B\}_{en}$ меняется на $\{M, B'\}_{en}$.

Если избиратель обнаруживает, что его голос засчитан неправильно (свойство 9), он может подать протест, предоставив счетчику $\{M, k_{secr}, \{M, B\}_{en}\}$.

Протокол, предложенный в 1992 г. Фудзика (Atsushi Fujioka), Окамото (Tatsuaki Okamoto) и Охта (Kazuo Ohta), является дальнейшим развитием предыдущего протокола и позволяет избежать сговора между регистратором и счетчиком [55]. Это достигается за счет использования «слепой» ЭЦП.

Схема голосования.

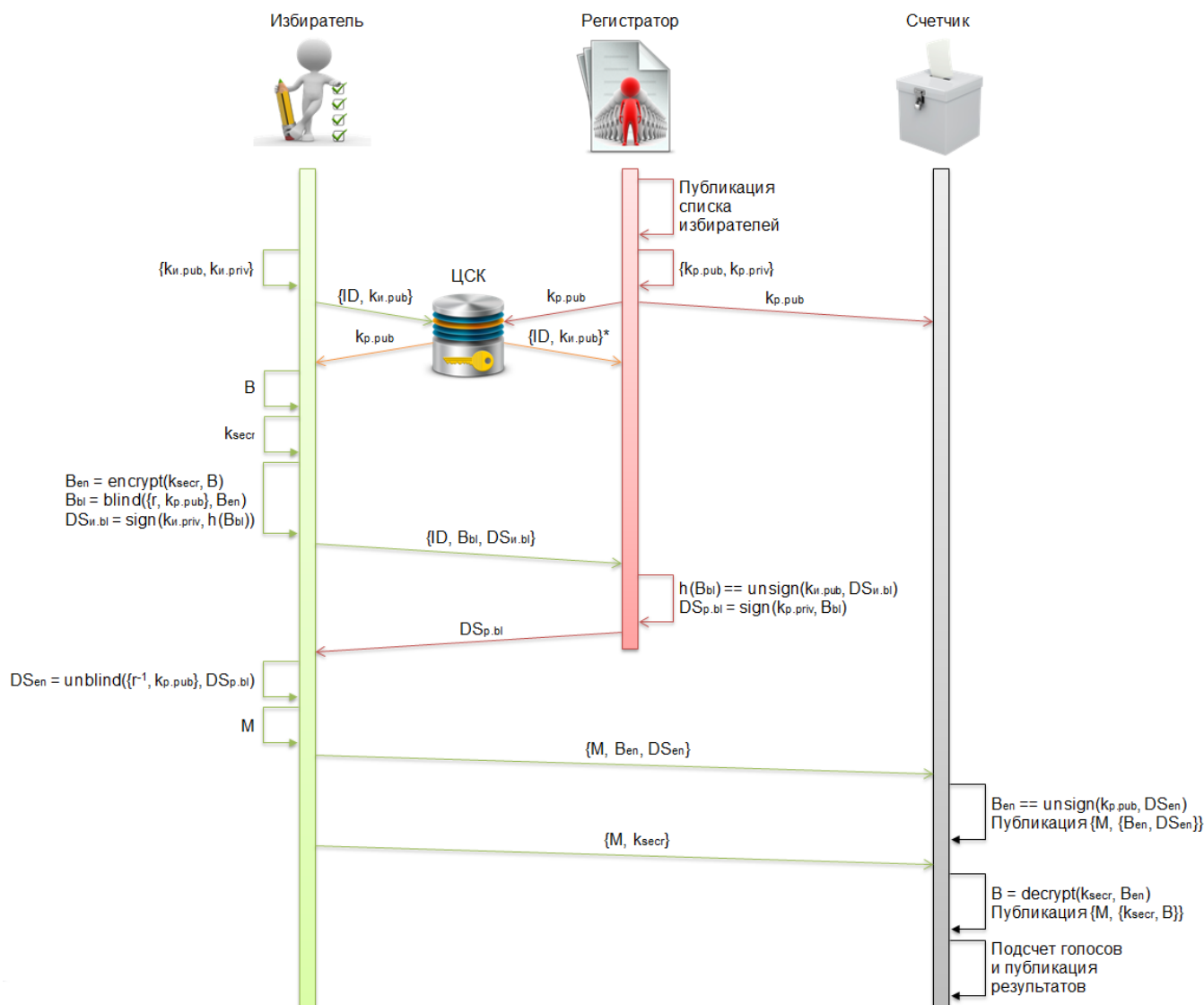


Рис.17.37. Схема протокола двух агентств Фудзика-Окамото-Охта

(1) Регистратор:

- публикует список всех правомочных избирателей;
- создает пару ключей для асимметричного шифрования $\{k_{p, pub}, k_{p, priv}\}$;
- публикует открытый ключ $k_{p, pub}$ в ЦСК. ЦСК может быть независимой организацией или подчиняться регистратору.

(2) Избиратель:

- создает пару ключей для асимметричного шифрования $\{k_{n, pub}, k_{n, priv}\}$ и публикует открытый ключ $k_{n, pub}$ в ЦСК. Публикация ключа подразумевает его регистрацию на конкретного избирателя с присвоенным ему ID;
- создает секретный ключ k_{secr} ;
- делает свой выбор в бюллетене B ;
- с помощью секретного ключа k_{secr} шифрует бюллетень $B_{en} = \text{encrypt}(k_{secr}, B)$;
- с помощью «закрывающего множителя» r и открытого ключа регистратора $k_{p, pub}$ скрывает содержимое зашифрованного бюллетеня $B_{bl} = \text{blind}(r, k_{p, pub}, B_{en})$;
- с помощью своего закрытого ключа $k_{n, priv}$ стандартным образом (через хеш-образ) подписывает скрытый зашифрованный бюллетень $DS_{n, bl} = \text{sign}(k_{n, priv}, h(B_{bl}))$;
- посылает регистратору свой идентификатор ID, скрытый зашифрованный бюллетень B_{bl} и ЭЦП к нему $DS_{n, bl}$.

(3) Регистратор:

- стандартным образом (через хеш-образ) с помощью открытого ключа избирателя $k_{n, pub}$ проверяет его ЭЦП к скрытому зашифрованному бюллетеню $h(B_{bl}) == \text{unsign}(k_{n, pub}, DS_{n, bl})$;
- с помощью своего закрытого ключа $k_{p, priv}$ подписывает скрытый зашифрованный бюллетень $DS_{p, bl} = \text{sign}(k_{p, priv}, B_{bl})$;
- посылает избирателю «слепую» ЭЦП $DS_{p, bl}$ к скрытому зашифрованному бюллетеню B_{bl} ;

(4) Избиратель:

- снимает «закрывающий множитель» r со «слепой» ЭЦП регистратора $DS_{p,bl}$ и получает ЭЦП регистратора $DS_{en} = \text{unblind}(\{r^{-1}, k_{p,pub}\}, DS_{p,bl})$ к зашифрованному бюллетеню B_{en} ;
- создает секретную уникальную метку M ;
- анонимно посылает счетчику свою метку M , зашифрованный бюллетень B_{en} и ЭЦП регистратора к нему DS_{en} .

(5) Счетчик:

- с помощью открытого ключа регистратора $k_{p,pub}$, высланного напрямую регистратором или полученному из ЦСК, проверяет ЭЦП к зашифрованному бюллетеню $B_{en} == \text{unsign}(k_{p,pub}, DS_{en})$;
- по истечении времени, отведенного на голосование, публикует все метки M и зашифрованные бюллетени с ЭЦП к ним $\{B_{en}, DS_{en}\}$ в доказательство избирателю, что его голос принят.

(6) Избиратель:

- анонимно высылает счетчику секретный ключ k_{secc} для метки M .

(7) Счетчик:

- с помощью секретного ключа k_{secc} расшифровывает бюллетень $B = \text{decrypt}(k_{secc}, B_{en})$;
- в дополнение к $\{M, \{B_{en}, DS_{en}\}\}$ публикует $\{M, \{k_{secc}, B\}\}$ для того, чтобы избиратель убедился в правильности учета его голоса;
- подводит подсчет голосов;
- публикует результаты голосования.

Достоинства и недостатки. Т.к. никто, кроме избирателя, не может сопоставить одновременно DS_{en} , $DS_{n,bl}$ и $DS_{p,bl}$, а также ID и M , то исключается раскрытие выбора избирателя (обеспечивается полная анонимность).

Свойства 7 не может быть обеспечено, если только избиратель не раскроет свою личность.

Для изменения выбора избирателя в течение заданного периода времени (свойство 8):

- избирателю вначале необходимо аннулировать свой бюллетень у счетчика с раскрытием своей личности, предоставив $\{ID, M, k_{secc}\}$;
- счетчик должен уведомить регистратора, что бюллетень избирателя с конкретным ID аннулирован;
- повторить этапы со 2 по 5.

Раскрытие личности при аннулировании бюллетеня необходимо с целью исключения повторного голосования избирателем.

Незначительной модификацией данного протокола является протокол **Sensus** [<http://lorrie.cranor.org/voting/sensus>], предложенный Лорри Кранор (Lorrie F. Cranor) и Роном Ситроном (Ron K. Cytron) в 1997 г. [56]. На этапе (5), после проверки подписи регистратора, счетчик сразу высылает избирателю квитанцию с уведомлением, что его голос принят, а избиратель, не дожидаясь конца подачи голосов остальными избирателями, высылает счетчику секретный ключ k_{secc} .

17.3.6. Протокол голосования с одной Центральной комиссией на базе протокола ANDOS [8]

ANDOS (англ. All or Nothing Disclosure Of Secrets - раскрытие секрета «всё или ничего») - криптографический протокол «секретной продажи секретов». Пусть продавец имеет список секретов с ответами и выставляет их на продажу. Покупатель желает купить секрет, но не хочет раскрывать какой именно. Протокол гарантирует, что покупатель получит нужный ему секрет и ничего более, в то время как продавец не будет знать, какой именно секрет получил покупатель.

Схема голосования.

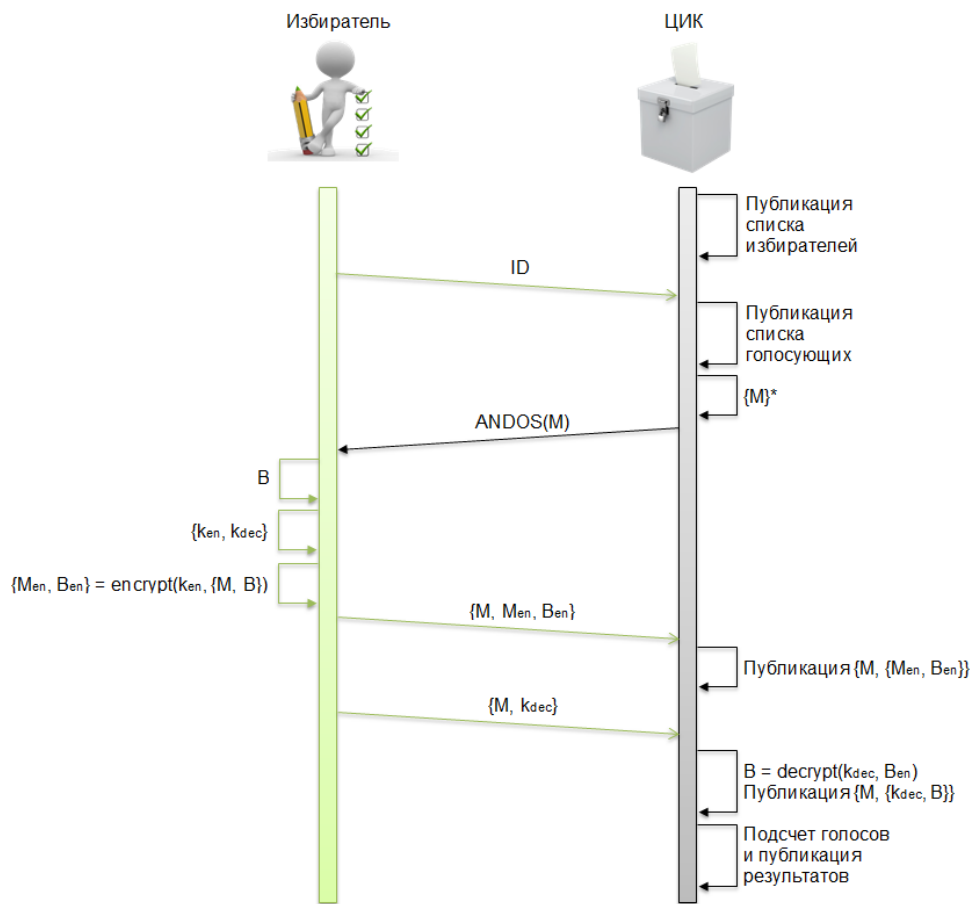


Рис.17.38. Схема протокола голосования с одной Центральной комиссией на базе протокола ANDOS

(1) ЦИК:

- публикует список всех правомочных избирателей.

(2) Избиратель:

- регистрируется для голосования, т.е. в течение определенного срока сообщает в ЦИК, собирается ли он голосовать.

(3) ЦИК:

- публикует список голосующих;
- генерирует набор уникальных меток $\{M\}^*$ и с помощью протокола ANDOS распределяет их между голосующими. Особенность протокола заключается в невозможности для ЦИК в дальнейшем определить принадлежность метки конкретному избирателю.

(4) Избиратель:

- создает пару ключей для асимметричного шифрования $\{k_{en}, k_{dec}\}$. В отличие от классического асимметричного шифрования один из ключей (аналог открытого ключа) не публикуется;
- делает свой выбор в бюллетене B ;
- с помощью секретного ключа k_{en} шифрует бюллетень и уникальную метку $\{M_{en}, B_{en}\} = \text{encrypt}(k_{en}, \{M, B\})$;
- анонимно посылает в ЦИК незашифрованную уникальную метку M , зашифрованную метку M_{en} и бюллетень B_{en} .

(5) Счетчик:

- по истечении времени, отведенного на голосование, публикует все метки M и соответствующую ей зашифрованную пару $\{M_{en}, B_{en}\}$ в доказательство избирателю, что его голос принят.

(6) Избиратель:

- анонимно высылает счетчику секретный ключ дешифрования k_{dec} для метки M .

(7) Счетчик:

- с помощью секретного ключа k_{dec} расшифровывает бюллетень $B = \text{decrypt}(k_{dec}, B_{en})$;
- в дополнение к $\{M, \{M_{en}, B_{en}\}\}$ публикует $\{M, \{k_{dec}, B\}\}$ для того, чтобы избиратель убедился в правильности учета его голоса;
- подводит подсчет голосов;
- публикует результаты голосования.

Этапы (1) – (3) являются предварительными. Их цель состоит в том, чтобы узнать и опубликовать всех действительных избирателей. Хотя некоторые из них, вероятно, не примут участие в голосовании, это уменьшает возможность ЦИК добавить поддельные бюллетени.

На этапе (4) два избирателя могут получить одну и ту же метку. Эта возможность может быть минимизирована, если число возможных меток будет гораздо больше, чем число реальных избирателей. Если два избирателя присылают бюллетени с одинаковой меткой, ЦИК генерирует новую метку M' , выбирает одного из избирателей и публикует $\{M, M', \{M_{en}, B_{en}\}\}$.

Т.к. ключ шифрования k_{en} не публикуется, то асимметричное шифрование в протоколе можно заменить симметричным с одним ключом k_{seer} .

Достоинства и недостатки. Протокол обладает всеми свойствами идеального протокола, включая дополнительные 8 и 9, за исключением свойства 7.

Если избиратель хочет изменить свой выбор (свойство 8) с **B** на **B'**, то он посылает ЦИК $\{M, k_{dec}, \{M_{en}, B'_{en}\}\}$. С помощью секретного ключа k_{dec} ЦИК расшифровывает предыдущее зашифрованное сообщение $M' = \text{decrypt}(k_{dec}, M_{en})$, сравнивает метки $M' = M$ и, в случае совпадения меняет $\{M_{en}, B_{en}\}$ на $\{M_{en}, B'_{en}\}$. Естественно для создания новой пары $\{M_{en}, B'_{en}\}$ должна быть применена новая пара ключей $\{k_{en}, k_{dec}\}$.

Если избиратель обнаруживает, что его бюллетень подсчитан неправильно (свойство 9), он протестует, посылая ЦИК $\{M, k_{dec}, \{M_{en}, B_{en}\}\}$.

Одной из проблем этого протокола является то, что ЦИК сможет воспользоваться правом голоса людей, которые сообщили о намерении голосовать на этапе (2), но не голосовали в действительности. Другой проблемой является сложность протокола ANDOS (плохая масштабируемость). Авторы рекомендуют разбивать избирателей на меньшие группы, например избирательные округа.

17.3.7. Протокол голосования с одной Центральной комиссией на базе «слепой» подписи

В основе протокола лежит идея использования «слепой» ЭЦП, но не для бюллетеня, как в протоколах двух агентств Фудзико-Окамото-Охта и Sensus, а для персонифицированной метки **M** с целью обеспечения анонимности избирателя (свойство 3). Эта идея очевидна, но автор не встречал в открытой печати описание подобного протокола.

Схема голосования.

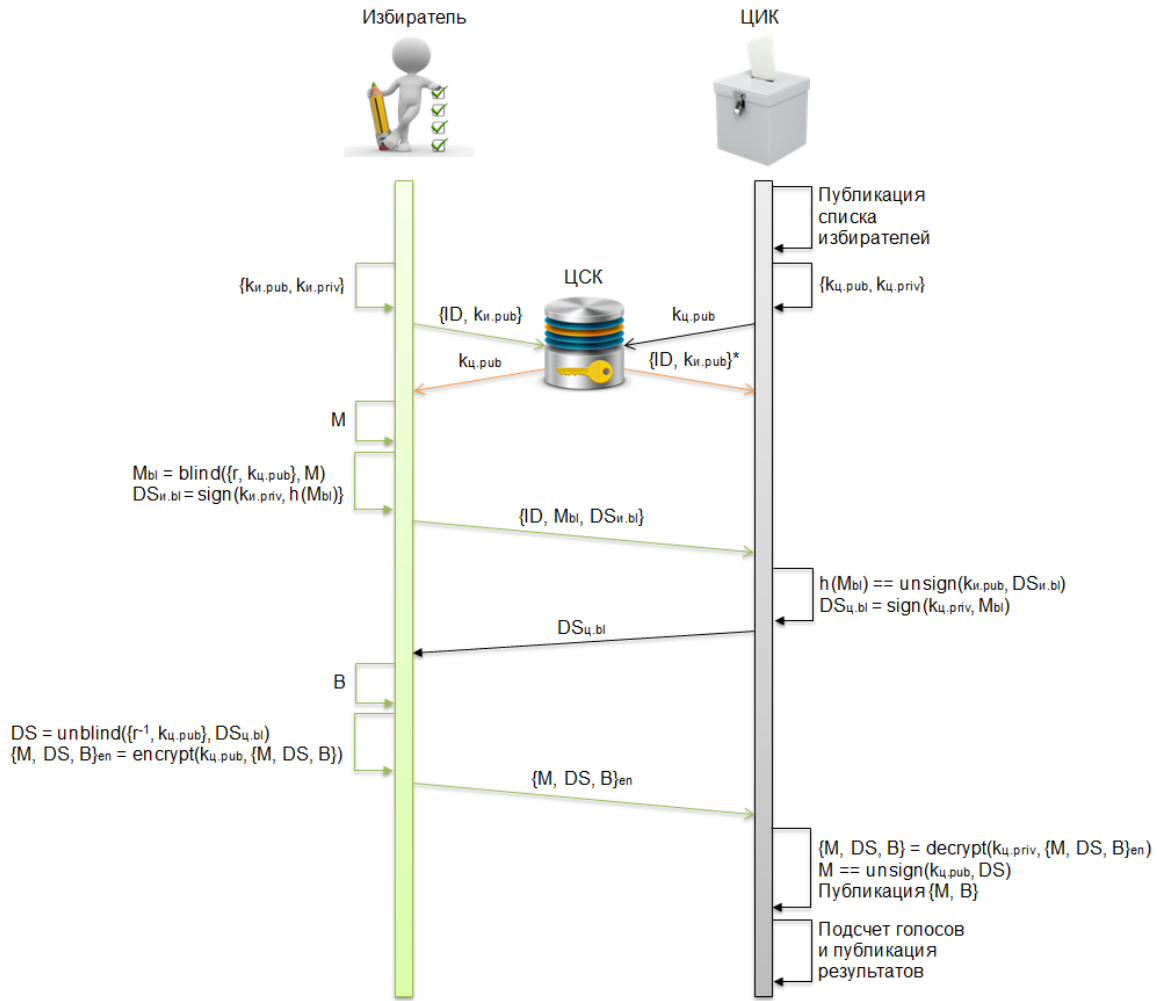


Рис.17.39. Схема протокола голосования с одной Центральной комиссией на базе «слепой» подписи

(1) ЦИК:

- публикует список всех правомочных избирателей;
- создает пару ключей для асимметричного шифрования $\{k_{p, pub}, k_{p, priv}\}$;
- публикует открытый ключ $k_{p, pub}$ в ЦСК. ЦСК может быть независимой организацией или подчиняться ЦИК.

(2) Избиратель:

- создает пару ключей для асимметричного шифрования $\{k_{u, pub}, k_{u, priv}\}$ и публикует открытый ключ $k_{u, pub}$ в ЦСК. Публикация ключа подразумевает его регистрацию на конкретного избирателя с присвоенным ему **ID**;
- генерирует уникальную метку **M**;
- с помощью «закрывающего множителя» **r** и открытого ключа ЦИК $k_{u, pub}$ скрывает содержимое метки $M_{bl} = \text{blind}(\{r, k_{u, pub}\}, M)$;
- стандартным образом (через хеш-образ) с помощью своего закрытого ключа $k_{u, priv}$ подписывает содержимое метки $DS_{u, bl} = \text{sign}(k_{u, priv}, h(M_{bl}))$;
- посылает ЦИК свой **ID**, скрытую метку M_{bl} и ЭЦП к ней $DS_{u, bl}$.

(3) ЦИК:

- стандартным образом (через хеш-образ) с помощью открытого ключа избирателя $k_{u, pub}$ проверяет его ЭЦП к скрытой метке $h(M_{bl}) = \text{unsign}(k_{u, pub}, DS_{u, bl})$ с целью аутентификации избирателя (проверки, что сообщение пришло действительно от избирателя с указанным **ID**);

- с помощью своего закрытого ключа $k_{u,priv}$ подписывает скрытую метку $DS_{u,bl} = \text{sign}(k_{u,priv}, M_{bl})$;
- посылает избирателю «слепоую» ЭЦП $DS_{u,bl}$ к скрытой метке M_{bl} .

(4) Избиратель:

- снимает «закрывающий множитель» r со «слепой» ЭЦП комиссии $DS_{u,bl}$ и получает ЭЦП комиссии $DS = \text{unblind}(r^{-1}, k_{u,pub}, DS_{u,bl})$ к метке M ;
- делает свой выбор в бюллетене B ;
- с помощью открытого ключа ЦИК $k_{u,pub}$ шифрует в виде единого файла метку M , ЭЦП к ней DS и бюллетень B $\{M, DS, B\}_{en} = \text{encrypt}(k_{u,pub}, \{M, DS, B\})$. Шифрование выполняется, чтобы при посылке данного набора информации никто не смог бы подменить бюллетень. Правда, существует возможность подмены бюллетеня комиссией;
- анонимно посылает зашифрованный файл $\{M, DS, B\}_{en}$ в ЦИК.

(5) ЦИК:

- с помощью своего секретного ключа $k_{u,priv}$ расшифровывает файл $\{M, DS, B\} = \text{decrypt}(k_{u,priv}, \{M, DS, B\}_{en})$;
- с помощью своего открытого ключа $k_{u,pub}$ проверяет свою подпись DS к метке $M == \text{unsign}(k_{u,pub}, DS)$;
- публикует $\{M, B\}$ для того, чтобы избиратель убедился в правильности учета его голоса;
- подводит подсчет голосов;
- публикует результаты голосования.

Достоинства и недостатки. Протокол обладает всеми свойствами идеального протокола за исключением свойства 7.

Если избиратель хочет изменить свой выбор (свойство 8) с B на B' , то ему достаточно послать ЦИК $\{M, DS, B'\}_{en}$.

Для подачи протеста в случае, если избиратель обнаруживает, что его голос засчитан неправильно (свойство 9), протокол может быть усложнен по аналогии с протоколами, рассмотренными выше. Для этого на этапе (4) бюллетень вначале шифруется секретным ключом избирателя $B_{seccr} = \text{encrypt}(k_{seccr}, B)$, а затем формируется шифрованный файл $\{M, DS, B_{seccr}\}_{en} = \text{encrypt}(k_{u,pub}, \{M, DS, B_{seccr}\})$. ЦИК, расшифровав принятый файл $\{M, DS, B_{seccr}\}_{en}$ и проверив подпись к метке, публикует на сайте $\{M, B_{seccr}\}$. По истечении времени приема бюллетеней, избиратель анонимно высылает ключ для дешифрования $\{M, k_{seccr}\}$, ЦИК дешифрует бюллетень $B = \text{decrypt}(k_{seccr}, B_{seccr})$, публикует $\{M, k_{seccr}, B\}$, выполняет подсчет голосов и публикацию результатов голосования.

Существенным недостатком протокола является возможность продажи голосов. Получив от ЦИК подпись DS к анонимной метке M , избиратель может продать пару $\{M, DS\}$ заинтересованному лицу, которое, в свою очередь, может сделать выгодный для него выбор в бюллетене B'' и отослать $\{M, DS, B''\}_{en}$ в ЦИК. Подобный недостаток характерен для всех рассмотренных видов и протоколов голосования, включая традиционное («бумажное») голосование - избиратель может быть подкуплен до момента, когда он делает выбор в бюллетене.

17.3.8. Краткий сравнительный анализ протоколов голосования

Для рассмотренных выше протоколов характерны свои достоинства и недостатки. **Общим недостатком** является невозможность противостоять подкупу избирателей (продаже голосов). **Другой характерный недостаток** – возможность недобросовестной избирательной комиссией голосования за избирателей, не сделавших свой выбор, а также внесение в списки избирателей «мертвых душ» с последующим голосованием за них. Противостоять этому можно публикацией списка проголосовавших (свойство 7) и контролем со стороны неравнодушных граждан и организаций.

В следующей таблице приведены свойства идеального протокола и соответствие им предлагаемых протоколов.

Таблица 17.10

Свойство	Протокол						
	Традиционное («бумажное») голосование	Упрощенный протокол голосования №1	Упрощенный протокол голосования №2	Протокол двух агентств Нурми-Саломеаа-Сантин	Протоколы двух агентств Фудзикока-Окамото-Охта и Sensus	Протокол голосования с одной ЦИК на базе протокола ANDOS	Протокол голосования с одной ЦИК на базе «слепой» подписи
1. Голосование правомочными избирателями	+	-	+	+	+	+	+
2. Учет только одного голоса избирателя	+	-	+	+	+	+	+
3. Анонимность голосования	+	+	-	1)	+	+	+
4. Невозможность голосования за другого избирателя	-	-	-	+	+	+	+
5. Невозможность тайной подмены голоса избирателя	2)	+	+	+	+	+	+
6. Проверка избирателем правильности учета его голоса	-	-	-	+	+	+	+
7. Публикация списка проголосовавших	3)	-	+	+	-	-	-
8. Возможность изменения своего голоса избирателем	-	-	+	+	+	+	+
9. Возможность подачи протеста при неправильном учете голоса	-	-	-	+	+	+	+

Примечания.

- 1) Анонимность не обеспечивается по отношению к агентству, выполняющему регистрацию избирателей (регистратору).
- 2) Недобросовестные члены комиссии могут сделать бюллетень недействительным, непреднамеренно или специально исказить выбор избирателя.
- 3) С технической стороны ничто этому не мешает, но на выборах городского масштаба и выше не практикуется.

В масштабах страны для голосования используется специализированная система ГАС «Выборы». Начало создания ГАС «Выборы» положил Указ президента РФ в августе 1994 г. «О разработке и создании Государственной автоматизированной системы Российской Федерации «Выборы»». Генеральный заказчик системы - ЦИК Российской Федерации. В декабре 1999 г. были проведены государственные испытания системы. Актом, утвержденным заместителем председателя правительства РФ, ГАС «Выборы» с июля 2000 г. введена в эксплуатацию. В 2002 г. Государственной Думой принят Федеральный закон «О государственной автоматизированной системе Российской Федерации «Выборы»».

ГАС «Выборы» – это уникальная, учитывающая географические и демографические факторы современной России, территориально-распределенная система общегосударственного уровня. Она позволяет комплексно решать задачи организации избирательного процесса на всех этапах – планирование подготовки проведения выборов, учет избирателей, ввод сведений о кандидатах в депутаты, проведение голосования, подведение итогов и последующую статистическую обработку результатов. Кроме того, в систему заложены функции согласования работы избирательных комиссий разных уровней – практически в режиме реального времени подводить итоги голосования и с помощью средств отображения и Интернета доводить их до каждого гражданина России.

ГАС «Выборы» используется как во время выборов, так и в период между ними. Специальное ПО представляет собой комплексы программ (КП), позволяющие автоматизировать:

- учёт избирателей (КП «Избиратель»);
- избирательные процессы (КП «Планирование», «Территория», «Кандидат/Депутат», «Итоги»);
- подготовку картографических данных (КП «Картография»);
- учёт кадрового состава избирательных комиссий (КП «Кадры»);
- учёт и контроль использования избирательных фондов (КП «Контроль финансов»);
- процессы делопроизводства (КП «Дело»);
- процессы предоставления информации по правовому законодательству (КП «Право»).

Электронное голосование в нашей стране предусмотрено Федеральным законом «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» [33].

8 октября 2006 г. в Новгородской области впервые в истории выборов России в качестве эксперимента состоялось голосование с использованием **комплексов электронного голосования (КЭГ)** - комплексов для анонимного электронного голосования, работающих по «технологии прямой записи». КЭГ разработан отечественными производителями и с даты своего создания прошел собственный тернистый путь развития и совершенствования – требования к нему постоянно повышаются. Если в 2004 г. ему вменялось в обязанность обеспечивать выполнение 9 функций, то сейчас – уже 28.

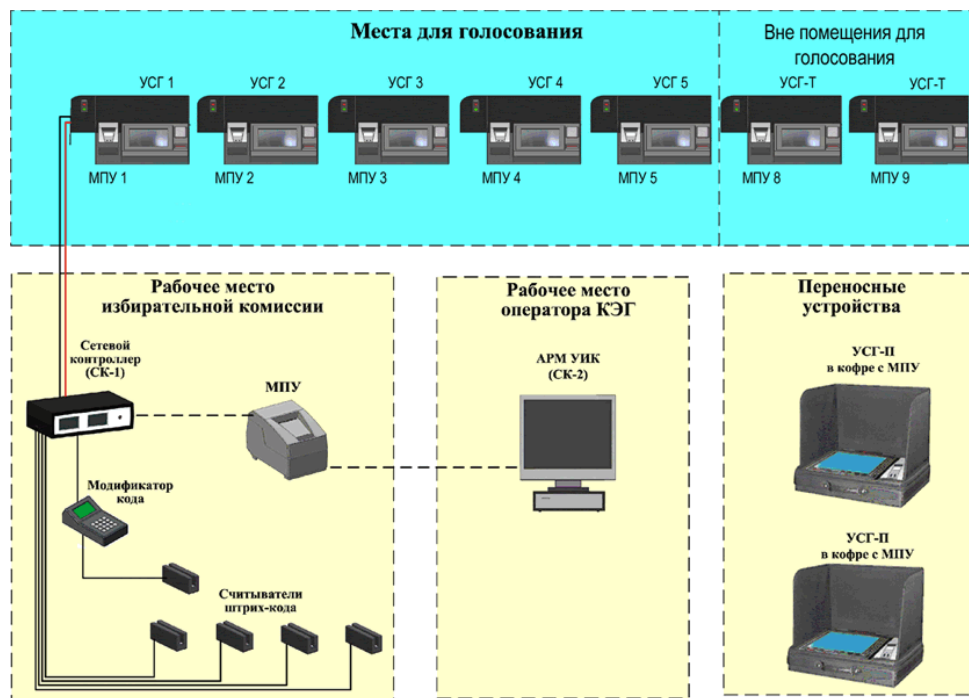


Рис.17.40. КЭГ

Технические возможности позволяют использовать в КЭГ от 2-х до 9-ти стационарных электронных машин, работающих по технологии прямой записи – **устройств для сенсорного голосования (УСГ)**, непосредственно на которых по электронному бюллетеню голосует избиратель.



Рис.17.41. УСГ

В Российской Федерации комплектация избирательного участка, утвержденная постановлением ЦИК России, предполагает использование комплекса, который в состав которого входят 5 стационарных УСГ, 2 переносных УСГ для голосования вне помещений для голосования и 2 УСГ – тренажера.

Помимо перечисленных УСГ в состав КЭГ входит периферийное оборудование (25 единиц оборудования различного назначения). В такой комплектации были оборудованы избирательные участки на выборах в единые дни голосования: в марте 2010 г. при проведении выборов депутатов Рязанской областной Думы пятого созыва 1 участок (1220 избирателей, включенных в списки избирателей) и в марте 2011 г. – 10 избирательных участков в Республике Башкортостан (10 155 избирателей).

КЭГ обеспечивает проведение электронного голосования, подсчет и распределение голосов, а также подготовку и вывод на печать протокола об итогах голосования, т.е. автоматизирует весь процесс голосования на участке. Кроме того, он имеет техническую возможность передачи данных об итогах голосования в автоматизированном режиме в вышестоящую избирательную комиссию с использованием ЭЦП.

В КЭГ не используются бумажные бюллетени. Вместо этого избиратель делает свой выбор, выбирая пальцем на экране КЭГ соответствующую его воле кандидатуру или партию. Результат этого выбора (номер выбранной кандидатуры или партии) запоминается в памяти КЭГ, а также печатается на специальной бумажной ленте, которая, впрочем, недоступна для обозрения во время голосования. С целью обеспечить доступ избирателя к голосованию, ему выдается «карточка со штрих-кодом».



Рис.17.42. Карточка со штрих-кодом

Эту карточку выбирает сам избиратель, после чего она активируется для голосования - избиратель прикладывает в избирательной кабине карточку со штрих-кодом к оптическому считывателю, данному штрих-коду программным путем присваивается признак «Голосует». Это делает данную карточку непригодной для повторного голосования, после этого избиратель голосует. Полное завершение голосования подтверждается избирателем путем нажатия экранной кнопки «ДА» в ответ на вопрос «Вы действительно хотите завершить голосование и подтверждаете Ваш выбор?»

После окончания голосования итоги голосования с каждого КЭГ переносятся в так называемый «сервисный блок» и там суммируются. После погашения оставшихся карточек и ввода данных, полученных при обработке списков избирателей, сервисный блок выдает протокол об итогах голосования.

Перед началом голосования операторы комплекса электронного голосования устанавливают в сетевой контроллер и в каждое переносное устройство для электронного голосования энергонезависимые карты памяти с записанными на них исходными данными и опечатывают их.

Основа программной среды КЭГ – операционная система Windows и СУБД Oracle.

Другой распространенный способ голосования в России, обеспечивающий автоматический подсчет голосов, заключается в использовании **комплексов обработки избирательных бюллетеней** (КОИБ, «электронная урна»).



Рис.17.43. КОИБ

В КОИБ сканирует предварительно заполненный бумажный бюллетень с волеизъявлением избирателя и производит подсчет голосов. Время двустороннего сканирования черно-белого оригинала формата А4 составляет всего полторы секунды. На подключенный к КОИБ принтер может выводиться протокол избирательной комиссии, который также в автоматическом режиме может быть передан по телекоммуникационным сетям в вышестоящую избирательную комиссию. Благодаря этим возможностям весь комплекс рассматривается как составная часть системы ГАС «Выборы».

Впервые КОИБ применялись на выборах депутатов Государственной думы и выборах президента Республики Башкортостан 7 декабря 2003 г. На выборах депутатов Государственной Думы 4 декабря 2011 г. планировалось использовать 327 КЭГ в семи субъектах Российской Федерации и 4828 в 76 регионах страны, а также на участках за рубежом – в Польше, Германии, Латвии. На 250 избирательных участках использовались КОИБ нового поколения, которые выполнены из полупрозрачного пластика. В новый КОИБ входит прибор для печати протоколов, флеш-карта с исходными данными о бюллетенях, сканирующее устройство. Бюллетень должен опускаться лицевой стороной вниз, после чего сканирующее устройство проверяет номера печатей. На устройствах стоят номерные пломбы, которые невозможно снять без механических повреждений.

Наличие бумажных бюллетеней в урне КОИБ может способствовать облегчению наблюдения за выборами и выявлению возможных нарушений или ошибок программного обеспечения (в этом его преимущество перед КЭГ). Так, нормативы ЦИК предусматривают проведение ручного пересчета голосов на 5 % оборудованных КОИБ участков, выбираемых по жребию. При этом жеребьевка проводится вышестоящей комиссией в течение получаса после окончания времени голосования.

[51] Помимо уже прочно вошедших в практику электронного голосования УСГ и КОИБ в России были эксперименты и с другими способами голосования. В 2008 г. в г. Новомосковск Тульской области на выборах депутатов муниципального образования желающие могли проголосовать с помощью Интернета. Избирателям, выбравший данный способ голосования, на избирательном участке выдавался компакт-диск в пластиковой коробке, опечатанной специальным стикером.



Рис.17.44. Логотип диска для Интернет-голосования в Новомосковске

Компакт-диск для электронного опроса (ДЭО) имел защиту от повторного использования и мог быть применен только однократно. Интернет-голосование можно было сделать в специально оборудованных компьютерных классах или из любого другого места, чем воспользовалось 9% принявших участие в эксперименте. В следующей таблице приведены результаты Интернет-голосования.

Таблица 17.11. Результаты Интернет-голосования в г. Новомосковск

	Окружная комиссия № 3	Избирательные участки				
		№ 550	№ 551	№ 552	№ 553	№ 554
Число ДЭО, полученных для проведения эксперимента	5000	1000	1000	1000	1000	1000
Число ДЭО, выданных участникам эксперимента	3126	660	730	612	504	620
Число отправленных опросных листов	2978	630	630	586	475	593

Голосование с помощью ДЭО в сравнении с традиционным «бумажным» имеет немного плюсов – быстрая скорость обработки результатов голосования и исключение некоторых видов махинаций со стороны членов избирательных комиссий. К недостаткам можно отнести следующие:

- необходимость прихода голосующих на избирательный участок;
- большие затраты времени во время голосования для избирателя по сравнению с бумажным бюллетенем (для подготовленного пользователя в 5-10 раз);
- высокая стоимость ДЭО по сравнению с бумажным бюллетенем (в несколько раз);
- низкая надежность ДЭО как носителя информации;

- быстрое устаревание ДЭО, как и любого другого переносного компьютерного носителя.

В 2009 г. во Владимирской, Волгоградской, Вологодской, Томской областях и Ханты-Мансийском автономном округе – Югре наряду с ДЭО было опробовано голосование с использованием **мобильной связи** стандарта GSM-900/1800 и **электронных социальных карт**.

При голосовании по телефону участника опроса должен был зарегистрироваться у оператора мобильной связи (в ходе регистрации использовался номер телефона). Оператор вносил запись об участнике опроса в базу данных регистрации. Персональные данные участника опроса не использовались. Ему присваивался уникальный идентификатор, который был заложен в специальное программное обеспечение (СПО), загружаемое в мобильный телефон участника опроса. Этот же идентификатор использовался затем при информационном обмене в процессе электронного опроса, который защищался криптографическими средствами. С целью обеспечения анонимности волеизъявления до сервера подсчета голосов информация от избирателя проходила сервер деперсонализации, на котором определялась однократность голосования. Граждане, желающие опробовать новый способ голосования, могли также воспользоваться «общественными» телефонами избирательных комиссий, на которых было установлено многопользовательское СПО. Перед процедурой голосования по «общественному» телефону необходимо было ввести заранее сгенерированный оператором одноразовый PIN-код. Результаты голосования по одному из округов представлены в следующей таблице.

Таблица 17.12. Сравнительные данные итогов голосования и электронного опроса избирателей на выборах депутатов Законодательного Собрания Владимирской области пятого созыва по одномандатному избирательному округу

	Избирательные участки			
	№ 496	№ 498	№ 499	№ 501
Число избирателей по списку	2302	2535	2275	2778
Число проголосовавших бюллетенями	996	959	889	1077
Число проголосовавших по мобильному телефону	367	377	308	444

В г. Нижнеурт Ханты-Мансийского автономного округа желающие могли проголосовать через информационные киоски с помощью электронных социально-платежных карт «Югра». Как и в предыдущем случае, информация от избирателя вначале проходила через сервер деперсонализации с целью обеспечения анонимности и проверки целостности (с помощью ЭЦП). Результаты голосования по одному из округов представлены в следующей таблице.

Таблица 17.13. Сравнительные данные итогов голосования и электронного опроса избирателей на выборах главы муниципального образования г. Нижнеурт

	Избирательные участки		
	№ 564	№ 565	№ 566
Число избирателей по списку	2339	1173 ?	2074
Число проголосовавших бюллетенями	1183	922	1017
Число проголосовавших по ЭСК «Югра»	888	785	773

Вопросы для самопроверки

1. Назовите достоинства и недостатки традиционного («бумажного») голосования.
2. Что понимается под электронным голосованием?
3. Назовите основные свойства идеального протокола голосования (по Б. Шнайеру).
4. В чем отличие УСГ от КОИБ?

18.1. Тайные многосторонние вычисления [8]

Суть протокола заключается в определении результата некоторых преобразований над информацией, которой владеют несколько людей (субъектов). При этом они не хотят раскрывать ее для других.

Пример протокола.

Задача – определение средней заработной платы трех сотрудников: Директора (Д), Секретаря (С) и Уборщицы (У).

Заработная плата, которую сотрудники не хотят раскрывать друг другу:

- Директор – 10 у.е.;
- Секретарь – 5 у.е.;
- Уборщица – 2 у.е.

Пары ключей асимметричного шифрования (RSA) для обмена информацией между собой:

- Директор: открытый ключ – $e_d = 5$ и $n_d = 91$; закрытый ключ - $d_d = 29$;
- Секретарь: открытый ключ – $e_c = 7$ и $n_c = 91$; закрытый ключ - $d_c = 31$;
- Уборщица: открытый ключ – $e_y = 17$ и $n_y = 91$; закрытый ключ - $d_y = 17$.

В рассмотренном примере подбор ключей некорректен, т.к. выбор простых чисел для определения модуля должен выполняться каждым индивидуально. Данное упрощение принято в целях рассмотрения работы протокола.

Таблица 18.1. Протокол тайных многосторонних вычислений

№ п/п	Описание операции	Пример
1	У прибавляет случайное секретное число x к сумме своей зарплаты, шифрует результат с помощью открытого ключа С и отправляет его С.	$x = 3$ $(2 + 3)^7 \bmod 91 = 47$
2	С расшифровывает результат, добавляет к нему свою зарплату, шифрует результат с помощью открытого ключа Д и отправляет его Д.	$47^{31} \bmod 91 = 5$ $(5 + 5)^5 \bmod 91 = 82$
3	Д расшифровывает результат, добавляет к нему свою зарплату, шифрует результат с помощью открытого ключа У и отправляет его У.	$82^{29} \bmod 91 = 10$ $(10 + 10)^{17} \bmod 91 = 76$
4	У расшифровывает результат, отнимает x и объявляет среднюю зарплату.	$76^{17} \bmod 91 = 20$ $C3 = (20 - 3)/3 = 5.(6)$

В данной схеме поочередное шифрование/дешифрование необходимо для предотвращения вычисления мошенником информации, которой владеют участники протокола. Если пересылаемую информацию не шифровать, то мошенник, зная функцию преобразования и перехватив информацию, направленную одному из участников и высланную им следующему, может легко вычислить скрываемые исходные данные. Например, противник или недобросовестный участник протокола, перехватив информацию, высланную уборщицей секретарю (5) и секретарем директору (10), определит зарплату секретаря $10 - 5 = 5$ у.е. Шифрование предотвращает подобную атаку.

18.2. Протоколы разбиения и разделения секрета

18.2.1. Общие положения

Сущность данных протоколов заключается в том, что владелец секрета распределяет его части (доли) между несколькими людьми (субъектами). Каждая часть сама по себе ничего не значит и не дает информации о секрете. Для восстановления секрета требуется собрать все или определенное количество его долей. В первом случае говорят о **разбиении** (англ. *splitting*), а во втором о **разделении** (англ. *sharing*) секрета.

Второе отличие протоколов разбиения от протоколов разделения заключается в распределении долей. При разбиении разные доли передаются разным людям, при разделении – один человек может владеть сразу несколькими долями.

Примерами подобных ситуаций может быть сохранение в тайне до определенного момента рецепта изготовления продукта, сущности изобретения, кодов запуска баллистических ракет и т.п.

18.2.2. Разбиение секрета с использованием гаммирования

Простую и в то же время эффективную схему разбиения секрета можно построить на базе гаммирования по модулю 2. В этом случае секрет вначале кодируется в двоичном виде. Для его разбиения владелец генерирует несколько битовых строк (гамм), которые отдельно передает каждому из участников протокола. Кроме этого он складывает по модулю 2 битовое представление секрета со всеми гаммами и результат (шифrogramму) выкладывает в доступное для участников место. Для восстановления секрета необходимо сложить шифrogramму со всеми выданными гаммами, при чем не важно, в каком порядке.

В следующей таблице представлен пример разбиения секрета между тремя участниками.

Таблица 18.2. Протокол разбиения секрета на трех участников

--	--	--

№ п/п	Описание операции	Пример				
1	Кодирование секрета – слово «КОД».	Секрет	Буква	К	О	Д
			Вin-код	1100 1010	1100 1110	1100 0100
2	Генерация случайных гамм и передача их участникам.	Гамма ₁	Буква	Ю	Л	Я
			Вin-код	1101 1110	1100 1011	1101 1111
		Гамма ₂	Буква	Ш	А	Р
			Вin-код	1101 1000	1100 0000	1101 0000
		Гамма ₃	Буква	С	У	К
			Вin-код	1101 0001	1101 0011	1100 1010
3	Получение шифрограммы и выкладывание её в доступное для участников место.	Секрет	⊕	1100 1010	1100 1110	1100 0100
		Гамма ₁		1101 1110	1100 1011	1101 1111
		Гамма ₂		1101 1000	1100 0000	1101 0000
		Гамма ₃		1101 0001	1101 0011	1100 1010
4	Восстановление секрета.	Шифрограмма	Вin-код	0001 1101	0001 0110	0000 0001
		Шифрограмма Гамма ₂ Гамма ₁ Гамма ₃	⊕	0001 1101	0001 0110	0000 0001
				1101 1000	1100 0000	1101 0000
				1101 1110	1100 1011	1101 1111
				1101 0001	1101 0011	1100 1010
		Секрет	Вin-код	1100 1010	1100 1110	1100 0100
			Буква	К	О	Д

Примечание. Бинарное представление символов в соответствии с кодировкой Windows 1251.

Для восстановления секрета участники протокола, которым выданы гаммы, должны собраться вместе и в любой последовательности сложить свои гаммы с шифрограммой. В том случае, если гаммирование выполняется поочередно и обмен информации между участниками выполняется по открытым каналам связи (например, первый участник складывает шифрограмму со своей гаммой и отправляет результат второму, второй складывает полученный результат со своей гаммой и отправляет третьему и т.д.), то пересылаемую между ними информацию необходимо шифровать, как при тайных многосторонних вычислениях. В противном случае мошенник может определить гаммы участников протокола.

В общем случае, в основе протокола разбиения секрета лежит шифрование с разными ключами (например, как в рассмотренном примере или тройном DES) или последовательное применение разных методов шифрования (например, как в комбинированных шифрах).

18.2.3. Разделение секрета по схеме Шамира (интерполяционных полиномов Лагранжа)

В отличие от разбиения секрета участнику (субъекту) может передаваться сразу несколько равных долей и для восстановления секрета необязательно иметь все доли. Например, код запуска баллистической ракеты разбивается на пять долей, которые передаются трем полковникам (по одной доле) и одному генералу (две доли). Если для восстановления кода запуска (секрета) необходимо собрать три доли, то это могут сделать три полковника или генерал с одним полковником. Такая схема, где секрет делится на **n** долей, а для его восстановления необходимо собрать не менее чем **m** долей, где $m < n$, называется **(m, n)–пороговой схемой**.

В 1979 г. Ади Шамир (один из авторов RSA) предложил протокол разделения секрета с использованием полиномов (многочленов), максимальная степень которых равна $m-1$. Для восстановления секрета используются формулы интерполяционного полинома Лагранжа.

Интерполяционный полином Лагранжа.

Пусть имеется некоторая исходная функция $f(x)$, с помощью которой определены m точек – пар (x_i, y_i) . Тогда можно подобрать полином степени $m-1$, который будет проходить через все точки и максимально близко описывать исходную функцию.

Интерполяционный полином $L(x)$ определяется формулой

$$f(x) \approx L(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \dots + a_2x^2 + a_1x + a_0 = \sum_{i=0}^{m-1} y_i l_i(x), \quad (18.1)$$

где a_i - коэффициенты интерполяционного полинома Лагранжа;

y_i - значения исходной функции в i -ой точке;

$l_i(x)$ - базисные полиномы, определяемые по формуле

$$l_i(x) = \prod_{j=0, j \neq i}^{m-1} \frac{x - x_j}{x_i - x_j}, \quad (18.2)$$

где x_i, x_j - значения аргумента функции в i -ой и j -ой точках.

Пример подбора интерполяционного полинома Лагранжа.

Исходная функция $f(x) = \sin(x^2)$.

Точки исходной функции:

- $x_0 = -2, f(x_0) = -0.7568$;
- $x_1 = -1, f(x_1) = -0.8415$;
- $x_2 = 0, f(x_2) = 0$;
- $x_3 = 1, f(x_3) = 0.8415$;
- $x_4 = 2, f(x_4) = 0.7568$.

Определение базисных полиномов:

$$l_0(x) = \prod_{j=1}^4 \frac{x-x_j}{x_0-x_j} = \frac{x-x_1}{x_0-x_1} \cdot \frac{x-x_2}{x_0-x_2} \cdot \frac{x-x_3}{x_0-x_3} \cdot \frac{x-x_4}{x_0-x_4} = \frac{x+1}{-2+1} \cdot \frac{x-0}{-2-0} \cdot \frac{x-1}{-2-1} \cdot \frac{x-2}{-2-2} = \frac{x+1}{-1} \cdot \frac{x}{-2} \cdot \frac{x-1}{-3} \cdot \frac{x-2}{-4} = \frac{1}{24} \cdot (x^4 - 2x^3 - x^2 + 2x)$$

$$l_1(x) = \prod_{j=0, j \neq 1}^4 \frac{x-x_j}{x_1-x_j} = \frac{x-x_0}{x_1-x_0} \cdot \frac{x-x_2}{x_1-x_2} \cdot \frac{x-x_3}{x_1-x_3} \cdot \frac{x-x_4}{x_1-x_4} = \frac{x+2}{-1+2} \cdot \frac{x-0}{-1-0} \cdot \frac{x-1}{-1-1} \cdot \frac{x-2}{-1-2} = \frac{x+2}{1} \cdot \frac{x}{-1} \cdot \frac{x-1}{-2} \cdot \frac{x-2}{-3} = \frac{1}{-6} \cdot (x^4 - x^3 - 4x^2 + 4x)$$

$$l_2(x) = \prod_{j=0, j \neq 2}^4 \frac{x-x_j}{x_2-x_j} = \frac{x-x_0}{x_2-x_0} \cdot \frac{x-x_1}{x_2-x_1} \cdot \frac{x-x_3}{x_2-x_3} \cdot \frac{x-x_4}{x_2-x_4} = \frac{x+2}{0+2} \cdot \frac{x+1}{0+1} \cdot \frac{x-1}{0-1} \cdot \frac{x-2}{0-2} = \frac{x+2}{2} \cdot \frac{x+1}{1} \cdot \frac{x-1}{-1} \cdot \frac{x-2}{-2} = \frac{1}{-4} \cdot (x^4 - 5x^2 + 4)$$

$$l_3(x) = \prod_{j=0, j \neq 3}^4 \frac{x-x_j}{x_3-x_j} = \frac{x-x_0}{x_3-x_0} \cdot \frac{x-x_1}{x_3-x_1} \cdot \frac{x-x_2}{x_3-x_2} \cdot \frac{x-x_4}{x_3-x_4} = \frac{x+2}{1+2} \cdot \frac{x+1}{1+1} \cdot \frac{x-0}{1-0} \cdot \frac{x-2}{1-2} = \frac{x+2}{3} \cdot \frac{x+1}{2} \cdot \frac{x}{1} \cdot \frac{x-2}{-1} = \frac{1}{-6} \cdot (x^4 + x^3 - 4x^2 - 4x)$$

$$l_4(x) = \prod_{j=0}^3 \frac{x-x_j}{x_4-x_j} = \frac{x-x_0}{x_4-x_0} \cdot \frac{x-x_1}{x_4-x_1} \cdot \frac{x-x_2}{x_4-x_2} \cdot \frac{x-x_3}{x_4-x_3} = \frac{x+2}{2+2} \cdot \frac{x+1}{2+1} \cdot \frac{x-0}{2-0} \cdot \frac{x-1}{2-1} = \frac{x+2}{4} \cdot \frac{x+1}{3} \cdot \frac{x}{2} \cdot \frac{x-1}{1} = \frac{1}{24} \cdot (x^4 + 2x^3 - x^2 - 2x)$$

Определение интерполяционного полинома Лагранжа:

$$L(x) = \sum_{i=0}^{m-1} y_i l_i(x) = \frac{y_0}{24} \cdot (x^4 - 2x^3 - x^2 + 2x) + \frac{y_1}{-6} \cdot (x^4 - x^3 - 4x^2 + 4x) + \frac{y_2}{-4} \cdot (x^4 - 5x^2 + 4) + \frac{y_3}{-6} \cdot (x^4 + x^3 - 4x^2 - 4x) + \frac{y_4}{24} \cdot (x^4 + 2x^3 - x^2 - 2x) =$$

$$\frac{-0.7568}{24} \cdot (x^4 - 2x^3 - x^2 + 2x) + \frac{0.8415}{-6} \cdot (x^4 - x^3 - 4x^2 + 4x) + \frac{0}{-4} \cdot (x^4 - 5x^2 + 4) + \frac{0.8415}{-6} \cdot (x^4 + x^3 - 4x^2 - 4x) + \frac{-0.7568}{24} \cdot (x^4 + 2x^3 - x^2 - 2x) = -0.3436x^4 + 1.1851x^2$$

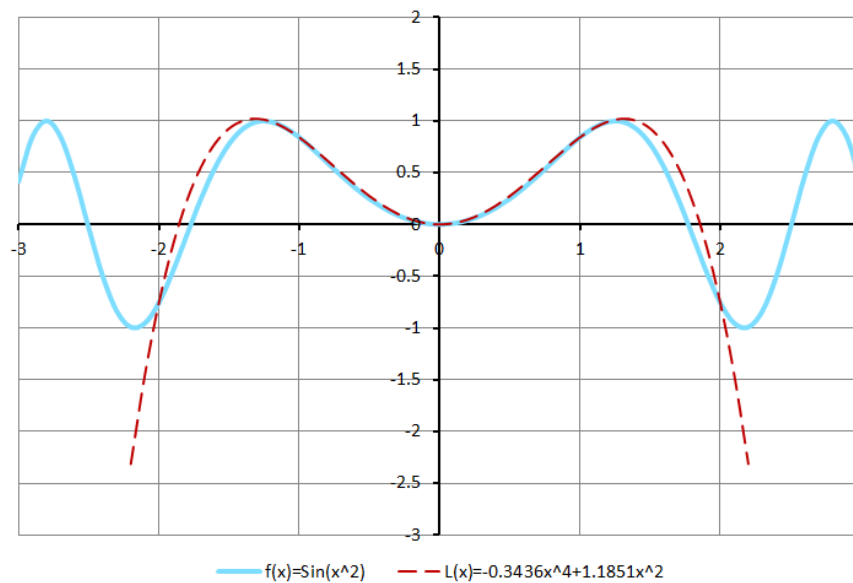


Рис.18.1. Графики исходной функции и интерполяционного полинома

Как видно на рисунке, интерполяционный полином довольно хорошо аппроксимирует исходную функцию в диапазоне $x \in [-2; 2]$.

Протокол разделения секрета на основе интерполяционных полиномов Лагранжа.

Для разделения секрета S , восстанавливаемого с помощью m долей, используется полином степени $m-1$ по модулю p

$$f(x) = L(x) = (a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \dots + a_2x^2 + a_1x + S) \bmod p, \quad (18.3)$$

где $f(x) = L(x)$ - исходная функция и интерполяционный полином Лагранжа;

a_i - целочисленные коэффициенты полинома;

$S = a_0$ - разделяемый секрет, закодированный в виде числа;

p - простое число.

Коэффициенты полинома a_i выбираются произвольно, за исключением $a_0 = S$. Модуль p должен быть простым числом, большим секрета S и общего количества долей p . Владелец секрета для $x_i = 1..n$ определяет значения полинома $y_i = f(x_i)$ и передает пары (x_i, y_i) участникам согласно определенному для каждого количеству долей. Для восстановления секрета необходимо собрать m долей (пар (x_i, y_i)) и найти значения коэффициентов интерполяционного полинома, включая секрет $S = a_0$.

Т.к. исходная функция и интерполяционный полином выражаются одинаковой формулой, то определенные по известным точкам (долям) коэффициенты интерполяционного полинома совпадут с коэффициентами исходной функции.

Пример протокола.

Секрет $S = 11$.

Количество долей, необходимых для восстановления секрета, $m = 3$.

Общее количество долей $n = 5$.

Таблица 18.3. Процедура определения и распределения долей (выполняет владелец)

№ п/п	Описание операции	Пример
-------	-------------------	--------

1	Выбор простого числа p , которое больше количества долей n и секрета S .	$p = 59$
2	Выбор произвольного многочлена степени m-1 : $f(x) = (a_2x^2 + a_1x + S) \bmod p$, где значения a₂ и a₁ выбираются случайным образом, хранятся в тайне и отбрасываются после распределения долей.	$a_2 = 10, a_1 = 23$ $f(x) = (10x^2 + 23x + 11) \bmod 59$
3	Определение долей (x_i , y_i), где $y_i = f(x_i)$ и $x_i = i + 1$.	$y_0 = (10 \cdot 1^2 + 23 \cdot 1 + 11) \bmod 59 = 44$ $y_1 = (10 \cdot 2^2 + 23 \cdot 2 + 11) \bmod 59 = 38$ $y_2 = (10 \cdot 3^2 + 23 \cdot 3 + 11) \bmod 59 = 52$ $y_3 = (10 \cdot 4^2 + 23 \cdot 4 + 11) \bmod 59 = 27$ $y_4 = (10 \cdot 5^2 + 23 \cdot 5 + 11) \bmod 59 = 22$
4	Публикация p и распределение долей (x_i , y_i) между участниками.	$p = 59$ $(x_0, y_0) = (1, 44)$ $(x_1, y_1) = (2, 38)$ $(x_2, y_2) = (3, 52)$ $(x_3, y_3) = (4, 27)$ $(x_4, y_4) = (5, 22)$

Таблица 18.4. Процедура восстановления секрета
(выполняют участники)

№ п/п	Описание операции	Пример
1	Сбор m долей.	$(x_1, y_1) = (2, 38)$ $(x_2, y_2) = (3, 52)$ $(x_4, y_4) = (5, 22)$
2	Определение базисных полиномов.	$l_1(x) = \frac{x-3}{2-3} \cdot \frac{x-5}{2-5} = \frac{x-3}{-1} \cdot \frac{x-5}{-3} = \frac{1}{3} \cdot (x^2 - 8x + 15)$ $l_2(x) = \frac{x-2}{3-2} \cdot \frac{x-5}{3-5} = \frac{x-2}{1} \cdot \frac{x-5}{-2} = \frac{1}{-2} \cdot (x^2 - 7x + 10)$ $l_4(x) = \frac{x-2}{5-2} \cdot \frac{x-3}{5-3} = \frac{x-2}{3} \cdot \frac{x-3}{2} = \frac{1}{6} \cdot (x^2 - 5x + 6)$
3	Определение интерполяционного полинома Лагранжа.	$L(x) = \left[\frac{38}{3} \cdot (x^2 - 8x + 15) + \frac{52}{-2} \cdot (x^2 - 7x + 10) + \frac{22}{6} \cdot (x^2 - 5x + 6) \right] \bmod 59$ $L(x) = \left[\frac{76}{6} \cdot (x^2 - 8x + 15) - \frac{156}{6} \cdot (x^2 - 7x + 10) + \frac{22}{6} \cdot (x^2 - 5x + 6) \right] \bmod 59$ $L(x) = \left[\frac{1}{6} \cdot (-58x^2 + 374x - 288) \right] \bmod 59$
4	Определение обратного числа по модулю b⁻¹ для дробного множителя полинома 1 / b .	$\frac{1}{b} = \frac{1}{6}$ $b^{-1} = 10 [(6 \cdot 10) \bmod 59 = 1]$
5	Замена дробного множителя 1 / b и умножение коэффициентов полинома на множитель b⁻¹ .	$L(x) = [10 \cdot (-58x^2 + 374x - 288)] \bmod 59 = (-580x^2 + 3740x - 2880) \bmod 59$
6	Приведение коэффициентов полинома и определение секрета S .	$a_2 = -580 \bmod 59 = -49 \bmod 59 = 10$ $a_1 = 3740 \bmod 59 = 23$ $S = a_0 = -2880 \bmod 59 = -48 \bmod 59 = 11$ $L(x) = (10x^2 + 23x + 11) \bmod 59$

Примечание. Обратное число по модулю определяется из выражения $(b \cdot b^{-1}) \bmod p = 1$ (например, с помощью расширенного алгоритма Евклида).

Как отмечает Брюс Шнайер применительно к пороговой схеме (6, n):

Наиболее впечатляющим моментом совместного использования секрета является то, что, если коэффициенты выбраны случайным образом, пять человек даже при помощи бесконечных вычислительных мощностей не смогут узнать ничего, кроме длины сообщения (которая и так им известна). Это также безопасно, как одноразовый блокнот. Попытка выполнить исчерпывающий поиск (т.е., перебор всех возможных шести коэффициентов) покажет, что любое возможное сообщение останется секретным.

Брюс Шнайер. «Практическая криптография»

18.2.4. Разделение секрета по схеме Асмута-Блума [8, 17]

В (m, n)-пороговой схеме Асмута-Блума для распределения долей используются простые¹ и взаимно простые числа², а для восстановления - китайская теорема об остатках.

Схема и пример протокола.

Секрет $S = 11$.

Количество долей, необходимых для восстановления секрета, $m = 3$.

Общее количество долей $n = 5$.

Таблица 18.5. Процедура определения и распределения долей
(выполняет владелец)

№ п/п	Описание операции	Пример
1	Выбор простого числа p , которое больше секрета S .	$p = 13$
2	Выбор n взаимно простых чисел d_i , удовлетворяющих условиям: - $d_i > p$; - $d_i < d_{i+1}$; - $d_1 \cdot d_2 \cdot \dots \cdot d_m < p \cdot d_{n-m+2} \cdot d_{n-m+3} \cdot \dots \cdot d_n$.	$d_i \in \{17, 20, 23, 29, 37\}$ $17 \cdot 20 \cdot 23 < 13 \cdot 29 \cdot 37$ $7820 < 13949$

3	Выбор произвольного числа r , удовлетворяющего условию $r < \frac{\prod_{i=1}^m d_i - S}{p}$. Вычисление $S' = S + r p$.	$r = 30$ $\left[30 < 600.7 = \frac{17 \cdot 20 \cdot 23 - 11}{13} \right]$ $S' = 11 + 30 \cdot 13 = 401$
4	Определение долей (d_i, k_i) , где $k_i = S' \bmod d_i$.	$k_1 = 401 \bmod 17 = 10$ $k_2 = 401 \bmod 20 = 1$ $k_3 = 401 \bmod 23 = 10$ $k_4 = 401 \bmod 29 = 24$ $k_5 = 401 \bmod 37 = 31$
5	Публикация p и распределение долей (d_i, k_i) между участниками.	$p = 13$ $(d_1, k_1) = (17, 10)$ $(d_2, k_2) = (20, 1)$ $(d_3, k_3) = (23, 10)$ $(d_4, k_4) = (29, 24)$ $(d_5, k_5) = (37, 31)$

Сущность **китайской теоремы об остатках** заключается в определении некоторого числа S' по набору его остатков k_i от деления на некоторые заданные взаимно простые числа d_i .

$$\begin{cases} S' \bmod d_1 = k_1 \\ S' \bmod d_2 = k_2 \\ \dots \\ S' \bmod d_m = k_m \end{cases} \quad (18.4)$$

Например, для трех пар $(d_i, k_i) - (3, 1), (5, 3)$ и $(8, 3)$ – таким числом является $S' = 43$.

$$\begin{cases} 43 \bmod 3 = 1 \\ 43 \bmod 5 = 3 \\ 43 \bmod 8 = 3 \end{cases}$$

В следующей таблице, наряду с процедурой восстановления секрета, приведен алгоритм определения числа S' (китайской теоремы об остатках) в пп. 2-5.

Таблица 18.6. Процедура восстановления секрета
(выполняют участники)

№ п/п	Описание операции	Пример
1	Сбор m долей.	$(d_2, k_2) = (20, 1)$ $(d_3, k_3) = (23, 10)$ $(d_5, k_5) = (37, 31)$
2	Вычисление произведения D взаимно простых чисел d_j .	$D = 20 \cdot 23 \cdot 37 = 17020$
3	Вычисление сомножителей $D_j = D / d_j$.	$D_1 = 17020 / 20 = 851$ $D_2 = 17020 / 23 = 740$ $D_3 = 17020 / 37 = 460$
4	Определение обратных чисел D_j^{-1} по модулям d_j .	$D_1^{-1} = 11 [(851 \cdot 11) \bmod 20 = 1]$ $D_2^{-1} = 6 [(740 \cdot 6) \bmod 23 = 1]$ $D_3^{-1} = 7 [(460 \cdot 7) \bmod 37 = 1]$
5	Вычисление $S' = (\sum k_j D_j D_j^{-1}) \bmod D$.	$S' = (1 \cdot 851 \cdot 11 + 10 \cdot 740 \cdot 6 + 31 \cdot 460 \cdot 7) \bmod 17020 = 153581 \bmod 17020 = 401$
6	Определение секрета $S = S' \bmod p$.	$S = 401 \bmod 13 = 11$

Примечание. Обратное число по модулю определяется из выражения $(b \cdot b^{-1}) \bmod p = 1$ (например, с помощью расширенного алгоритма Евклида).

¹**Простое число** – натуральное число, большее единицы и не имеющее других натуральных делителей, кроме самого себя и единицы.

²**Взаимно простые числа** – числа, не имеющие общих делителей, кроме 1, т.е. наибольший общий делитель которых равен 1.

18.2.5. Другие разновидности схем разделения секрета [8]

- Кроме классической пороговой схемы разделения секрета (владелец раздает доли и при восстановлении участники раскрывают свои доли) существуют и другие схемы.
- Разделение секрета без владельца.** Участники могут создать секрет и разделить его на доли так, что никто из них не узнает секрета, пока они совместно его не восстановят.
 - Разделение секрета без раскрытия долей при восстановлении.** В этом смысле протокол представляет собой нечто среднее между разделением секрета и тайными многосторонними вычислениями.
 - Разделение секрета с возможностью проверки корректности отдельных долей.** Каждый из участников независимо от других может проверить корректность своей доли без восстановления секрета.
 - Разделение секрета с возможностью блокирования восстановления секрета.** Каждый из участников получает две доли: «да» и «нет». Если при восстановлении секрета число долей «нет» превышает некоторое пороговое значение, то его восстановление невозможно, даже, если количества долей «да» достаточно.
 - Разделение секрета с возможностью блокирования долей.** Если после распределения долей, некоторые из участников теряют доверие, то можно заблокировать их доли.
 - Разделение секрета с возможностью выявления фальшивых долей.** При восстановлении секрета возможно выявление участников, предоставивших фальшивые доли.
 - Групповое разделение секрета.** Секрет распределяется среди участников, объединенных в k групп. Для восстановления секрета необходимо собрать в каждой группе

определенное количество долей. Т.е. имеет место $((m_1, n_1), (m_2, n_2), \dots, (m_k, n_k))$ -пороговая схема.

Вопросы для самопроверки

1. Для чего необходимо применение шифрования с открытым ключом в тайных многосторонних вычислениях?
2. Что означает (m, n) -пороговая схема разделения секрета.
3. Назначение интерполяционного полинома Лагранжа.
4. Сущность китайской теоремы об остатках.

19.1. Сложность алгоритмов

Сложность алгоритма определяется вычислительными мощностями, необходимыми для его исполнения. Вычислительную сложность алгоритма часто определяют двумя параметрами [8]:

- **временная сложность T** (в худшем, среднем или наилучшем случае) – функция размера входных и выходных данных, равная количеству (максимальному, среднему или минимальному) элементарных операций, выполняемых алгоритмом для решения экземпляра задачи указанного размера;
- **пространственная сложность S** - требования к памяти для решения экземпляра задачи.

Вычислительную сложность алгоритма обычно выражают через символ «**O** большое», указывающей порядок величины вычислительной сложности. Он является членом разложения функции сложности, быстрее всех растущий с ростом n ; все члены низшего порядка игнорируются. Например, если временная сложность алгоритма равна $4n^2 + 7n + 12$, его вычислительная сложность порядка n^2 – выражается как $O(n^2)$.

Оценка вычислительной сложности наглядно показывает, как объем входных данных влияет на требования к времени и объему памяти. Например, если $T = O(n)$, удвоение входных данных удвоит и время исполнения алгоритма. Если $T = O(2^n)$, добавление всего одного бита к входным данным удвоит время исполнения алгоритма.

Классификация алгоритмов в соответствии с их временной сложностью:

- постоянные $O(1)$ – сложность не зависит от n ;
- логарифмические $O(\log n)$ – сложность возрастает с ростом n , но незначительно. Обычно присуще задачам, решаемым в несколько этапов. При этом при переходе от одного этапа к другому размер данных последовательно уменьшается;
- линейные $O(n)$ – сложность возрастает линейно;
- полиномиальные $O(n^c)$, где c – константа;
- субэкспоненциальные $O(c^{n^\epsilon})$, где c – константа ($c > 1$), ϵ – константа ($0 < \epsilon < 1$);
- экспоненциальные $O(c^{f(n)})$, где c – константа ($c > 1$), $f(n)$ – некоторая полиномиальная функция от n ;
- суперполиномиальные – подмножество экспоненциальных алгоритмов, у которых $f(n)$ возрастает медленнее линейной зависимости.

19.2. Простые числа

Простое число – натуральное (целое положительное) число, большее единицы и не имеющее других натуральных делителей, кроме самого себя и единицы. Множество натуральных чисел обозначается $\mathbb{N}$.

Основная теорема арифметики – любое натуральное число n , большее единицы, представимо в виде произведения простых чисел, причём единственным способом с точностью до порядка следования сомножителей.

$$n = p_1^{e_1} * p_2^{e_2} * \dots * p_k^{e_k}, \quad (19.1)$$

где $p_1, p_2, \dots, p_k$ – простые сомножители, $1 < p_1 < p_2 < \dots < p_k$;
 $e_1, e_2, \dots, e_k$ – количество (степени) простых сомножителей.

Например, $n = 600 = 2^3 * 3^1 * 5^2$.

В «Началах» Евклида теорема не встречается, однако в VII книге появляются предложения, которые ей эквивалентны. Первая точная формулировка и доказательство приводятся в книге немецкого математика Иоганна Карла Фридриха Гаусса «Арифметические исследования», изданной в 1801 г.

Теорема Евклида – простых чисел бесконечно много. Простое и элегантное доказательство теоремы было приведено в IX книге «Начал» [52].

Возьмем ряд последовательных простых чисел (например, $\{2, 3, 5\}$) и перемножим их:

$$2 * 3 * 5 = 30. \quad (19.2)$$

Добавим к результату единицу:

$$2 * 3 * 5 + 1 = 30 + 1 = 31. \quad (19.3)$$

Если разделить 31 на любое простое число из этого ряда (2, 3 или 5), то в остатке получится 1:

$$31 \bmod 2 = 1,$$

$$31 \bmod 3 = 1, \quad (19.4)$$

$$31 \bmod 5 = 1.$$

Это означает, что число 31 не делится на числа ряда. Такие рассуждения справедливы и в общем случае: если взять ряд последовательных простых чисел, перемножить их и добавить единицу, то полученное число не будет делиться ни на одно из исходных простых чисел. Число 31 тоже простое число, но его нет в первоначальном списке, который, следовательно, является неполным.

Возьмем следующий ряд чисел в качестве примера - $\{2, 3, 5, 7, 11, 13\}$, перемножим их и добавим единицу:

2 * 3 * 5 * 7 * 11 * 13 + 1 = 30 030 + 1 = 30 031. (19.5)

Результат не является простым числом, так как может быть разложен в произведение двух других чисел:

30 031 = 59 * 509. (19.6)

Согласно основной теоремы арифметики любое натуральное число может быть единственным образом разложено в произведение простых множителей. В случае с числом 30 031, которое является составным числом, ясно, что для его разложения в произведение простых множителей чисел в списке {2, 3, 5, 7, 11, 13} будет недостаточно, т.е. этот список неполон.

Следствием теоремы Евклида является утверждение: каким бы ни был первоначальный ряд простых чисел, при их перемножении и добавлении единицы получается новое число одного из двух типов:

- 1. простое число, которого нет в списке;
- 2. составное число, при разложении которого на простые множители получаются простые числа, не входящие в список.

Таким образом, первоначальный ряд простых чисел всегда является неполным, если он не является бесконечно длинным.

На текущий момент в открытом доступе отсутствуют сведения о найденной формуле или полиномиальном алгоритме (далее, правиле), позволяющем определять появление простых чисел в последовательности натуральных. Суть правила - по заданному номеру простого числа определить значение этого числа. Исследователи, занимающиеся этой проблемой, предложили ряд формул частного характера. Наиболее известными из них являются:

- числа Мерсена: $2^p - 1$, где p – простое число. В 1947 г. был получен полный список p: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 и 127;
- числа Ферма: $2^{2^n} + 1$, где $0 \leq n \leq 4$.

Гаусс подошел к проблеме распределения простых чисел с другой стороны. Он ввел функцию $\pi(x)$ – количество простых чисел, меньших, чем x. Для первых десяти миллиардов зависимость π выглядит следующим образом.

Таблица 19.1. Распределение простых чисел

x	$\pi(x)$
10	4
100	25
1 000	168
10 000	1 229
100 000	9 592
1 000 000	78 498
10 000 000	664 579
100 000 000	5 761 455
1 000 000 000	50 847 534
10 000 000 000	455 052 511

По результатам своих исследований Гаусс выдвинул гипотезу

$\pi(x) \approx \frac{x}{\ln x}$, при $x \rightarrow \infty$. (19.7)

Данная гипотеза была доказана в 1896 г. независимо друг от друга французскими математиками Жаком Адамаром и Шарлем Жаном де ля Валле-Пуссенон и получила наименование «теорема о распределении простых чисел».

Немецкий математик Бернхард Риман исследовал теорему о распределении простых чисел с помощью дзета-функции Римана $\zeta(x)$ и выдвинул гипотезу:

«Все нетривиальные нули дзета-функции имеют действительную часть, равную 1/2».

Данная гипотеза относится к одной из семи проблем тысячелетия, за решение каждой из которых Математический институт Клэя (Clay Mathematics Institute, Кембридж, Массачусетс) выплатит награду в один миллион долларов США. Если быть точным, то их осталось шесть, т.к. доказательство гипотезы Пуанкаре (сейчас уже теоремы) было найдено в 2002 г. Григорием Перельманом.

Если гипотеза Римана верна, то все простые числа распределены регулярно (или почти регулярно), что означает существование правила их определения в числовой последовательности.

Особый класс простых чисел **p** составляют т.н. «простые числа-близнецы», среди которых можно выделить следующие разновидности [17, 52].

Таблица 19.2. Разновидности простых чисел-близнецов

Формула	Наименование	Примеры	Особенности
(p, p + 1)		(2, 3)	Единственная пара простых чисел-близнецов этого вида, т.к. четные и нечетные числа чередуются между собой, а 2 является единственным простым четным числом.
(p, p + 2)	простые парные числа-близнецы	(3, 5), (5, 7), (11, 13), (71, 73)	Все пары близнецов, кроме первых двух, имеют вид (30n + 11, 30n + 13), (30n + 17, 30n + 19) или (30n + 29, 30n + 31), где n ≥ 0. Существует гипотеза, что парных простых чисел-близнецов бесконечное множество. Наибольшая известная пара на 2011 г. – 3 756 801 695 685 * 2 ⁶⁶⁶⁶⁶⁹ ± 1.
(p, p + 2, p + 4)	простые числа-триплеты	(3, 5, 7)	Единственная тройка простых чисел-близнецов этого вида.
(p, p + 2, p + 6)		(5, 7, 11), (41, 43, 47)	
(p, p + 4, p + 6)		(7, 11, 13), (67, 71, 73)	
(p, p + 2, p + 6, p + 8)	простые числа-квадруплеты	(5, 7, 11, 13), (11, 13, 17, 19),	Все квадруплеты, кроме первого, по модулю 30 имеют вид (11, 13, 17, 19).

		(101, 103, 107, 109)	
(p, p + 4, p + 6, p + 10, p + 12, p + 16)	простые числа-секступлеты	(7, 11, 13, 17, 19, 23), (97, 101, 103, 107, 109, 113), (16057, 16061, 16063, 16067, 16069, 16073)	Все секступлеты, кроме первого, по модулю 210 имеют вид (97, 101, 103, 107, 109, 113).

По мере возрастания последовательности натуральных чисел, простые числа в ней появляются все реже, что следует из гипотезы Гаусса (19.7). Промежутки между простыми числами могут быть любой протяженности, что легко доказуемо.

Рассмотрим последовательность из первых четырех натуральных чисел (1, 2, 3, 4) и числа, сгенерированные на их основе:

$$1 * 2 * 3 * 4 + 2 = 2 * (1 * 3 * 4 + 1) = 26,$$

$$1 * 2 * 3 * 4 + 3 = 3 * (1 * 2 * 4 + 1) = 27, \quad (19.8)$$

$$1 * 2 * 3 * 4 + 4 = 4 * (1 * 2 * 3 + 1) = 28.$$

Из (19.8) видно, что сгенерированные числа составные и каждое из них делится на одно из чисел взятой последовательности. Таким образом, если требуется получить тысячу последовательно расположенных составных чисел, то можно воспользоваться последовательностью чисел 1001! + 2, 1001! + 3, ..., 1001! + 1001.

Основные задачи, связанные с использованием простых чисел в криптографии.

1. Разложение числа **n** на простые сомножители.
2. Нахождение начального списка простых чисел вплоть до некоторого значения **n**.
3. Тестирование числа **n** на простоту.
4. Определение наибольшего общего делителя (НОД) двух чисел **n** и **m** (определение взаимной простоты чисел **n** и **m**).

19.3. Разложение числа на простые сомножители

Представление натурального числа в виде произведения простых называется **разложением числа на простые сомножители** или **факторизацией¹⁾ числа**. На настоящий момент неизвестны полиномиальные алгоритмы факторизации чисел, хотя и не доказано, что таких алгоритмов не существует. На предполагаемой большой вычислительной сложности задачи факторизации базируется криптосистема RSA и некоторые другие. Факторизация с полиномиальной сложностью теоретически возможна на квантовом компьютере с помощью алгоритма Шора.

В зависимости от сложности алгоритмы факторизации можно разбить на две группы. Первая группа – **экспоненциальные алгоритмы**, сложность которых экспоненциально зависит от длины входящих параметров (т.е. от длины самого числа в бинарном представлении). Вторая группа – **субэкспоненциальные алгоритмы**.

А. Экспоненциальные алгоритмы:

- перебор возможных делителей;
- метод факторизации Ферма;
- р-алгоритм Полларда;
- и др.

Б. Субэкспоненциальные алгоритмы:

- алгоритм Диксона;
- метод непрерывных дробей (CFRAC);
- метод квадратичного решета;
- метод эллиптических кривых;
- общий метод решета числового поля (считается самым быстрым алгоритмом на текущий момент);
- и др.

Рассмотрим два простых экспоненциальных алгоритма.

Перебор делителей – алгоритм факторизации числа путем полного перебора всех возможных потенциальных делителей. Суть алгоритма заключается в переборе всех целых чисел **i** от 1 до $\sqrt{n}$ и вычислении остатка от деления **n** на **i** (**n mod i**). Если остаток от деления равен нулю, то **i** является делителем **n**.

Описание алгоритма с полным перебором.

```

1. i := 1
2. Если n mod i = 0
   то i и n/i добавить в список делителей числа n
3. i := i + 1
4. Если i >  $\sqrt{n}$ 
   то завершить работу
   иначе перейти к шагу 2

```

Приведенный алгоритм позволяет найти все делители (в т.ч. и составные). Более эффективная (по вычислительной сложности) реализация алгоритма перебора, позволяющая найти все простые сомножители, приведена ниже.

```
1. i := 2
2. Если n mod i = 0
    то
        2.1. Добавить i в список простых сомножителей
        2.2. n := n / i
        2.3. Перейти к шагу 2
3. Если i = 2
    то i := i + 1
    иначе i := i + 2
4. Если i > √n
    то добавить n в список простых сомножителей и завершить работу
    иначе перейти к шагу 2
```

Метод факторизации Ферма.

Суть метода состоит в том, чтобы попробовать представить нечетное число **n** в виде $n = x^2 - y^2$, где **x**, **y** - неотрицательные целые числа. Если такие числа найдены, то $n = x^2 - y^2 = (x - y)(x + y)$. Значит, $(x - y)$ и $(x + y)$ являются делителями (не обязательно простыми) числа **n**.

В дополнение к методу Ферма можно использовать следующее правило. Если $(n - 1) / 2$ - нечетное число, тогда **x** - четное, **y** - нечетное. И, наоборот, если $(n - 1) / 2$ - четное число, тогда **x** - нечетное, **y** - четное.

Описание алгоритма.

```
1. x:=⌈√n⌉, где ⌈√n⌉ - округление до ближайшего большего целого
2. Если x = 1
    то завершить работу (n - простое)
3. Если n = x^2
    то завершить работу (x является делителем числа n)
4. Если [(n - 1) / 2 - нечетное и x - нечетное] или [(n - 1) / 2 - четное и x - четное]
    то x := x + 1
5. Если x > (n + 1) / 4
    то завершить работу (n - простое)
    иначе y:=√x^2 - n
6. Если y - целое
    то завершить работу ((x + y) и (x - y) являются делителями числа n)
    иначе x := x + 2 и перейти к шагу 5
```

Например, $n = 1\,342\,127$, $(n - 1) / 2 = 671063$ – нечетное, $x_0 = \lceil \sqrt{n} \rceil = \lceil \sqrt{1\,342\,127} \rceil = \lceil 1158.5 \dots \rceil = 1159$.

Таблица 19.3. Таблица итераций (шаги 5 и 6)

№ итерации	x	$y := \sqrt{x^2 - n}$
1	1160	58.93...
2	1162	90.09...
3	1164	113

Тогда делителями $n = 1\,342\,127$ являются $(x + y) = (1164 + 113) = 1277$ и $(x - y) = (1164 - 113) = 1051$.

Как отмечалось выше, если в результате работы алгоритма получены делители, то они могут, в свою очередь, оказаться составными числами. Например, при $n = 105$ уже на первой итерации получаем $x = \lceil \sqrt{105} \rceil = \lceil 10.25 \dots \rceil = 11$, $y = \sqrt{11^2 - 105} = \sqrt{16} = 4$, $(x + y) = (11 + 4) = 15$ и $(x - y) = (11 - 4) = 7$. Очевидно, что число 15 - составное.

Т.о., чтобы найти все простые делители числа **n** необходимо использовать описанный выше алгоритм рекурсивно для каждого вновь найденного делителя. Если для него соблюдается условие шага 5, то он действительно является простым делителем числа **n**.

Для вскрытия шифрограммы, полученной с помощью алгоритма RSA, требуется найти два простых делителя числа $n = p * q$ (напомним, **n** – часть открытого ключа). Отсюда, достаточно единожды (без рекурсивных вызовов) применить метод Ферма и найти два делителя, чтобы вскрыть шифрограмму. Но, т.к. по рекомендациям Лаборатории RSA на сегодняшний день, длина числа **n** составляет 2048 битов ($n \approx 2 * 10^{600}$), использование метода Ферма неперспективно. Более того, если один из множителей относительно другого очень мал или **n** является простым числом, то алгоритм на базе метода Ферма вычислительно менее эффективен алгоритмов перебора делителей.

1) От лат. facite - делать или производить. Каждый делитель (множитель) «производит» исходное число.

19.4. Нахождение начального списка простых чисел

Простые способы нахождения начального списка простых чисел вплоть до некоторого значения n дают решето Эратосфена, решето Сундарамы и решето Аткина. Существуют и геометрические модели нахождения простых чисел.

Решето Эратосфена – алгоритм приписывают древнегреческому математику Эратосфену Киренскому (III век до н.э.).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

а) результат первой итерации

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

б) окончательный результат

Рис.19.1. Иллюстрация решета Эратосфена

Описание алгоритма.

1. Выписать подряд все целые числа от двух до n (2, 3, 4, ..., n).
2. Пусть переменная p изначально равна двум – первому простому числу.
3. Считая от p шагами по p , зачеркнуть в списке все числа от $2p$ до n кратные p (то есть числа $2p$, $3p$, $4p$, ...).
4. Найти первое незачеркнутое число, большее чем p , и присвоить значению переменной p это число.
5. Повторять шаги 3 и 4 до тех пор, пока p не станет больше, чем n .

Оставшиеся незачеркнутые числа – простые. Для отыскания списка простых чисел меньших числа n достаточно проверить делители от 2 до $\sqrt{n}$.

Решето Сундарамы – детерминированный алгоритм, разработанный индийским студентом С.П. Сундарамом в 1934 г.

Описание алгоритма.

1. Из ряда натуральных чисел от 1 до n исключаются все числа вида

$$i + j + 2ij,$$

где индексы $i \leq j$ пробегает все натуральные значения, для которых $i + j + 2ij \leq N$, а именно значения

$$i = 1, \left\lfloor \frac{\sqrt{2n+1}-1}{2} \right\rfloor \text{ и } j = i, \left\lfloor \frac{n-1}{2i+1} \right\rfloor.$$

2. Каждое из оставшихся чисел умножается на 2 и увеличивается на 1.

Полученная в результате последовательность представляет собой все нечётные простые числа в отрезке $[1, 2n + 1]$.

Геометрическое решето Ю. Матиясевича и Б. Стечкина – геометрический способ нахождения начального списка простых чисел.

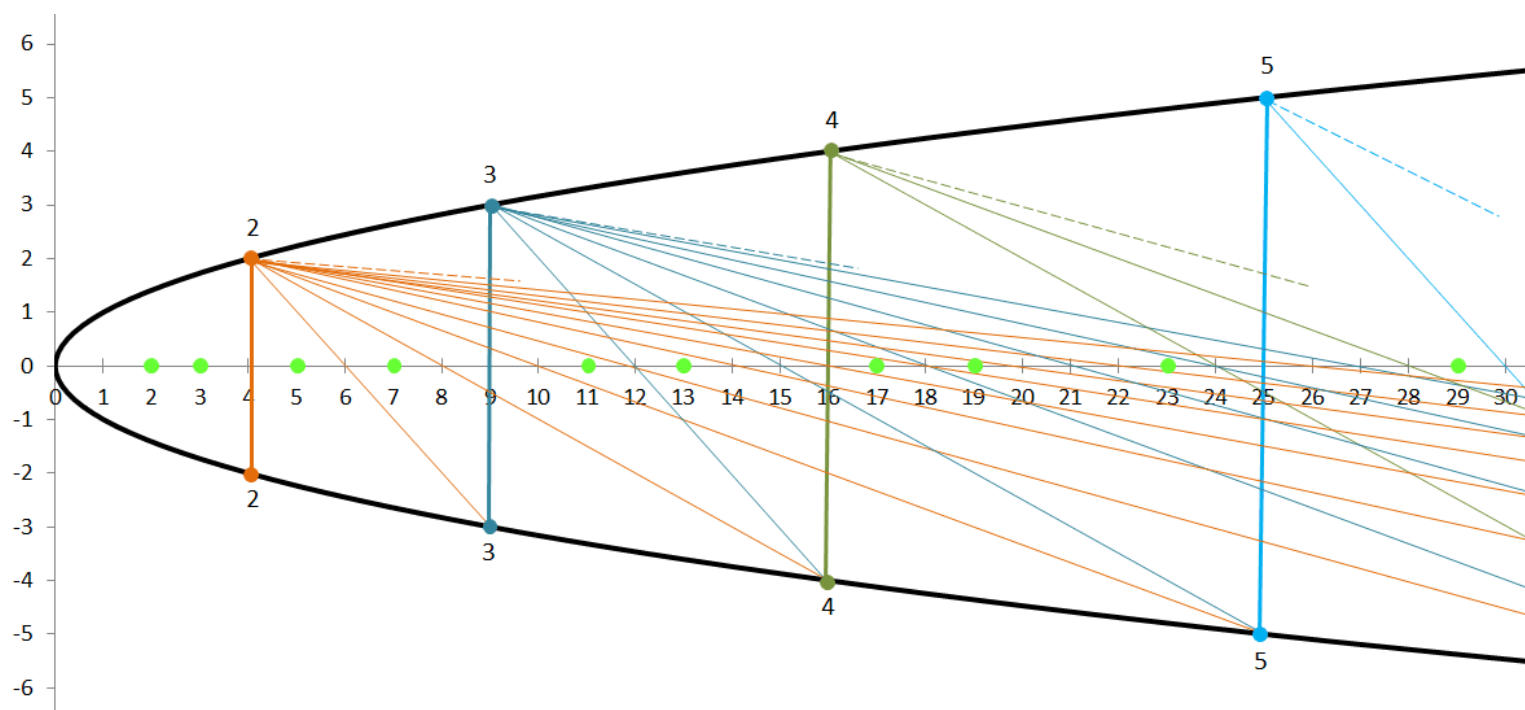


Рис.19.2. Геометрическое решето Матиясевича – Стечкина
(простые числа отмечены зелеными точками)

Описание алгоритма.

1. Строится парабола вдоль горизонтальной оси, на которой отмечена последовательность натуральных чисел от нуля до n ($0, 1, 2, 3, 4, \dots, n$).
2. Проводятся перпендикуляры к оси в точках, соответствующих квадратам натуральных чисел ($2^2 = 4, 3^2 = 9, 4^2 = 16, 5^2 = 25, \dots$). Квадраты чисел на оси представляются точками на параболе ($2, 3, 4, 5, \dots$).
3. Каждая точка верхней ветви параболы соединяется со всеми точками нижней ветви. Каждый из этих отрезков пересечет ось в точке, соответствующей произведению двух соединенных чисел (например, отрезок, соединяющий числа 2 и 3, пересекает ось в точке 6).

Натуральные числа (точки) на горизонтальной оси, через которые не проходит ни один из таких отрезков – простые (за исключением 0 и 1).

Другие наглядные (графические) способы определения простоты и делимости чисел можно посмотреть в статье "Графические этюды на тему простоты и делимости чисел".

19.5. Тестирование числа на простоту

Во многих асимметричных алгоритмах шифрования требуется применение простых чисел с длиной сотни, а иногда и тысячи бит. Генерация простого числа такой длины (за приемлемое время) является задачей нерешенной. Вместо этого поступают, как правило, следующим образом.

1. Генерируется битовая строка требуемой длины со случайным набором бит (0 или 1).
2. Первый и последний бит устанавливается равным 1.
3. Полученное число n тестируется на простоту.

При тестировании на простоту можно попытаться применить алгоритмы разложения числа n на множители и, если среди множителей только единица и само число, то сделать вывод, что число простое. Однако рассмотренные выше и известные на текущий момент алгоритмы разложения также неприемлемы по времени. Для проверки простоты числа существуют детерминированные и вероятностные тесты. Некоторые **детерминированные тесты простоты**:

- перебор возможных делителей;
- тест Миллера;
- тест простоты Люка;
- тест Агравала - Каяла – Саксены (самый быстрый);
- и др.

Перебор делителей – аналогичен алгоритму факторизации числа n . Выполняется перебор всех возможных потенциальных делителей от 2 до $\sqrt{n}$. При нахождении числа из этого диапазона, делящего n нацело, поиск прекращается, т.к. n - составное.

Тест Миллера [9, 10, 17].

Тест базируется на числах, называемых свидетелями простоты. Пусть n - нечётное число большее 1. Число $n - 1$ однозначно представляется в виде $n - 1 = 2^k * q$, где q нечётно (например, $n = 561$, тогда $n - 1 = 560 = 2^4 * 35$). Целое число b , называется свидетелем простоты числа n , если выполняется условие:

$$b \bmod n = 1, \quad (19.9)$$

или

$$\text{существует } s \ (0 \leq s < k) \text{ такое, что } b^{2^s q} \bmod n = n - 1. \quad (19.10)$$

По гипотезе Римана, если n – составное число, тогда найдется $b < 2 \ln^2 n^2$, которое не будет являться свидетелем простоты. Проверка одного основания b не дает стопроцентной гарантии простоты n . Например, тест для числа $n = 2047 = 23 * 89$ по основанию $b = 2$ будет говорить о том, что n – простое. Для стопроцентной уверенности необходимо проверить все свидетели простоты от 2 до $2 \ln^2 n$. Для числа $n = 60000$ число проверяемых свидетелей простоты примерно равно числу проверяемых делителей по процедуре с полным перебором от 2 до $\sqrt{n}$ (≈ 240). Учитывая простоту теста с перебором делителей, он более эффективен с вычислительной точки зрения, чем тест Миллера. Однако при $n = 10^9 + 1$ (1110111001 1010110010 1000000001)₂, при полном переборе делителей необходимо проверить ≈ 31600 делителей, а по тесту Миллера ≈ 860 . Сравните n с рекомендованными для RSA числами, длиной в 1024 битов.

Если положительное нечетное целое число n составное, а тест Миллера для одного b ($1 < b < n - 1$) его не распознал, то оно называется **строго псевдосоставным (сильно псевдосоставным)**. Для основания $b = 2$ псевдопростых чисел от 1 до 10^9 всего 1282, что говорит об эффективности данного теста. Наименьшее строго псевдосоставное число одновременно по основаниям 2, 3 и 5 – 25 326 001.

Практическое применение детерминированных тестов затруднено из-за их большой вычислительной сложности. В связи с этим на практике используются **вероятностные тесты простоты**:

- тест Ферма;
- тест Лемана;
- тест Миллера – Рабина;
- тест Соловея – Штрассена;
- и др.

Тест Ферма (основан на малой теореме Ферма).

Если n – простое число, то оно удовлетворяет сравнению $b^{n-1} \bmod n = 1$ для любого b . В тесте выбирается m случайных чисел b и для каждого из них проверяется выражения $b^{n-1} \bmod n = 1$. Если для всех b_i ($i = 1..m$) выражение истинно, то вероятность того, что n составное число равна $1/2^m$.

Выполнение сравнения является необходимым, но не достаточным признаком простоты числа. Если хотя бы для одного b сравнение невыполнимо, то n составное, в противном случае ничего определенного сказать нельзя. Если для составного n выполняется сравнение $b^{n-1} \bmod n = 1$, то число n называют **псевдопростым** по основанию b . Например, **числа Кармайкла** – составные числа, для которых сравнение $b^{n-1} \bmod n = 1$ выполняется для всех b взаимно простых с n . Чисел Кармайкла – бесконечное множество, наименьшее число Кармайкла – $561 = 3 * 11 * 17$.

Тест Лемана.

Сущность теста аналогичная тесту Ферма, за исключением:

- $b_i < n$;
- проверяемое выражение - $b^{(n-1)/2} \bmod n \neq \pm 1$.

Тест Миллера – Рабина.

Является модификацией теста Миллера и заключается в проверке только части свидетелей простоты b в интервале от 2 до $n - 2$, выбираемых случайным образом. Согласно недоказанной **теореме Рабина**, если тест Миллера, примененный к n для более, чем $n / 4$ свидетелей простоты, не распознает в n составного числа, то n – простое. Т.о. при положительной проверке m свидетелей простоты b вероятность того, что n составное число равна $1/4^m$. Рекомендуется брать $m \approx \log_2(n)$ (например, для $n = 10^5 + 1$, требуется проверить 13 свидетелей простоты).

Описание алгоритма.

1. Последовательно делим $n - 1$ на 2 пока не получим нечетное частное. В результате найдем положительное целое k и нечетное q , для которых $n - 1 = 2^k q$
2. Цикл А. Повторять m раз
 - 2.1. Выбрать случайно b в интервале $2 \dots n - 2$
 - 2.2. $x := b^q \bmod n$
 - 2.3. Если $x = 1$ или $x = n - 1$
то перейти к следующей итерации цикла А
 - 2.4. Цикл В. Повторять $k - 1$ раз
 - 2.4.1. $x := x^2 \bmod n$
 - 2.4.2. Если $x = 1$
то выдать « n – составное число» и завершить работу
 - 2.4.3. Если $x = n - 1$
то перейти к следующей итерации цикла А
 - 2.4.4. Перейти к следующей итерации цикла В
 - 2.5. Перейти к следующей итерации цикла А
3. Выдать « n – вероятно простое».

²⁾ Изначально у Римана было $70 \ln^2 n$, но в 1985 году Бах снизил необходимую границу до $2 \ln^2 n$, а в 2006 году Владимиров показал, что при последовательном

проходе b имеет смысл проверять только простые числа.

19.6. Определение наибольшего общего делителя

Наибольшим общим делителем (НОД) для двух целых чисел m и n называется наибольший из их общих делителей (например, для чисел 70 и 105 НОД равен 35). НОД существует и однозначно определён, если хотя бы одно из чисел m или n отлично от нуля. Возможные обозначения наибольшего общего делителя чисел m и n [17]:

- НОД(m, n);
- gcd(m, n) (англ. Greatest Common Divisor).

Наиболее известным способом определения НОД является **алгоритм Евклида**. Этот алгоритм не был открыт Евклидом, т.к. упоминание о нём имеется уже в «Топике» Аристотеля. В «Началах» Евклида он описан дважды - в VII книге для нахождения НОД двух натуральных чисел и в X книге для нахождения наибольшей общей меры двух однородных величин.

Суть алгоритма заключается в последовательном делении большего числа n на меньшее m , до тех пор, пока остаток от деления r не станет равным 0. При этом после каждого деления n присваивается текущее значение m , а m – остаток от деления r [17, 34] .

Описание алгоритма (при $n \geq m$).

```
1. Если  $m = 0$   
   то завершить работу ( $n$  является НОД)  
2.  $r := n \bmod m$   
3.  $n := m$   
4.  $m := r$   
5. Перейти к шагу 1
```

Пример. $n = 1071, m = 462$.

Таблица 19.4. Таблица итераций

№ итерации	n_i	m_i	$r_i = n_i \bmod m_i$
1	1071	462	147
2	462	147	21
3	147	21	0
4	21	0	конец

Результат – НОД(1071, 462) = 21.

Существует более мощный алгоритм определения НОД – **расширенный алгоритм Евклида** [10, 17, 34]. Несмотря на то, что он медленнее, данный алгоритм помимо НОД позволяет найти два таких числа α и β , что

$$\alpha n + \beta m = \text{НОД.} \tag{19.11}$$

Данное выражение называется **соотношением Безу**.

Суть расширенного алгоритма аналогична стандартному – последовательное деление большего числа n на меньшее m , до тех пор, пока остаток от деления r не станет равным 0. При этом на каждой итерации дополнительно вычисляются:

- целая часть q_i от деления n_i на m_i ;
- $\alpha_i = \alpha_{i-2} - q_i \alpha_{i-1}$;
- $\beta_i = \beta_{i-2} - q_i \beta_{i-1}$.

Для первой итерации принимаются $\alpha_{-1} = 1, \alpha_0 = 0, \beta_{-1} = 0, \beta_0 = 1$. Итоговые числа α и β равны $\alpha = \alpha_{k-2}, \beta = \beta_{k-2}$.

Описание алгоритма (при $n \geq m$).

```
1.  $\alpha_{-1} := 1$   
2.  $\alpha_0 := 0$   
3.  $\beta_{-1} := 0$   
4.  $\beta_0 := 1$   
5.  $i := 1$   
6. Если  $m = 0$   
   то  
     6.1.  $\alpha := \alpha_{k-2}$   
     6.2.  $\beta := \beta_{k-2}$ 
```

6.3. Завершить работу (n является НОД)

```

7. r := n mod m
8. n := m
9. m := r
10. qi := ni div mi
11. αi := αi-2 - qi αi-1
12. βi := βi-2 - qi βi-1
13. Перейти к шагу 2

```

Пример. $n = 1071, m = 462$.

Таблица 19.5. Таблица итераций

№ итерации	n_i	m_i	$r_i = n_i \bmod m_i$	$q_i = n_i \div m_i$	$\alpha_i = \alpha_{i-2} - q_i \alpha_{i-1}$	$\beta_i = \beta_{i-2} - q_i \beta_{i-1}$
					1	0
					0	1
1	1071	462	147	2	1	-2
2	462	147	21	3	-3	7
3	147	21	0	7	22	-51
4	21	0	конец			

Результат – НОД(1071, 462) = 21, $\alpha = -3, \beta = 7 \rightarrow (-3) * 1071 + 7 * 462 = 21$.

Расширенный алгоритм Евклида позволяет найти **обратное (мультипликативно обратное) число по модулю** [20] .

Пусть даны модуль **n** и число **m**. Требуется обратное число **m^{-1}** , такое, что

$$(m m^{-1}) \bmod n = 1. \quad (19.12)$$

Приведем следующее соотношение Безу

$$-a n + \beta m = 1. \quad (19.13)$$

Это равенство означает, что для некоторого целого α имеет место равенство $\beta m - \alpha n = 1$. Значит, мы можем вычислить $m^{-1} (= \beta)$ с помощью расширенного алгоритма Евклида. При этом значение переменной α нас не интересует. Если число $m^{-1} = \beta$ получается отрицательным, то нужно прибавить к нему n .

Пример. $n = 97, m = 30$.

Таблица 19.6. Таблица итераций

№ итерации	n_i	m_i	$r_i = n_i \bmod m_i$	$q_i = n_i \div m_i$	$\alpha_i = \alpha_{i-2} - q_i \alpha_{i-1}$	$m^{-1} = \beta_i = \beta_{i-2} - q_i \beta_{i-1}$
					1	0
					0	1
1	97	30	7	3	1	-3
2	30	7	2	4	-4	13
3	7	2	1	3	13	-42
4	2	1	0	2	-30	97
5	1	0	конец			

Т.к. m^{-1} – отрицательное число, то добавляем к нему $n \rightarrow m^{-1} = -42 + 97 = 55$. Проверяем $(m m^{-1}) \bmod n = (30 * 55) \bmod 97 = 1$.

Вопросы для самопроверки

1. Дайте классификацию алгоритмов в соответствии с их временной сложностью.
2. В чем суть основной теоремы арифметики?
3. Опишите метод факторизации Ферма.
4. Опишите алгоритм решета Эратосфена.
5. В чем суть теста Ферма на простоту числа.
6. Опишите алгоритм Евклида.
7. Приведите соотношение Безу.
8. Опишите расширенный алгоритм Евклида.

20.1. Угрозы безопасности при использовании криптографии

К основным угрозам безопасности при использовании криптографических систем можно отнести.

1. Перехват противником шифрограмм и получения из них защищаемой информации без знания примененного ключа – взламывание шифра.
2. Перехват противником шифрограмм и получения из них защищаемой информации с использованием ключей, добытых агентурным способом, с помощью шпионажа и т.д.
3. Преднамеренная (противником) или непреднамеренная (из-за искажений в каналах связи) подмена части или всей шифрограммы при передаче от одного абонента к другому.
4. Преднамеренная подмена части или всей шифрограммы одним из абонентов и выдачи ее за подлинную, отправленную другим абонентом.
5. Отказ одним из абонентов факта отправки шифрограммы.
6. Преднамеренное или непреднамеренное уничтожение шифрограммы при передаче от одного абонента к другому.
7. Посылка противником ложных шифрограмм от имени законных абонентов.
8. Преднамеренное или непреднамеренное уничтожение или подмена ключей.

Реализацией и предотвращением угроз первого типа занимаются в рамках криптоанализа шифров. Предотвращением угроз 3 - 8 типов занимаются в рамках криптоанализа криптографических протоколов, обеспечивающих целостность и подлинность авторства.

20.2. Краткая история

Термин криптоанализ был введен американским криптографом Уильямом Ф. Фридманом в 1920 г. Хотя понятие «криптоанализ» было введено сравнительно недавно, попытки дешифровки секретных сообщений стали предприниматься с момента появления первых шифров. В качестве показательного примера следует привести дешифровальное устройство Аристотеля «антисчиталу» (IV в. до н.э.).

В VIII-XV вв. значительный вклад в развитие криптоанализа сделали арабские ученые. Стоит отметить труды Халиля аль-Фарахида («Книга тайного языка»), Аль-Кинди («Манускрипт о дешифровке криптографических сообщений», 855 г.), Шихаба аль-Калкашанди («Субх ал-Ашаш», 1412 г.). В книге Аль-Кинди встречается первое известное упоминание о частотном криптоанализе, предназначенном для вскрытия шифров однозначной замены, а у Шихаба ал-Калкашанди - таблицы частоты появления букв в арабском языке на основе текста Корана.

Коран состоит из 114 глав, каждая из которых соответствует одному из откровений, полученных пророком Мухаммедом. Эти откровения были записаны во время жизни пророка различными его спутниками и позднее собраны воедино по решению первого халифа Абу Бакра. Умар и Усман, второй и третий халифы соответственно, завершили проект. Фрагментарный характер оригинальных писаний привел к рождению области богословия, посвященной точной датировке различных откровений. В частности, ученые-корановеды определили частоту появления некоторых слов, считавшихся новыми в периоды записи откровений. Если в каком-то откровении содержалось достаточное количество таких новых слов, было логично заключить, что это сравнительно позднее откровение.

Этот подход стал первым конкретным инструментом криптоанализа, получившим название **частотного анализа**. Первым человеком, оставившим письменное упоминание об этом революционном методе, был философ по имени Аль-Кинди, который родился в Багдаде в 801 г. Хотя он был астрономом, врачом, математиком и лингвистом, прославился он как создатель манускрипта по криптоанализу. Даже если Аль-Кинди не был первым, его имя, безусловно, занимает важное место в истории криптоанализа.

До недавнего времени очень мало было известно о новаторской роли Аль-Кинди. В 1987 г. в одном из архивов Стамбула была обнаружена копия его трактата «Манускрипт о дешифровке криптографических сообщений». Он содержит краткое изложение революционного метода:

Чтобы расшифровать зашифрованное сообщение, если мы знаем, на каком языке оно было написано, надо взять достаточно длинный текст, написанный на том же языке, а затем подсчитать, сколько раз каждая буква встречается в этом отрывке. Назовем наиболее часто встречающуюся букву «первой», вторую по частоте — «второй», и так далее, пока не переберем все буквы этого отрывка. Затем вернемся к шифрограмме, которую мы хотим расшифровать, и классифицируем ее символы тем же образом: найдем в шифрограмме символ, встречающийся чаще всех, и заменим его на «первую» букву из проанализированного текста, затем перейдем ко второму по частоте символу и заменим его на «вторую» букву, и так далее, пока не переберем все символы, используемые в шифрограмме.

Аль-Кинди. «Манускрипт о дешифровке криптографических сообщений»

В XV-XIX вв. развитие теории и практики криптоанализа получило новый импульс в Европе. Труды европейских ученых того времени были посвящены как описанию шифров, так и вопросам криптоанализа:

- итальянский писатель Леон Баттиста Альберти («Трактат о шифрах», 1466 г.);
- немецкий аббат Иоганн Трисемус («Полиграфия», 1518 г.);
- немецкий шифровальщик и археолог Фридрих Касиски («Тайнопись и искусство дешифрования», 1863 г.);
- голландский лингвист Огюст Керкхоффс («Военная криптография», 1883 г.);
- и многие другие.

В этот период стали появляться и государственные службы, в которых занимались вопросами дешифровки секретных сообщений.

Усиливающееся соперничество итальянских городов-государств вынудило правителей Венеции привлечь на службу людей, задача которых состояла в том, чтобы тайно просматривать почтовую корреспонденцию, предназначенную для послов других городов. Один из самых ранних примеров такого почтового досмотра относится к началу XVI в. В специально отведенном кабинете Дворца дождей трое высокооплачиваемых дешифровальщиков изучали всю корреспонденцию - от писем влиятельных торговых семейств до донесений послов. Сведения, которые обнаруживали дешифровальщики, позволяли правителям Венеции успешно разрабатывать военную и экономическую стратегию на десятилетия вперед. В атмосфере дворцовых интриг подобные службы стали обычным делом. Вскоре во Флоренции, Генуе и Неаполе последовали примеру Венеции, обзаведясь собственными дешифровальщиками.

После своего назначения в 1668 г. военный министр Людовика XIV Франсуа Лавуа организовал «черный кабинет» (фр. Cabinet Noir), в задачи которого входила перлюстрация¹ и дешифровка корреспонденции. Возглавить его доверили Антуану Россиньолю, который еще в молодости (1626 – 1628 гг.) успешно вскрывал шифры гугенотов, чем привлек к себе внимание и благосклонность первого министра Людовика XIII, кардинала Ришелье. Он стал первым криптоаналитиком, прославившимся благодаря своему таланту, в его честь слагали оды, а Шарль Перро включил его биографию в книгу «Знаменитые люди Франции». Вслед за Антуаном Россиньолем, начальниками черного кабинета были его сын и внук. Наименование службы стало нарицательным и, вслед за французами, оно стало применяться к подобным организациям.

Английский секретный кабинет появился, когда в 1655 г. Оливер Кромвель назначил Джона Терло, одного из организаторов секретной службы Парламента, Главным почтмейстером. Терло организовал при почтовой службе тайную канцелярию (англ. Secret Office) для перлюстрации писем и привлекал к сотрудничеству с ним лучшего математика Англии тех времен Джона Уоллиса.

Во времена правления императрицы Марии Терезии в Австрии была создана дешифровальная служба - Geheime Kabinets-Kanzlei. В начале XVIII в. Вена являлась средоточием европейской торговой и дипломатической деятельности, а также центром, через который проходила корреспонденция. И правители, и генералы Австрии были прекрасно осведомлены обо всем, здесь происходящем: о проезжающих путешественниках, о товарах и письмах, проходящих через Вену и обратно в столицы Западной Европы и более отдаленные города, такие, как Константинополь и Санкт-Петербург. Под покровительством императрицы Kabinets-Kanzlei процветал. Денежные премии, продвижение по службе, награды и почести - всем этим щедро награждались талантливые криптоаналитики.

По слухам, Мария Терезия сама была достаточно сведуща в криптографии и потому посоветовала австрийским дипломатическим представителям чаще менять свои номенклатуры и шифровальные ключи, чтобы дешифровальщики других стран не успевали их взломать.

На пике своей эффективности, пришедшемся на 1730 - 1760 гг., Kabinets-Kanzlei многие считали лучшей организацией подобного рода в Европе. К достижениям австрийских криптоаналитиков относится чтение шифрованной переписки Наполеона, Талейрана и множества других политических деятелей. Барон Игнац Кох (директор венского черного кабинета с 1749 по 1763 гг.), писал:

Это восемнадцатый шифр, который мы вскрыли в течение года... К сожалению, нас считают чересчур способными в этом искусстве, и мысль о том, что мы можем вторгнуться в их корреспонденцию, побуждает иностранные дворы непрерывно менять ключи, иначе говоря, посылать каждый раз более трудные в смысле дешифровки сообщения.

Барон Игнац Кох

В XVIII веке черные кабинеты стали распространенным явлением в странах Европы, в т.ч. Германии, Голландии, Дании и России.

В России датой учреждения первой государственной шифровальной службы можно считать 1549 г. - образование «посольского приказа» с «циферным отделением». Как минимум с 1702 г. Петра сопровождала походная посольская канцелярия под руководством первого министра Ф.А. Головина, которая с 1710 г. приобрела статус постоянного учреждения. В ней сосредоточилась криптографическая работа с перепиской между Петром, его приближенными и различными получателями, а также по созданию новых шифров.

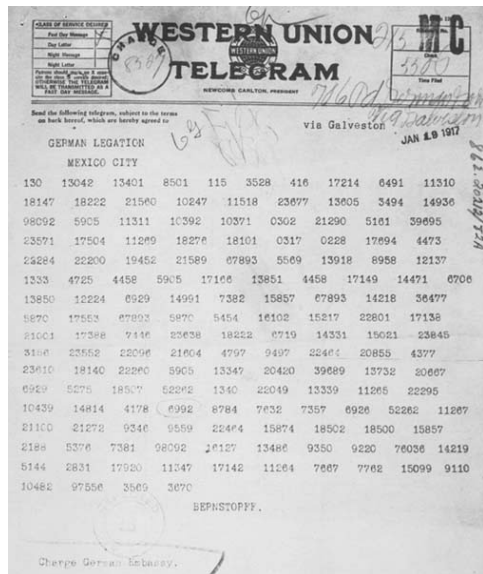
При Елизавете Петровне в России директором почт Бестужевым-Рюминым была налажена систематическая перлюстрация дипломатической корреспонденции. Санкт-Петербургскому почтамту было вменено в обязанность вскрывать и копировать всю ограниченную переписку зарубежных послов. Под контролем Бестужева-Рюмина, при коллегии иностранных дел вполне успешно действовала дешифровальная служба под началом секретаря Российской академии наук Кристиана Гольдбаха.

Формально датой организации российского черного кабинета можно считать 18 апреля 1794 г. В этот день Екатерина II секретным указом определила организацию службы перлюстрации во всероссийском масштабе. По указу, этой работой должны были заниматься чиновники Санкт-Петербургского почтамта и Рижской почтовой конторы.

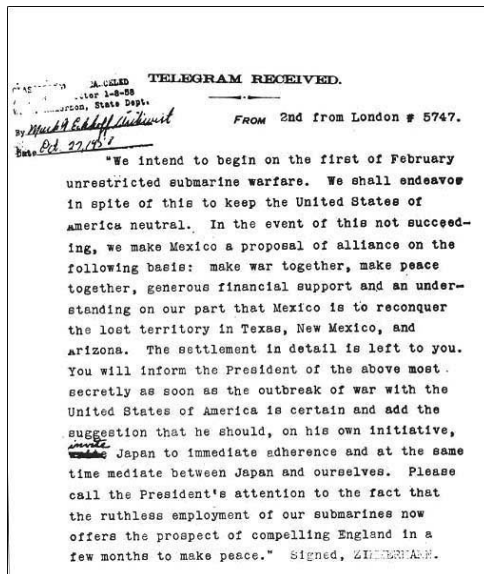
Бурные политические события середины XIX в. и развитие гражданского общества привели к ограничению власти европейских правительств и секретных органов надзора. В июне 1844 г. английское правительство объявило о прекращении перехвата переписки, в 1848 г. закрылись австрийский и французский черные кабинеты. В 1911 г. энциклопедия Британика писала, что черные кабинеты больше не существуют.

Первая мировая война и события после нее вновь остро поставили вопрос о воссоздании криптоаналитических служб.

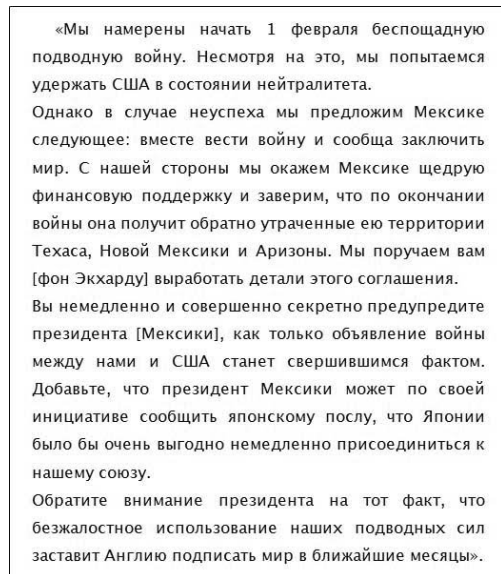
Вскоре после начала Первой мировой войны в Англии создается «секция 25 Разведывательного управления», более известная как «комната 40», поскольку именно в помещении с таким номером она и располагалась в здании Британского Адмиралтейства. За свою недолгую историю (1917-1919 гг.) сотрудники «Комнаты 40» расшифровали около 15 000 немецких сообщений, в т.ч. и известную «телеграмму Циммермана²», после огласки которой Конгресс США объявил войну Германии.



а) шифрограмма



б) расшифрованный текст на английском языке



в) расшифрованный текст на русском языке

Рис.20.1. Телеграмма Циммермана

В 1919 г. «Комната 40» была расформирована, и на ее базе, а также базе криптографического подразделения разведки британской армии МП1б была сформирована «Правительственная школа кодирования и шифрования» (Government Code and Cypher School, GC&CS), которая во время Второй мировой войны размещалась в Блетчли-Парке. Наиболее значимой работой GC&CS в этот период была операция «Ультра», нацеленная на дешифровку сообщений немецкой шифровальной машины «Энигма». Впоследствии GC&CS стала независимой от военной разведки службой радиоэлектронной разведки, в 1946 г. переименована в «Центр правительственной связи» (Government Communications Headquarters, GCHQ).

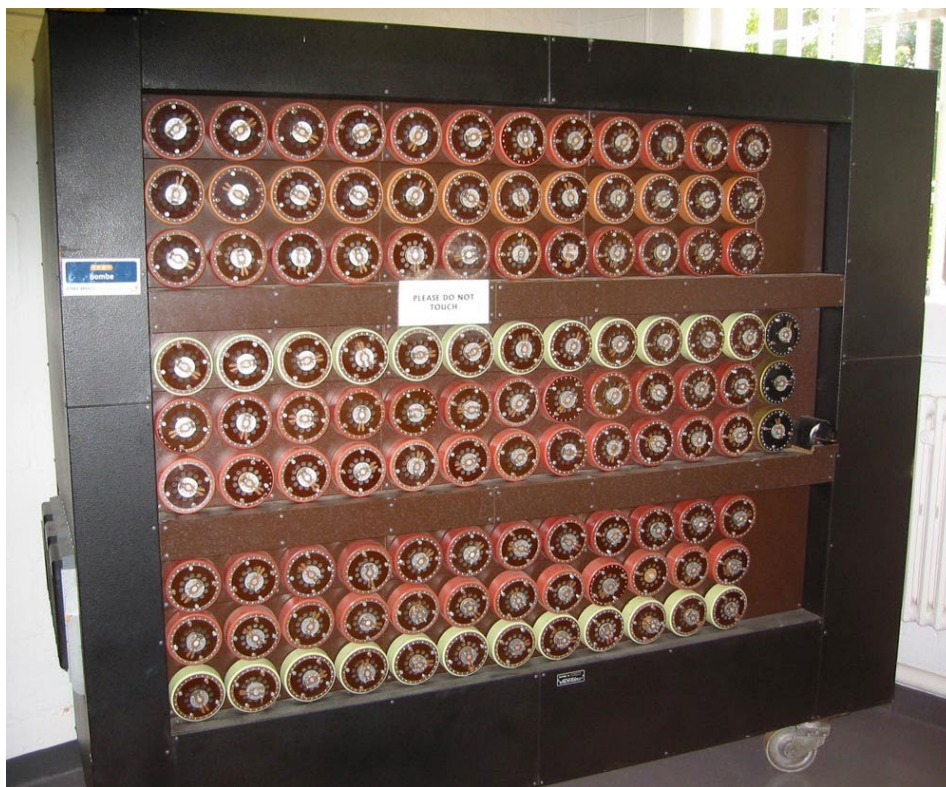


Рис.20.2. Дешифровальная машина Алана Тьюринга «Бомба» из Блетчли-Парка для взлома «Энигмы»

В Японии в 1925 г. при службе связи Генерального штаба Императорского военного флота был создан дешифровальный отдел Токуму Хан, или специальный отдел. В 1929 г. в Морском министерстве было создано подразделение радиоперехвата; в 1932 г., когда японцы заняли Шанхай, это подразделение, известное как «X Facility», действовало совместно с десантными отрядами ВМС. Именно это подразделение поставляло криптоаналитикам из Токуму Хан перехваченные радиогаммы Национальной китайской армии. Гоминьдановские войска Чан Кайши пытались противостоять интервенции японцев в Китай, однако превосходство военно-морских сил Токио и его более совершенные криптоаналитические возможности оказались для китайских войск слишком крепким орешком.

Во время советско-финской войны (1939 – 1940 гг.) Швеция успешно дешифровывала сообщения СССР и помогала Финляндии. Так, например, во время битвы при Суомуссалми успешный перехват сообщений о продвижении советской 44-й стрелковой дивизии помог Карлу Маннергейму вовремя выслать подкрепления, что стало залогом победы. Успешное дешифрование приказов о бомбовых ударах по Хельсинки позволяло часто включить систему оповещения о воздушном ударе еще до того, как самолеты стартуют с территории Латвии и Эстонии.

30 декабря 1937 г. было образовано 7-е отделение (в дальнейшем - 11-й отдел) Управления разведки Наркомата ВМФ, задачей которого являлось руководство и организация дешифровальной работы. В годы войны на дешифровально-разведочной службе (ДРС) СССР состояло около 150 человек. В 1941 - 1943 гг. ДРС Балтийского флота было взломано 256 германских и финляндских шифров, прочитано 87 362 сообщения. ДРС Северного флота (всего 15 человек) взломало 15 кодов (в 575 вариантах) и прочитала более 55 тыс. сообщений от самолетов и авиабаз противника, что, по оценке некоторых экспертов, позволило полностью контролировать всю закрытую переписку ВВС Германии. ДРС СФ также раскрыто 39 шифров и кодов, используемых аварийно-спасательной, маячной и радионавигационной службами и береговой обороны противника и прочитано около 3 тыс. сообщений. ДРС Черноморского флота имело информацию о текущей боевой обстановке и перехватывало некоторые стратегические сообщения.

Во время Второй мировой войны одним из важнейших источников информации для немецких войск как на суше, так и на море была «Служба наблюдения» (нем. Beobachtungs-Dienst, B-Dienst). Это название командующий немецкими ВМС адмирал Карл Дениц дал своей небольшой, но исключительно способной криптоаналитической группе. В марте и апреле 1940 г., когда Гитлер разрабатывал планы вторжения в Норвегию и захвата ее богатых месторождений руды, B-Dienst удалось взломать британские коды, в результате чего выяснилось, что английские ВМС планируют заминировать порт Нарвик в Норвегии. Эти сведения помогли нацистам устроить отвлекающую атаку, ввести англичан в заблуждение и благополучно высадить войска на норвежскую землю.

B-Dienst сумела также раскрыть многие коды британских торговых судов, которые передавались через сеть радиопередатчиков BAMS (Broadcasting for Allied Merchant Ships).

На второй год войны в B-Dienst занимались дешифрованием сообщений, в которых раскрывалось местоположение конвоев. Приказы капитанам транспортов снабжения держаться поодаль от опасных районов немцы использовали для того, чтобы указать «воющим стаям» их жертву. В течение весны 1941 г. потери союзников сильно возросли; в среднем уничтожалось одно судно каждые 16 часов. К марту 1943 г. B-Dienst могла даже читать

английскую «Оперативную сводку о местонахождении подводных лодок», и эти предупреждения судам на самом деле помогали субмаринам преодолевать систему обороны конвоев. «Волчий стан» находились на вершине успеха: криптоаналитики В-Dienst могли выбирать конвои в различных портах и определять их курс, время движения и скорость. С 16 по 19 марта эскадры Деница, потеряв всего одну субмарину, потопили 21 корабль общим водоизмещением 141 тыс. тонн.

Проблемы в области разведки во Второй мировой войне побудили американского президента Трумэна в 1952 г. реорганизовать Управление безопасности вооруженных сил в Агентство национальной безопасности (АНБ), которое в последующие годы добилося гораздо лучшей координации работ по сбору разведывательных данных и обеспечению безопасности. АНБ является не только центром американской криптологии, но и разрабатывает способы сокрытия информации для различных правительственных ведомств США, а также осуществляет криптоанализ кодов и шифров других стран.

В СССР данными вопросами занималось Восьмое главное управление КГБ (создано в 1954 г.), в настоящее время Шифровальная служба ФСБ РФ.

- 1Перлюстрация (от лат. perlustro - «обозреваю») - просмотр личной пересылаемой корреспонденции, совершаемый в тайне от отправителя и получателя.
- 2Артур Циммерман (нем. Arthur Zimmermann) - немецкий дипломат и политический деятель, статс-секретарь иностранных дел (министр иностранных дел) Германии 1916-1917 гг.

20.3. Общие сведения о криптоанализе

Напомним, что разработкой методов шифрования и дешифрования информации занимается **криптология**, которая разделяется на два направления — криптографию и криптоанализ.

Криптография – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Криптоанализ – наука, занимающаяся вопросами оценки сильных и слабых сторон методов шифрования, а также разработкой методов, позволяющих взламывать криптосистемы.

Классификация криптоатак приведена на следующем рисунке.

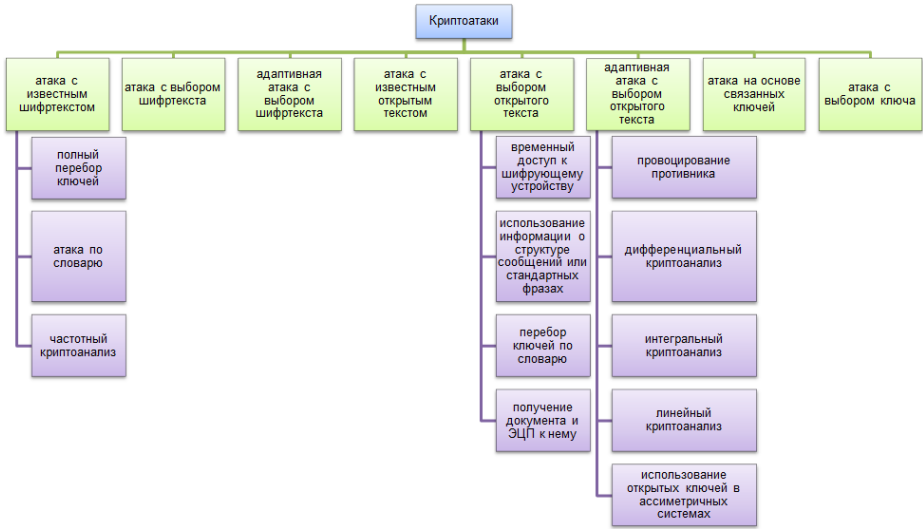


Рис.20.3. Классификация криптоатак

I. Атака с известным шифртекстом (ciphertext only attack). Предполагается, что противник знает алгоритм шифрования, но не знает секретный ключ. Кроме того, в его распоряжении имеется набор перехваченных шифрограмм. Разновидности:

- **полный перебор ключей**;
- **атака по словарю**, перебор ключей по словарю (dictionary attack). Использование Интернет-червя в 1988 г. предоставляет хорошо документированный случай взлома паролей. Интернет-червь пытался взломать пароли, работая с серией словарей. На первом этапе атаки было использовано множество слов, содержащее имена пользователей, взятых из файла паролей системы Unix. Если это не имело успеха, использовался внутренний словарь 432 общепринятых, используемых в Интернет-жаргоне, слов. Если второй этап не имел успеха, использовался Unix словарь, состоящий из 24474 слов. Червь также проверял на пустой пароль. Сайты, на которые производилась атака, сообщили, что около 50 % паролей было успешно взломано, используя данную стратегию;
- **частотный криптоанализ** - метод вскрытия шифра, основывающийся на предположении о существовании зависимости между частотой появления символов в открытых сообщениях и соответствующих шифрознамен в шифрограммах. Метод частотного криптоанализа известен с IX-го века (работы Аль-Kindи), хотя наиболее известным случаем его применения в реальной жизни, возможно, является дешифровка египетских иероглифов Ж.-Ф. Шампольоном в 1822 г. В художественной литературе наиболее известными упоминаниями являются рассказы «Золотой жук» Эдгара По, «Пляшущие человечки» Конан Дойля, а также роман «Дети капитана Гранта» Жюль Верна.

II. Атака с выбором шифртекста (chosen ciphertext attack). Криптоаналитик имеет возможность выбрать необходимое количество шифрограмм и получить соответствующие им открытые тексты. Криптоаналитик может воспользоваться устройством расшифрования один или несколько раз для получения шифротекста в расшифрованном виде. Используя полученные данные, он может попытаться восстановить секретный ключ для расшифровки.

III. Адаптивная атака с выбором шифртекста (adaptive chosen ciphertext attack). Криптоаналитик имеет возможность выбирать новые шифрограммы для расшифровки с учетом того, что ему известна некоторая информация из предыдущих сообщений. В некоторых криптографических протоколах при получении шифрограммы, несоответствующей стандарту (содержащей ошибки), отправитель получает ответное сообщение, иногда с детализированным описанием этапа проверки и причины возникновения ошибки. Криптоаналитик может использовать эту информацию для последовательной отсылки и уточнения параметров криптосистемы.

IV. Атака с известным открытым текстом (known plaintext attack). То же, что и предыдущая, но противник для некоторых шифрограмм получает в свое распоряжение соответствующие им открытые сообщения. Во время «холодной войны» американские дипломаты в Москве пользовались шифровальными машинами, получившими кодовое название «бриллианты». Оборудование располагалось на девятом этаже здания посольства США в особом защищенном помещении, называвшемся узлом связи. Внутри этого помещения была еще одна комната, где шифровальные машины зашифровывали и расшифровывали шифрограммы, которыми обменивались посольство и штаб-квартира ЦРУ в Лэнгли (штат Виргиния). В другой части узла связи другие машины передавали перехваченную АНБ информацию или вели обмен сообщениями между Госдепартаментом и его представителями в Москве. Чтобы обеспечить как можно более полную защиту этого помещения, были предприняты особые меры безопасности в отношении его стен, электропроводки, линий электропитания и подачи воздуха. Сами шифровальные машины представляли собой новейшую разработку АНБ с цифровыми кодами на магнитных лентах, которые менялись каждые 24 часа. Кроме того, каждое сообщение пропусклось через две машины, зашифровываясь дважды. Все это создавало впечатление неуязвимости как узла связи, так и «бриллиантов». Но, несмотря на все меры безопасности, русские сумели тайно подменить «чистые» кабели электропитания шифровальных машин. Таким образом они смогли обойти электронные фильтры защиты и улавливали сигналы напрямую с «бриллиантов». В печатающих устройствах шифровальных машин были заменены печатные платы и кремниевые микросхемы, что позволило агентам КГБ снимать и записывать незашифрованные сигналы с линий связи и принтеров. Получив в свое распоряжение открытый текст, они имели возможность затем сравнить его с зашифрованными сообщениями и найти ключи шифрования. Сверхсекретное шифровальное оборудование в Москве превратилось в огромное подслушивающее устройство.

V. Атака с выбором открытого текста (chosen plaintext attack). Криптоаналитик обладает определённым числом открытых текстов и соответствующих шифротекстов, кроме того, он имеет возможность зашифровать несколько предварительно выбранных открытых текстов (до начала атаки). Разновидности:

- **временный доступ к шифрующему устройству** - американским спецслужбам удалось, подкупив охрану, выкрасть из японского посольства шифровальную машину на два дня. Возможность взлома машины была исключена, так как это бы привело к раскрытию операции и к смене всех ключей. Зато, американцы получили возможность осуществить атаку японского шифра на основе подобранного открытого текста;
- **использование информации о структуре сообщений или стандартных фразах** – криптоаналитики из Блетчли-Парка могли определить открытый текст сообщений в зависимости от того, когда эти сообщения были посланы. Например, ежедневный отчет о погоде посылался немецкими связистами в одно и то же время. По той причине, что военные доклады имеют определенную структуру, криптоаналитикам удавалось расшифровывать остальную информацию, пользуясь данными о погоде в той местности. Другим ярким примером являлись перехваченные сообщения офицера африканского корпуса, который постоянно отсылал «Нечего докладывать». Другие операторы тоже часто использовали стандартные ответы или приветствия;
- **перебор ключей по словарю** (dictionary attack) – криптоаналитик шифрует слова и фразы, наличие которых предполагается в шифрограмме, с использованием различных ключей. Совпадение зашифрованных слов и фраз с частями шифрограммы может говорить об обнаружении ключа;
- **получение документа и ЭЦП к нему**, сгенерированной с помощью закрытого ключа.

VI. Адаптивная атака с выбором открытого текста (adaptive chosen plaintext attack). Криптоаналитик имеет возможность выбирать новые открытые тексты с учетом того, что ему известна некоторая информация из предыдущих сообщений. Т.е. он может получить пары «открытое сообщение – шифрограмма», в т.ч. и после начала атаки. Разновидности:

- **провоцирование противника на использование в сообщениях определенных слов или фраз** – во время Второй мировой в Блетчли-Парк был придуман следующий способ заставить немцев отсылать определенные сообщения. По просьбе криптоаналитиков Королевские военновоздушные силы Великобритании минировали определенные участки Северного моря, этот процесс был назван «Садоводством» (англ. «gardening»). Практически сразу после этого немцами посылались зашифрованные сообщения, включающие слово «мины» и названия мест, где они были сброшены;
- **дифференциальный криптоанализ** – метод вскрытия симметричных блочных шифров (и других криптографических примитивов, в частности, хеш-функций), основанный на изучении разностей между шифруемыми значениями на различных раундах для пары подобранных открытых сообщений при их шифровании с одним и тем же ключом. Предложен в 1990 г. израильскими специалистами Эли Бихамом и Ади Шамиром. Является статистической атакой, в результате работы которой предлагается список наиболее вероятных ключей шифрования. Дифференциальный криптоанализ применим для взлома DES, FEAL и некоторые других шифров, как

правило, разработанных ранее начала 90-х. Количество раундов современных шифров (AES, Camellia и др.) рассчитывалось с учетом обеспечения стойкости, в т.ч. и к дифференциальному криптоанализу;

- **интегральный криптоанализ** – аналогичен дифференциальному криптоанализу, но в отличие от него рассматривает воздействие алгоритма не на пару, а сразу на множество открытых текстов. Впервые применен в 1997 г. Ларсом Кнудсеном;

- **линейный криптоанализ** – метод вскрытия шифра, использующий линейные приближения для описания его работы. Линейный криптоанализ был изобретён японским криптологом Мицуру Мацуи (Mitsuru Matsui). Предложенный им в 1993 г. алгоритм был изначально направлен на вскрытие DES и FEAL. Впоследствии линейный криптоанализ был распространён и на другие алгоритмы. На сегодняшний день наряду с дифференциальным криптоанализом является одним из наиболее распространённых методов вскрытия блочных шифров. Разработаны атаки на блочные и потоковые шифры. Криптоанализ выполняется в два шага. Первый – построение линейных соотношений между открытым текстом, шифрограммой и ключом, которые справедливы с высокой вероятностью. Второй – использование этих соотношений вместе с известными парами «открытый текст – шифрограмма» для получения битов ключа;

- **использование открытых ключей в асимметричных системах** – криптоаналитик имеет возможность получить шифротекст, соответствующий выбранному сообщению, на основе открытого ключа.

VII. Атака на основе связанных ключей (related key attack). Криптоаналитик знает не сами ключи, а некоторые различия (соотношения) между ними. Множество реальных систем используют разные ключи, связанные известным соотношением. Например, для каждого нового сообщения предыдущее значение ключа увеличивается на единицу.

VIII. Атака с выбором ключа (chosen key attack). Криптоаналитик задает часть ключа, а на оставшуюся часть ключа выполняет атаку на основе связанных ключей.

Вопросы для самопроверки

- 1. Перечислите основные угрозы безопасности при использовании криптографических систем.
- 2. Перечислите основные разновидности адаптивной атаки с выбором открытого текста.

Как отмечалось ранее, разработкой средств и методов сокрытия факта передачи сообщения занимается **стеганография** (греч. *στεγανός* — скрытый и *γράφω* — пишу; буквально «тайнопись»). Наиболее эффективно ее применение совместно с криптографическими методами. Обычно стеганографию делят на два направления: классическую и компьютерную.

21.2. Классическая стеганография

Среди классических методов можно выделить следующие:

- манипуляции с носителем информации (контейнером);
- симпатические чернила;
- микронадписи и микроточки;
- литературные приемы;
- семаграммы.

Манипуляции с носителем информации.

Первые следы применения стеганографических методов теряются в глубокой древности. Существует версия, что древние шумеры одними из первых использовали стеганографию, так как было найдено множество глиняных клинописных табличек, в которых одна запись покрывалась слоем глины, а на втором слое писалась другая. Однако противники этой версии считают, что это было вовсе не попыткой сокрытия информации, а всего лишь практической потребностью.

В третьей и седьмой книгах «Истории» древнегреческого ученого Геродота встречается описание еще двух методов сокрытия информации [43]:

- в V веке до н.э. греческий тиран Гистий, находясь под надзором персидского царя Дария в Сузах, должен был послать секретное сообщение своему родственнику в азиатский город Милет. Он побрил наголо своего раба и вытатуировал послание на его голове. Когда волосы снова отросли, раба отправили в путь;

- в Древней Греции тексты писались на дощечках, покрытых воском. В 480 г. до н.э. персидская армия под предводительством Ксеркса I двигалась на греческие города-государства. Узнав, что Ксеркс готов к выступлению, греческий царь Демарат, сосланный в Персию, предупредил об этом спартанцев. Он соскоблил воск с двух деревянных дощечек для письма, написал все, что ему стало известно о намерениях персов, а затем снова покрыл дощечки воском. Эти на вид чистые дощечки были без проблем доставлены в Лакедемон (Спарта). Горго, жена царя Леонида, внимательно осмотрела дощечки и обнаружила скрытое послание. То, что она прочитала, принесло ей и радость, и горе. Ее супруг, Леонид, со своими людьми поспешил форсированным маршем к решающему рубежу обороны на пути наступающих персов. Этим местом был проход, называвшийся Фермопилы. Из-за предателей, знавших тайный путь, Леонид и его 300 воинов-спартанцев погибли, но они три дня удерживали свои позиции, дав время городам-государствам подготовиться к сражению и снискав славу героев.

Эней Тактик в своих исторических трактатах (IV в. до н.э.) описывал способ тайной передачи посланий, когда в пергаменте над или под написанными буквами прокалывали крошечные отверстия. Этим способом пользовались в Англии до появления телеграфа с целью избежать больших расходов на почтовую пересылку. Отправка писем на дальние расстояния стоила крайне дорого, старые же газеты с наклеенной маркой можно было пересылать по стране взад и вперед. Многие из тех, кто не в состоянии был позволить себе оплатить почтовые расходы, ставили в газетах точки над буквами; таким образом, они писали письма, которые затем доставлялись бесплатно. Получатель просто последовательно выписывал все отмеченные таким образом буквы, и в результате получалось адресованное ему сообщение.

К 1000 г. н.э. китайские военачальники записывали важные сообщения на очень тонкой бумаге или шелке. Затем такое послание плотно скатывалось и покрывалось воском. Когда воск остывал, курьер прятал письмо в своей одежде, проглатывал или пользовался как тайником одним из отверстий собственного тела.

Классический пример физического сокрытия информации - курительная трубка, столь любимая секретными агентами. Сообщение пряталось в полости стенок чаши и прикрывалось внутренней (поворотной) частью чаши, при этом можно было, набив трубку табаком, курить ее. В случае опасности шпиону достаточно было слегка повернуть внутреннюю часть чаши, чтобы бумага с записанным на ней сообщением упала в горящий табак.

Приведем интересный химический способ записи секретных сообщений внутри вареного яйца. Берется смесь квасцов, чернил и уксуса, записывается ею на скорлупе послание, выдерживается в крепком рассоле или уксусе, чтобы стравить с поверхности следы, и варится яйцо вкрутую. В результате текст сообщения оказывается под скорлупой сверху белка.

Симпатические (невидимые) чернила – чернила, записи которыми являются изначально невидимыми и становятся видимыми только при определенных условиях (нагрев, освещение, химический проявитель и т. д.) [17].

Невидимыми чернилами пользовались еще во времена Римской империи. В I в. н.э. римский писатель Плиний Старший в своей «Естественной истории» описывал применение для тайнописи жидкости, изготовленной из молочая. Греческий военный ученый Филон Византийский писал о жидкости из чернильных орешков, благодаря которой написанное сообщение было невидимым. Арабские ученые в начале XV в. упоминали о некоторых смесях из растений, произрастающих в их регионе; то же относилось к таким писателям эпохи Возрождения как Леон Баттиста Альберти и Джованни Порта. Французский сатирик Франсуа Рабле в романе «Гаргантюа и Пантагрюэль» (1532 г.) с юмором рассуждал о тайнописи. Среди прочих остроумных комментариев о жизни он описывал способ приготовления невидимых чернил из таких веществ, как сок белого лука, нашатырь и квасцы [43].

Примером может служить любопытный исторический эпизод: восставшими дворянами в Бордо был арестован францисканский монах Берто, являвшийся агентом кардинала Мазарини. Восставшие разрешили Берто написать письмо знакомому священнику в город Блэй. Однако в конце этого письма религиозного содержания, монах сделал приписку, на которую никто не обратил внимание: "Посылаю Вам глазную мазь; натрите ею глаза и Вы будете лучше видеть". Так он сумел переслать не только скрытое сообщение, но и указал способ его обнаружения. В результате монах Берто был спасен [36].

Во время гражданской войны между южанами и северянами два агента северян Сэмюэль Вудхулл и Роберт Тоунсенд передавали информацию Джорджу Вашингтону, используя специальные чернила.

Различные симпатические чернила использовали и русские революционеры в начале XX века, что нашло отражение в советской литературе. Куканов в своей повести "У истоков грядущего" описывает применение молока в качестве чернил для написания тайных сообщений. Впрочем, царская охранка тоже знала об этом методе (в архиве хранится документ, в котором описан способ использования симпатических чернил и приведен текст перехваченного тайного сообщения революционеров).

Симпатические чернила бывают, как правило, двух видов: химические и органические. Первые представляют собой химические растворы, которые делаются невидимыми при высыхании. Скрытые слова становятся видимыми при добавлении к ним других химических препаратов, называемых реагентами. Органическая группа представлен, в большинстве случаев легкодоступными веществами, такими, как лук, лимон, молоко и уксус. Они обычно становятся видимыми, если их осторожно нагреть [43].

В качестве симпатических чернил могут использоваться различные вещества [17].

Таблица 21.1. Симпатические чернила и их проявители

Чернила	Проявитель
Лимонная кислота (пищевая)	Бензилоранж
Воск	CaCO ₃ или зубной порошок
Яблочный сок	Нагрев
Молоко	Нагрев
Сок лука	Нагрев
Сок брюквы	Нагрев
Пирамидон (в спиртовом растворе)	Нагрев
Важущие средства для дезинфекции рта и глотки	Нагрев
Квасцы	Нагрев
Слюна	Очень слабый водный раствор чернил
Фенолфталеин	Разбавленная щелочь
Стиральный порошок	Свет лампы ультрафиолета
Крахмал	Йодная настойка
Аспирин	Соли железа

В целях обнаружения тайных сообщений, написанных с помощью симпатических чернил, американские цензоры во время Второй мировой войны "полосовали" письма, чтобы выявить наличие в них невидимых чернил. Лаборант водил по письму несколькими щетками, закрепленными в одном держателе и смоченными в растворах различных проявителей. Эти проявители обладали различными свойствами и реагировали даже на выделения человека, так что после обработки на бумаге появлялись отпечатки пальцев и капли пота [13].

Письма также проходили проверку в инфракрасных и ультрафиолетовых лучах. Текст, написанный крахмалом и невидимый при дневном или электрическом свете, начинал светиться под воздействием ультрафиолета. Инфракрасные лучи помогали различать цвета, неотличимые при обычном освещении. Например, зеленые надписи на зеленой почтовой марке.

Проблемы, в которых местные отделения не могли разобраться своими силами, передавались в лабораторию отдела безопасности. Одна из таких проблем заключалась в том, что немецкие агенты расслаивали лист бумаги пополам, писали текст невидимыми чернилами на внутренней поверхности, а половинки затем вновь соединяли между собой. Поскольку чернила оказывались внутри листа, никакой реагент, нанесенный на его внешнюю поверхность, не мог их проявить. Эта уловка была обнаружена лишь после того, как один немецкий агент использовал для своего письма слишком много чернил и их избыток просочился сквозь бумагу.

В 2011 г. Мануэль Паласиос (Manuel Palacios) из университета Тафтса и Джордж Уайтсайдс (George Whitesides) из Гарварда попробовали спрятать сообщение в массиве, состоящем из семи штаммов¹ бактерий Escherichia coli (E. coli). Технику в шутку называли SPAM (Steganography by Printed Arrays of Microbes), что можно перевести как стеганография при помощи печатных массивов микробов [37].

Учёные создали семь штаммов бактерий, каждый из которых производит свой белок, флуоресцирующий при определённом свете (подробности – в статье в журнале PNAS). Колонии бактерий наносятся на подложку в виде рядов точек. Каждая пара точек (цветов) является кодом для буквы, цифры или символа. Семь цветов дают 49 комбинаций, авторы работы использовали их для кодирования 26 букв и 23 других символов (таких как, цифры, @ или \$). Например, две жёлтых точки обозначают букву "t", а комбинация оранжевой и зелёной – "d". Получатель, зная коды дешифровки, легко прочтёт посланное сообщение – свечение заметно невооружённым глазом.



Рис 21.1. Пример "проявленного" послания

Чтобы создать сообщение, биологи наносят штаммы E.coli, устойчивые к определённому антибиотику, на подложку с агаром (средой, питательной для

бактерий). Затем поверх подложки кладут лист из нитроцеллюлозы – колонии отпечатываются на нём. Для проявки сообщения, получатель должен будет поместить нитроцеллюлозный листок в чашку с "проявочной" агаровой средой, запускающее работу нужных генов и свечение штаммов. В состав "проявочной" агаровой среды входит правильный антибиотик, который убивает все микроорганизмы, кроме тех, что кодируют сообщение (так как они устойчивы к действию лекарства). В результате при проявке он получит нужный код.

Сейчас британские и американские исследователи пробуют подобным образом зашифровать сообщения при помощи дрожжей и спороносных бактерий, а в дальнейшем "покушаются" и на растения. "Было бы здорово спрятать информацию в форме листьев или рисунке корневой системы. Чем больше черт, тем больший объём данных можно зашифровать" - говорит Паласиос.

Микронадписи и микроточки.

Страсть к изготовлению микроизображений насчитывает долгую историю [38]. Это и **надписи на амулетах** (самая ранняя из таких находок – амулет, найденный при раскопках южной стены Иерусалимского храма, относится к началу VIII века до нашей эры), и **микротексты**, вписанные или впечатанные в страницы различных фолиантов (вне всякого сомнения, самым характерным примером микронадписей является Псалтырь Св. Иеронима, написанный монахом Иоахимом Большим в 1481 г. в Роттенберге для библиотеки папы Сикста IV. Внизу второй страницы в круг диаметром 12 мм вписаны первые 14 стихов Евангелия от Иоанна. Этот текст содержит 168 слов из 744 букв. По расчетам каждая буква занимает площадь не более 0,15 кв.мм.) и **специальные подарочные издания**. Как правило, прочесть, а тем более, нанести такие надписи без применения увеличительных приборов невозможно. Нельзя исключать, что человек начал использовать оптические приборы значительно раньше знаменитого изобретения Левенгука. Во всяком случае, из греческих источников следует, что древним был известен способ использования маленьких стеклянных сосудов, наполненных водой, в качестве увеличительных приспособлений.

Уже в XVIII веке в Англии и Франции были созданы специальные механические устройства для выполнения микронадписей. Одно из самых совершенных таких устройств, Peter's Machine for Microscopic Writing (1862 г.), хранится в музее Оксфордского университета. Оно позволяло выполнять надписи с высотой символов всего в 2,5 микрона²!

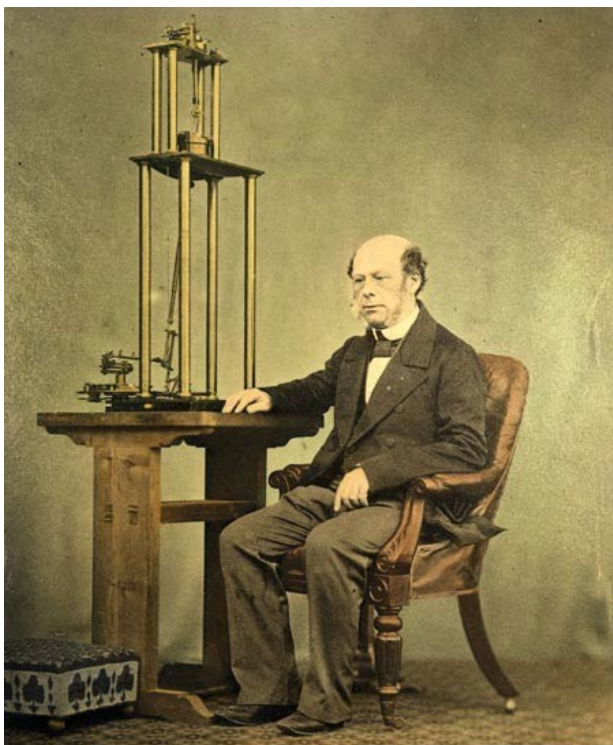


Рис 21.2. Peter's Machine for Microscopic Writing

Признанным пионером микрофотографии считается английский фотограф-энтузиаст Джон Б.Дэнсер. Похоже, именно он сделал первую микро-фоторепродукцию. В 1839 г., установив на камеру Даггера объектив от микроскопа с фокусным расстоянием 38 мм, он получил микро-даггеротип бумажного оригинала в масштабе 160 : 1. В 1856 г. ему удалось получить несколько удачных микроизображений, в том числе портретов членов королевской семьи, которые были подарены королеве Виктории.

В 1867 г. парижский фотограф Рене Дагрон (фр. Dagron) разработал свой метод микрофильмирования, который был использован во времена франко-прусской войны (в 1870 г.).

В ходе неудачной военной кампании 1870 г. войска Наполеона III потерпели поражение под Седаном. 2 – 4 сентября Париж был окружен объединенными германо-прусскими войсками, началась пятимесячная осада французской столицы, где была провозглашена 3-я Республика. Все связи с внешним миром были прерваны. Предпринимались отчаянные попытки использования самых разнообразных способов общения вплоть до "голубиной почты". Но грузоподъемность такого перевозчика авиапочты не очень велика. Вот тут-то и пригодился опыт Дагрона в микрофотографии.

12 ноября 1870 г. Дагрон и несколько его помощников вместе со своим оборудованием погрузились на два наполненных водородом воздушных шара, символично названных "Ньепс" и "Даггер" в честь изобретателей фотографии. После безумной гонки над головами немецких улан, пытавшихся посадить или сбить смелых воздухоплавателей, тем все же удалось достигнуть города Тура.

Прибыв на место, Дагрон развернул свою фотолабораторию и организовал микрофильмирование почты и других материалов, предполагавшихся к пересылке "голубиной почтой". Письма и сообщения выполнялись на прозрачных листах, разделенных на 12 секций размером 80 x 110 мм. Они копировались по частям контактным способом на фотографические пластинки, которые после химической обработки повторно переснимались с большим уменьшением с помощью специальной репродукционной камеры. В результате получались микроизображения размером не более 1 мм!

Полученные изображения вырезались и монтировались вместе с другими сообщениями на кусочке коллоидной пленки и подготавливались для отправки голубиной почтой в Париж. За 5 месяцев осады французской столицы Дагрону удалось скопировать на микропленку 470 листов, содержащих 2.5 миллиона сообщений. Как утверждают, один голубь мог нести от 36 до 54 тысяч сообщений, снятых на 18 тончайших пленок.

Первым создателем "настоящей" микроточки истории справедливо считают Эммануила Голдберга, который в 1925 г. не только собрал оригинальную оптическую схему для её фотографирования, но и подробно описал все этапы создания фото с высоким разрешением [39].

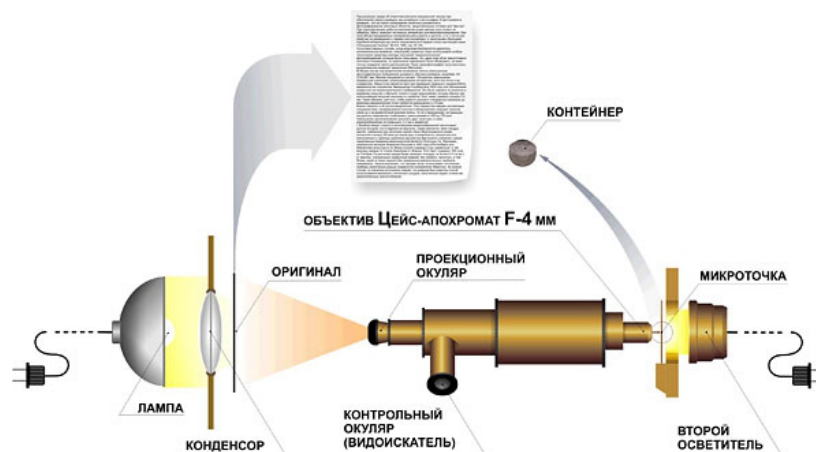


Рис 21.3. Оптическая схема Голдберга для изготовления микроточки

Из английских и американских архивов следует, что немецкая разведка АБВЕР перед Второй мировой войной самым активным образом использовала микроточки для связи с агентурой в Северной и Латинской Америке. По словам Гувера, первое предупреждение о существовании микроточек ФБР получило в январе 1940 г. Но обнаружили такую микроточку лишь в августе 1941 г., когда некий техник-фотолаборант случайно заметил отблеск света на конверте, изъятый у попавшего под подозрение немецкого агента. Причиной отблеска послужила микроточка, замаскированная под точку в конце предложения [43].

Западные историки микрофотографии также утверждают, что и советская разведка использовала микроточки еще до начала войны. После окончания войны в 1945 г. микроточки широко применялись советскими агентами, действовавшими по всему миру. Одним из таких агентов был Рудольф Абель. Он использовал данный метод в 1950-х гг., занимаясь шпионской деятельностью в районе Нью-Йорка [43].

Микроточки обладали способностью передавать большие объемы информации (сотни страниц и чертежей в одной точке) и обычно вклеивались в письмо или книгу. Микроточки прятали в украшениях, монетах, батарейках, предметах обихода, помещали в надрезанный край открытки с последующим аккуратным заклеиванием надреза.

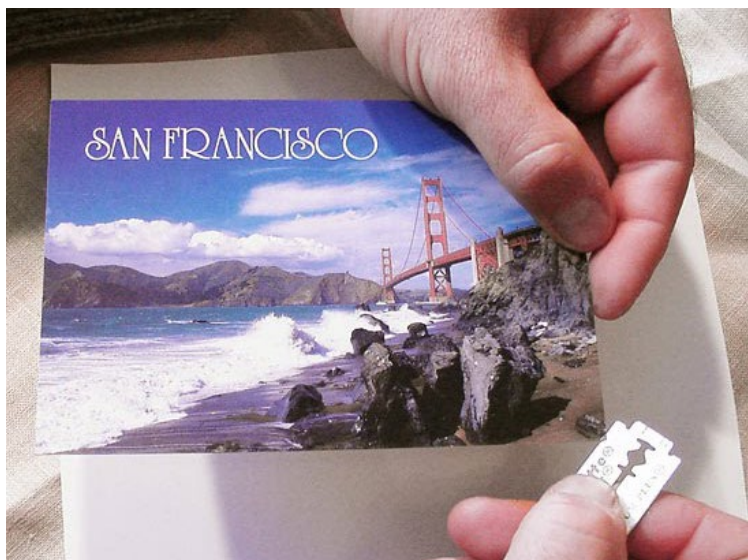


Рис 21.4. Надрезание края конверта для тайника микроточки

В 2001 г. в Австралии была разработана технология нанесения микроточек, содержащих Персональный идентификационный номер (ПИН), на важнейшие детали изделия (обычно - автомобиля). Такие, изготовленные с помощью лазера прозрачные микроточки наклеиваются в неприметных местах непосредственно на сборочном конвейере. Увидеть их можно только при освещении ультрафиолетовым светом. Этот процесс, дешёвый и эффективный, затрудняет угонщикам автомобилей легальную продажу украденной и разобранной машины в виде "запчастей" [17].

Производители цветных принтеров добавляли в них функцию печати т.к. называемых "желтых точек".

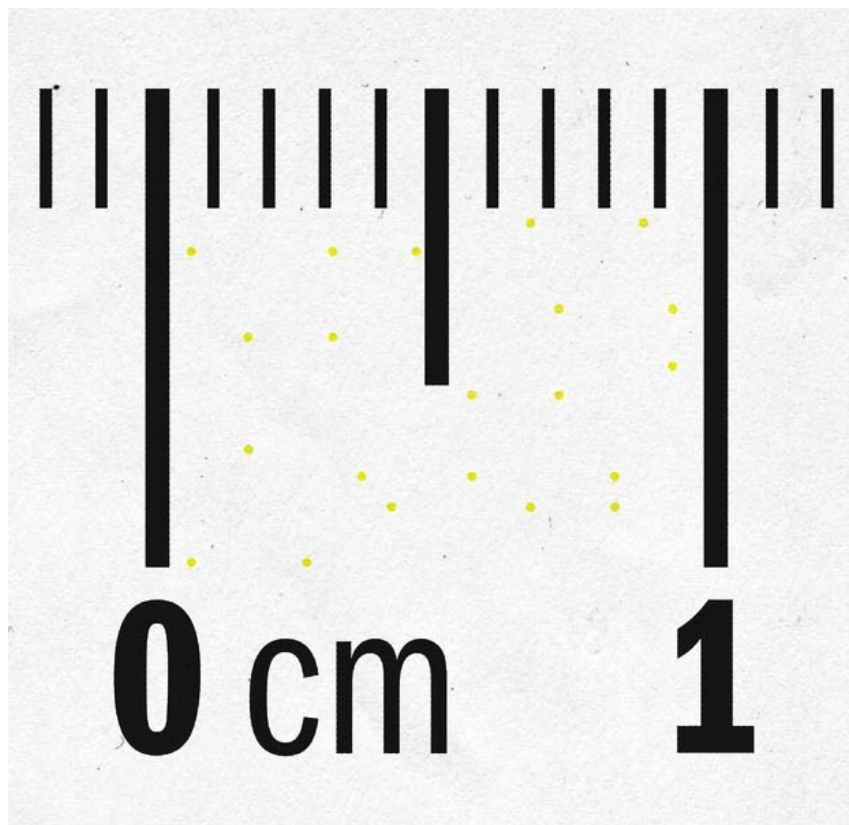


Рис 21.5. Желтые точки

Эти точки, едва видны невооруженным глазом, печатались на каждой странице и содержали в себе информацию о серийном номере принтера, а также дате и времени печати. Подтверждено использование данного метода в принтерах, выпускаемых под торговыми марками Brother, Canon, Dell, Epson, Hewlett-Packard, IBM, Konica, Kyocera, Lanier, Lexmark, NRG, Panasonic, Ricoh, Savin, Toshiba, Xerox. Введение данной меры, согласно комментариям производителей, являлось частью сотрудничества с правительством и консорциумом банков, направленного на борьбу с фальшивомонетниками.

В заключение следует отметить, что использование микроточек для передачи секретных сообщений описал еще греческий ученый Эней Тактик в сочинении "Об обороне укрепленных мест". Суть предложенного им так называемого "книжного шифра" заключалась в прокалывании малозаметные дырок в книге или в другом документе над буквами секретного сообщения. Во время Первой мировой войны германские шпионы использовали аналогичный шифр, заменив дырки на точки, наносимые симпатическими чернилами на буквы газетного текста.

Экзотическим способом хранения и передачи информации является использование для этих целей **ДНК-молекул**. В клетках животных и растений ДНК (дезоксирибонуклеиновая кислота) находится в ядре клетки в составе хромосом, а также в некоторых клеточных органоидах (митохондриях и пластидах). В клетках бактерий молекула ДНК прикреплена изнутри к клеточной мембране. У них и у низших эукариот (например, дрожжей) встречаются небольшие автономные молекулы ДНК, называемые плазмидами. Кроме того, ДНК-молекулы могут образовывать геном некоторых вирусов [17].

В 1998г. бразильский художник Эдуардо Кац перевёл фразу из Книги Бытия (лат. Genesis) в код Морзе, который, в свою очередь, представил в виде последовательности ДНК. Цитата из Бытия, ради эксперимента, была чуть подсокращена и модифицирована: «И да владычествует человек над рыбами морскими и над птицами небесными, и над всякой живностью, движущейся по земле» (Let man have dominion over the fish of the sea, and over the fowl of the air, and over every living thing that moves upon the earth). Синтезированный ген Кац клонировал в плазмиды, которые затем встроил в клетки бактерии E. Coli.

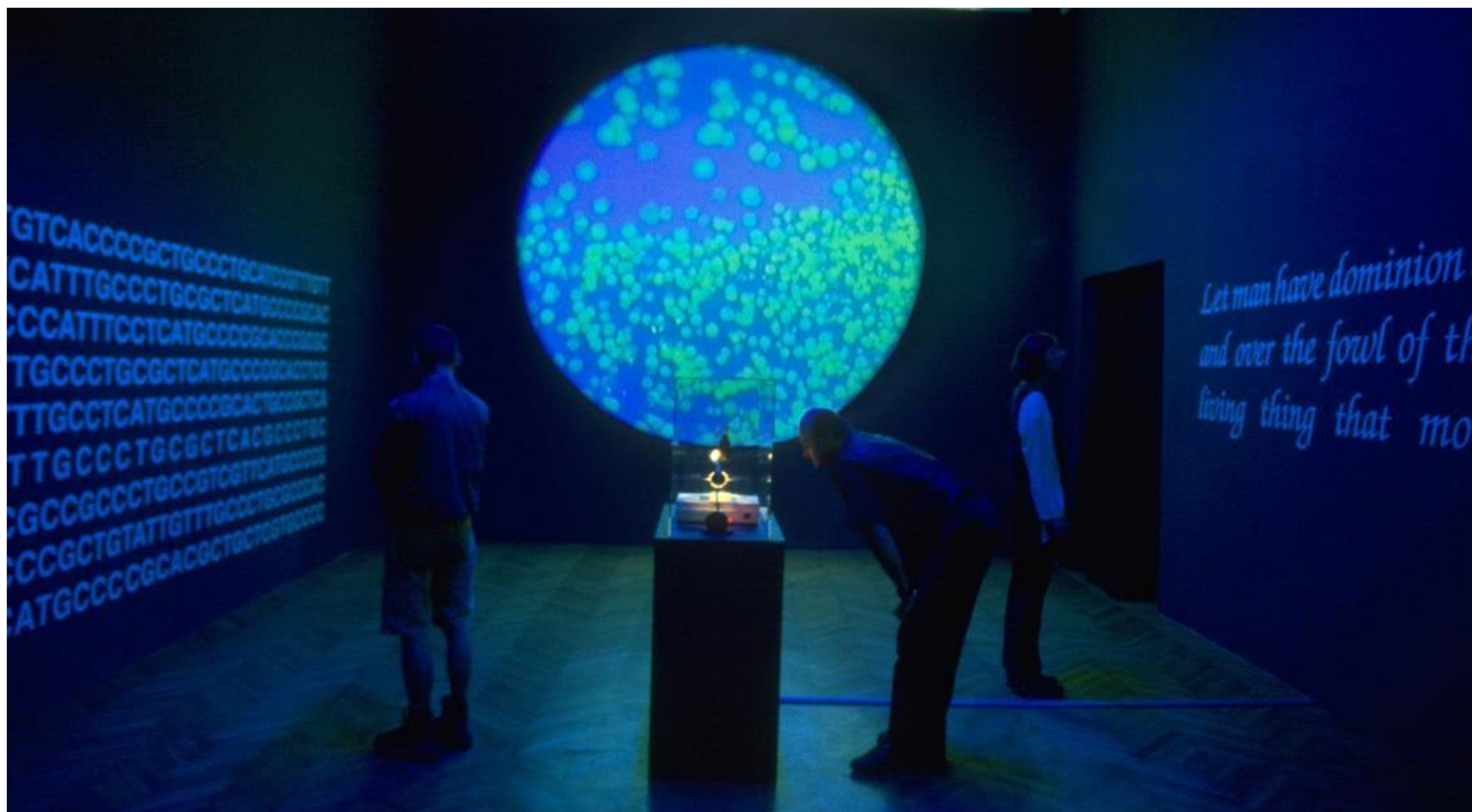


Рис 21.6. Инсталляция Genesis

(слева - цитата в виде ДНК; в центре - проекция чашки Петри с бактериями; справа - цитата на английском языке)

ДНК-молекулы являются компактным и надежным носителем информации. Группа ученых Гарварда подсчитала, что память из структур ДНК весом всего 4 грамма теоретически может хранить всю информацию, которую производит все человечество современности за один год. В пользу надежности говорит тот факт, что информация из ДНК может быть считана спустя сотни тысяч и даже миллионы лет. "ДНК можно хранить в далеко не идеальных условиях - к примеру, в мертвых животных. При этом она сохранится, и через 400 тыс. лет мы всё еще способны ее считать, - рассказывает руководитель исследований профессор Джордж Чёрч (George Church) из Гарвардской медицинской школы (США). - Запись в ДНК будет храниться куда дольше, чем на диске Blu-ray" [41].

Для кодирования информации ученые из Гарварда использовали специальный струйный принтер, который помещает короткие фрагменты химически синтезированной ДНК на поверхность крошечного стеклянного чипа. Имитируя двоичный код, исследователи использовали А (аденин) и С (цитозин) в качестве 0, а G (гуанин) и Т (тимин) – в качестве 1. Генетический код использовали, чтобы записать содержимое книги Дж. Чёрча "Регенезис. Как синтетическая биология заново придумает природу и нас" ("Regenesis: How Synthetic Biology Will Reinvent Nature And Ourselves"), состоящей из 53 тыс. слов и 11 изображений (≈ 300 страниц). 70 млрд. копий книги были "напечатаны" на ДНК-чипе, примерно равным ногтю мизинца.

Надежность и компактность ДНК-молекул делает их весьма перспективным объектом для применения в стеганографических целях. Ведь носителем секретной информации может являться человек, растение, бактерии и вирусы (причем как живые, так и мертвые). Поиск секретной информации в теле взрослого человека, в котором $\approx 3,5 \cdot 10^{16}$ молекул ДНК, на современном уровне развития науки и техники нереален.

Литературные приемы.

Хорошо известны различного рода литературные приемы, предназначенные для сокрытия тайной информации во внешне безобидных посланиях.

А) Пустышечный шифр [13]. При использовании данного шифра (точнее метода) слова или буквы секретного сообщения записываются в определенных позициях. Например, читаются каждое пятое слово или первая буква каждого слова, в то время как все остальные буквы или слова служат в качестве «пустышек» для сокрытия значимого текста. Во время Второй мировой войны пустышечные шифры в большинстве случаев применяли не шпионы, а вполне лояльные американцы, которые не могли устоять перед искушением «надуть» цензора. Особенно часто этим занимались военнослужащие, которые пытались сообщить о своем местонахождении семьям, которые ничего не знали о том, где находится их родственник. Одна такая система, несмотря на свою примитивность, привела получателей сообщения в состояние полного недоумения. Молодой американский солдат, пользуясь заранее условленной системой переписки со своими родителями, пытался довести до их сведения, что находится в Тунисе. Для этого в пяти письмах домой в качестве второго инициала своего отца он использовал сначала «Т», затем «У», «Н», «И» и «С». К несчастью, эти письма были получены в другом порядке, а беспечный солдат забыл проставить на письмах даты. Обезумевшие родители написали ему, что они перерыли весь свой атлас, но нигде не смогли найти «Нутси»! В 1943 г. подобные попытки настолько участились, что руководству ВМС США пришлось предупредить моряков о том, что пользование «семейными кодами» может привести к суровому наказанию.

Б) Акrostих. Тайное послание состоит из первых букв строк стихотворений. Принято считать, что акrostих впервые применил известный древнегреческий комедиограф, философ и врач Эпихарм Сиракузский (V век до н.э.). Первоначально функцией акrostиха была фиксация имени автора в тексте его произведения. Затем эта функция расширилась, в них начали передавать скрытые послания, нравоучения и т.д. Разновидностями акrostиха можно считать более редкие **телестих** и **месостих**, в которых дополнительный текст читается не по первым, а по последним и средним буквам стихотворной строки.

В) Решётка Кардано [14, 15, 17, 43]. Решетка, предложенная Кардано, представляла собой картонный или деревянный трафарет, в котором через неправильные интервалы сделаны прямоугольные вырезы. Накладывая этот трафарет на лист бумаги, можно было записывать в вырезы секретное сообщение (букву, слог или целое слово). После этого начиналась тяжелая работа по придумыванию правдоподобных и выглядящих безобидными посланий.

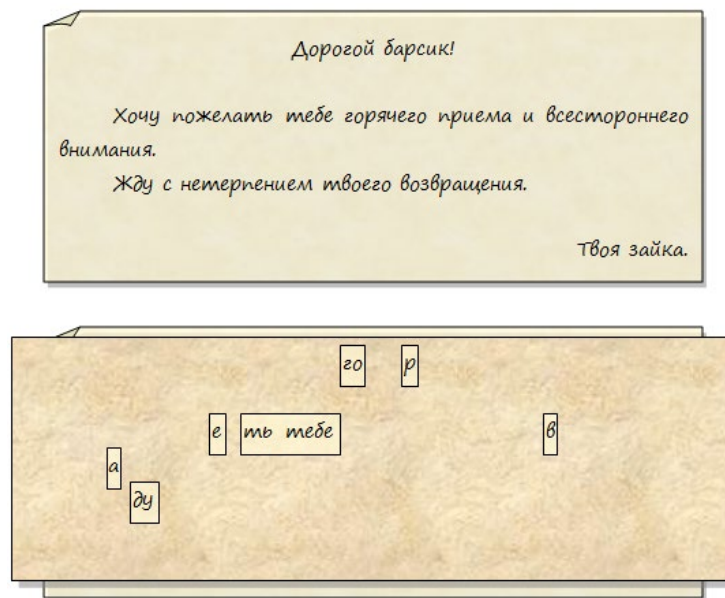


Рис 21.7. Пример использования решетки Кардано

Данный стеганографический метод использовал при переписке кардинал Ришелье. Подобным методом пользовался также известный русский писатель, общественный деятель и дипломат А.С. Грибоедов. Будучи послом в Персии, он писал своей жене «невинные» послания, которые, попав в руки жандармерии, для которой и были предназначены, расшифровывались по соответствующей «решетке» и передавались царскому правительству уже как секретные сведения. Пример использования решетки Кардано можно было также видеть в титрах легендарного советского сериала о Шерлоке Холмсе.

Г) Аллюзия (лат. *allusio* – шутка, намёк) или **жаргонный код**. Данный литературный прием заключается в использовании фраз, которые предполагаются известными тому, к кому обращена речь, и неизвестными посторонним лицам. Знаменитые фразы, которые передали по радио, – «Над всей Испанией чистое небо» (сигнал к началу франкистского путча в Испании, 17 июля 1936 г.) и «В Сантьяго идет дождь» (сигнал к началу военного переворота в Чили, 11 сентября 1973 г.) – знают даже школьники.

После нападения Японии Соединенные Штаты создали собственный орган цензуры. Вскоре его штат насчитывал около 15 тысяч сотрудников, которые размещались в 90 зданиях по всей стране, проверяли ежедневно около миллиона писем, подслушивали бесчисленное множество телефонных разговоров, просматривали кинофильмы, газеты, журналы и знакомились со сценариями радиопередач. Миллионы американцев получали письма в конвертах со следами ножиц цензора и штампом "Вскрыто цензурой" [13].

Чтобы перекрыть максимальное число стеганографических каналов связи, американская цензура категорически запретила отправку по почте целого ряда сообщений. Были отменены шахматные партии по переписке. Из писем вымарывались кроссворды, так как у цензоров не хватало времени решать их, чтобы проверить, не содержат ли они тайные послания. Из почтовых отправлений изымались газетные вырезки, потому что они могли содержать секретный текст. Не разрешалось пересылать по почте табели успеваемости учащихся. Одно письмо с инструкциями по вязанию было задержано до тех пор, пока цензор не связал по ним свитер, чтобы проверить, не содержат ли они какой-либо скрытой информации. В каждом цензурном отделении имелся запас марок: цензоры снимали подозрительные марки и заменяли их другими того же достоинства, но с иным номером и рисунком. Чистая бумага, которую жители США часто посылали своим родственникам, проживавшим в странах, где не хватало бумаги, также заменялась из соответствующих запасов, чтобы исключить применение симпатических чернил. Конфисковывались даже детские рисунки, которые родители слали дедушкам и бабушкам, так как среди этих рисунков могли попасться закодированные карты или схемы.

Один из сотрудников нью-йоркского отделения цензуры обратил внимание на письмо из Германии, в котором говорилось, что Гертруда добилась выдающихся успехов в плавании, и перечислялись ее победные результаты. Сотрудник проконсультировался со знакомым любителем плавания, и тот ответил, что подобных результатов человек достичь не в состоянии. В ходе дальнейшего расследования было установлено, что в действительности речь шла о скорости нового американского истребителя, характеристики которого разболтал хвастливый работник военного министерства.

Телеграммы с заказами на цветы ("Вручите субботу моей жене три белые орхидеи") предоставляли настолько удобную возможность для передачи секретной информации, что цензоры запретили указывать в них названия цветов и день вручения.

Служба цензуры отменила телефонные и телеграфные заказы на исполнение по радио тех или иных музыкальных произведений, а выполнение заявок, присланных по почте, велела задерживать на неопределенное время. Эти меры должны были исключить возможность передачи сообщения для подводных лодок противника с помощью модной песенки. Аналогичные меры были приняты в отношении передачи радиостанциями объявлений личного характера.

Изучением методов скрытия информации в тексте занимается **энигматология** – "учение о тайне" (греч. *αἰνυτια* – загадка). Текст, содержащий "тайное сообщение" – **эниграмма**. **Энигмализирование** – извлечение тайного смысла из текста.

Семаграммы.

Семаграмма (греч. *sema* – знак и *gramma* – написанный, нарисованный) – тайное сообщение, в котором секретными кодозаменами являются любые символы, кроме букв и цифр [13].

Секретными кодозаменами могут быть:

- точки на костяшках домино;
- предметы на фотографии, расположенные таким образом, чтобы передать заранее оговоренный смысл;
- вышитые на платье узоры, представляющие собой закодированное послание;
- картина, на которой длинные и короткие ветки деревьев представляют точки и тире азбуки Морзе;
- и т.п.

Однажды в нью-йоркском цензурном отделении перевели все стрелки в предназначенной для отправки партии часов, опасаясь, что их положение может заключать в себе какое-то сообщение [13, 43].

Во время Второй мировой войны был зарегистрирован случай, когда немецкие агенты в Англии послали в Германию свое донесение под видом связанного свитера. Он якобы предназначался для заключенного, но вместо этого попал к контрразведчикам. Когда свитер распустили, оказалось, что его шерстяные нитки были сплошь в узелках. Пряжу расправили, а узлы сопоставили с алфавитом, написанным вертикально на стене. Базисной линией был выбран пол, а алфавит располагался перпендикулярно к нему. Вначале на полу под алфавитом крепился конец пряжи, при этом первый узел оказывался рядом с одной из букв. Затем, прижав к полу первый узел, определяли, с какой буквой совместится второй узел, и т.д. Таким образом, шифрование (точнее кодировка) были выполнены по аналогии с «линейкой Энея». В какой-то момент узлы «поведали» о строящихся и уже готовых к спуску на воду военных кораблях союзников [43].

¹**Штамм** (от нем. Stamm - «основа») - чистая культура вирусов, бактерий, других микроорганизмов или культура клеток, изолированная в определенное время и в определенном месте.

²**Микрон** (микромметр, мкм) - 10⁻⁶м. Толщина человеческого волоса - 80-110 мкм.

21.3. Компьютерная стеганография

Развитие компьютерной технологии и средств коммуникации придали новый импульс развитию и совершенствованию стеганографии. Сегодня каждый может воспользоваться теми преимуществами, которые дает стеганография как в области скрытой передачи информации, что особенно полезно в странах, где существует запрет на стойкие средства криптографии, так и в области защиты авторских прав. В настоящее время методы компьютерной стеганографии активно используются для решения следующих задач.

1. Защита конфиденциальной информации от несанкционированного доступа. Это область использования компьютерной стеганографии является наиболее эффективной при решении проблем защиты конфиденциальной информации. Так, например, объем секретного сообщения в звуковых и графических файлах может составлять до 25 - 30 % от размера файла. Причем аудиовизуальные изменения таковы, что не обнаруживаются при прослушивании и просмотре файлов большинством людей, даже если факт сокрытия известен.

2. Преодоление систем мониторинга и управления сетевыми ресурсами. Стеганографические методы позволяют противостоять попыткам контроля над информационным пространством при прохождении информации через серверы управления локальных и глобальных вычислительных сетей.

3. Камуфлирование программного обеспечения. Применяется в тех случаях, когда использование ПО незарегистрированными пользователями является нежелательным. ПО может быть закомуфлировано под стандартные универсальные программные продукты (например, текстовые редакторы) или скрыто в файлах мультимедиа и использоваться только лицами, имеющими на это права.

4. Защита авторских прав. Одним из наиболее перспективных направлений компьютерной стеганографии является технология использования **цифровых водяных знаков ЦВЗ** (digital watermarking) – в данном случае, создание невидимых глазу знаков защиты авторских прав на графические и аудио файлы. Такие ЦВЗ, помещенные в файл, могут быть распознаны специальными программами, которые извлекут из файла много полезной информации: когда создан файл, кто владеет авторскими правами, как вступить в контакт с автором и т.д. При том повальном воровстве, которое происходит в Интернете, польза от такой технологии очевидна.

Сегодня на рынке существует довольно много фирм, предлагающих продукты для создания и детектирования водяных знаков. Один из лидеров - фирма Digimarc. Ее продуктами, если верить предоставленной самой фирмой информации, пользуются более миллиона официальных клиентов: дизайнеры, художники, онлайн-овые галереи, журнал Playboy. Специальные поисковые агенты сканируют ресурсы Интернет, просматривая картинки на наличие ЦВЗ, и сообщают владельцам о фактах использования их собственности.

Несмотря на все заверения создателей соответствующих продуктов, ЦВЗ оказались нестойкими. Они могут перенести многое - изменение яркости и контраста, использование спецэффектов, даже печать и последующее сканирование, но они не могут перенести воздействие специальных программ-стирателей, которые появились в Интернете.

Наиболее известные методы компьютерной стеганографии и их характеристика приведены в следующей таблице.

Таблица 21.2. Методы компьютерной стеганографии и их характеристика

Стеганографические методы	Краткая характеристика методов	Примечания
1. Методы, основанные на использовании специальных свойств носителей данных		
1.1. Скрытие информации в неиспользуемых местах дисков	1. Используются дорожки, доступные для чтения, но не воспринимаемые ОС (например, в резервную область жесткого диска). 2. Запись в неиспользуемые места оптических дисков (CD, DVD, Blue-ray и т.д.)	1. Низкая степень скрытности. 2. Возможна передача больших объемов информации.
1.2. Нанесение дополнительных дорожек на гибкие магнитные диски (вышли из употребления)	Т.к. ширина дорожки в несколько раз меньше расстояния между дорожками (для гибких магнитных дисков), то на диск можно нанести дополнительные дорожки и записать туда информацию, не доступную ОС.	Возможна передача больших объемов информации.
1.3. Специальное форматирование дисков	Форматирование диска под размер секторов отличный от принятого в ОС.	1. Наличие программ как форматирующих подобным образом диски, так и читающих любое форматирование. 2. Возможна передача больших объемов информации.
2. Методы, основанные на использовании специальных свойств форматов данных		
2.1. Методы использования полей данных, зарезервированных для расширения	Поля расширения имеются во многих мультимедийных форматах. Они заполняются нулевой информацией и не учитываются программой.	1. Низкая степень скрытности. 2. Передача небольших объемов информации.
	1. Использование смещения символов, слов, предложений или абзацев в тексте (можно обеспечить вставкой дополнительных пробелов).	1. Слабая производительность

2.2. Методы специального форматирования в текстовых документах	2. Выбор определенных позиций символов (например, акростих). 3. Использование дополнительных возможностей форматирования текстов (например, использование в MS Word: скрытого текста; специальных шрифтов; символов определенного шрифта, размера или цвета; белого цвета для символов и фона; одного пробела между словами для кодирования "0" и двух – для кодирования "1" и т.д.).	методов. 2. Передача небольших объемов информации. 3. Низкая степень скрытности.
2.3. Методы специального форматирования текстов при печати	1. Печать специальными шрифтами, символами определенного шрифта, размера или цвета. 2. Внесение малозаметных искажений информации при печати (Был использован при печати контрактов с клиентами в одной из московских компаний. Эта тайнопись выглядела как обычные незначительные дефекты печати и обеспечивала определенную степень подтверждения подлинности документа).	1. Слабая производительность методов. 2. Передача небольших объемов информации.
2.4. Скрытие информации в свободных областях диска	1. Использование свободной части последнего кластера файла. 2. Использование свободных кластеров без записи в таблицы размещения файлов информации о том, что в этих кластерах содержится информация.	1. Низкая степень скрытности. 2. Возможна передача больших объемов информации.
2.5. Использование особенностей файловой системы	1. Использование скрытых файлов. 2. Использование потоков в NTFS.	1. Низкая степень скрытности. 2. Возможна передача больших объемов информации.
3. Методы, основанные на использовании избыточности аудио- и видеoinформации		
3.1. Методы использования избыточности мультимедийных форматов	Младшие разряды байт, несущие информацию об интенсивности света и звука содержат очень мало полезной информации. Их заполнение практически не влияет на качество восприятия.	1. За счет введения дополнительной информации искажаются статистические характеристики цифровых потоков. 2. Для снижения компрометирующих признаков требуется коррекция статистических характеристик. 3. Возможна передача больших объемов информации.

Использование потоков в NTFS.

Любой файл в NTFS может содержать несколько потоков ("файлов"). Каждый файл NTFS содержит стандартный (default) или безымянный (unnamed) поток данных (data stream). Именно этот поток видит перед собой пользователь, открывающий файл в текстовом редакторе. И именно размер этого потока отображается в качестве размера файла. Альтернативный поток данных (alternate data stream) – файл, встраиваемый в другой. Ему может даваться любое имя и его размер не влияет на размер файла.

В частности, информация о файле с вкладки "Сводка" окна "Свойства" храниться в альтернативном потоке "SummaryInformation"

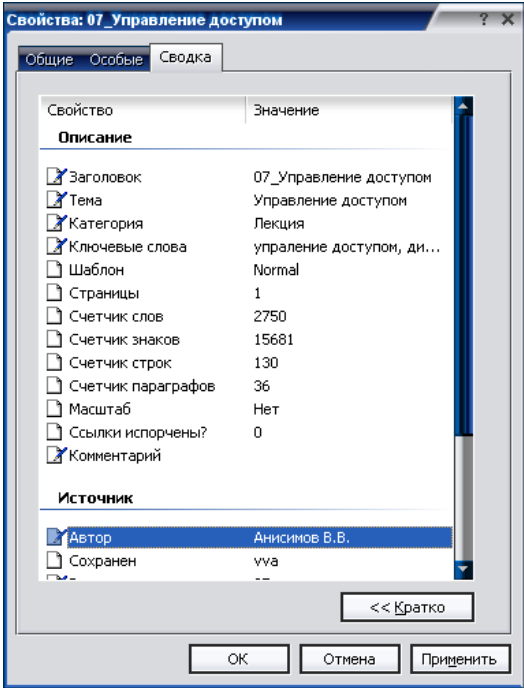


Рис 21.8. Свойства файла

Работа с потоками командами DOS.

Копирование файла "СовСек.txt" в альтернативный поток "ss" файла "HeСек.txt".

```
type СовСек.txt > HeСек.txt:ss
```

После копирования размер файла "HeСек.txt" не меняется.

Шутка. Таким образом, в файл размером 0 байт, можно записать несколько Гбайт мусора в потоки, заняв почти все место на диске, но файл по-прежнему будет иметь размер 0 байт.

Восстановление текстового файла из потока.

```
more < HeСек.txt:ss > СовСек.txt
```

Для выявления файлов, обладающих альтернативными потоками можно воспользоваться утилитой Streams (<http://technet.microsoft.com/ru-ru/sysinternals>, с исходным текстом утилиты на C).

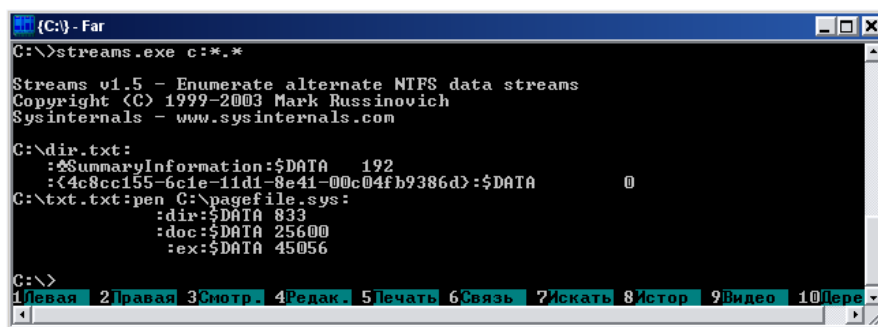


Рис 21.9. Отображение потоков утилитой Streams

Кроме легкого обнаружения, другим существенным недостатком является возможность использования данного способа только на дисках с NTFS. При копировании файлов на диски с другой файловой системой альтернативные потоки теряются.

Использование избыточности аудио- и видеофайлов.

Из всех приведенных в табл. 21.2 методов, этот является наиболее перспективным. Существуют различные его модификации, самый простой из которых LSB (Least Significant Bit, наименьший значащий бит). Суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Допустим, имеется 8-битное изображение в градациях серого (0 (00000000₂) обозначает черный цвет, 255 (11111111₂) – белый). Всего имеется 256 градаций. Также предположим, что сообщение состоит из 1 байта – например, (01101011₂). При использовании 2 младших бит в описании пикселей, нам потребуется 4 пикселя. Допустим, они черного цвета. Тогда пиксели, содержащие скрытое сообщение, будут выглядеть следующим образом: (00000001 00000010 00000010 00000011₂). Тогда цвет пикселей изменится: первого - на 1/256, второго и третьего - на 2/256 и четвертого - на 3/256. Такие искажения исходного изображения, как правило, незаметны для человеческого зрения. Для разноцветных изображений искажения еще менее заметны, тем более, что в них биты исходного изображения могут совпадать с битами секретного сообщения.

Одной из лучших программ в своем классе является SecretBMP (<http://www.bordak.fatal.ru/secretbmp/>). В примере при скрытии файла give-me-too.zip (570 404 байта) в файле 5tr500.bmp (1 229 852 байта) размер результирующего файла 5.bmp стал 1 229 850 байта, а качество рисунка осталось неизменным для глаза.

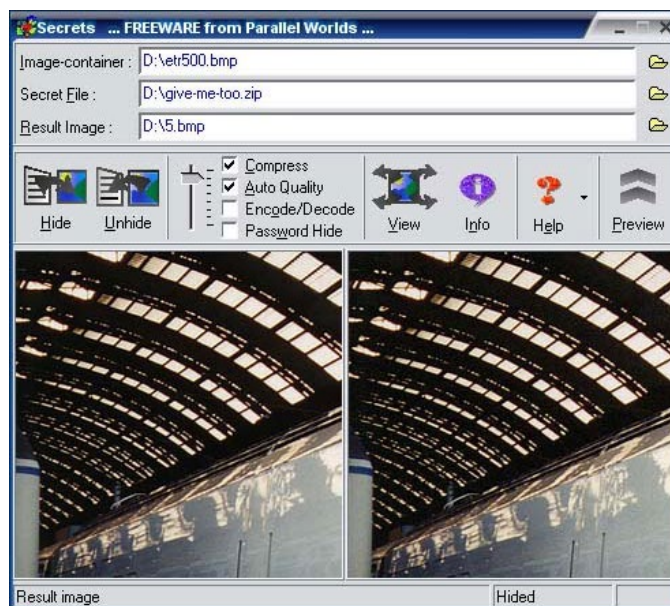


Рис 21.9. Окно программы SecretBMP
(слева – исходный файл-контейнер, справа – файл со вставленной секретной информацией)

Вопросы для самопроверки

1. Перечислите основные методы классической стеганографии и дайте им характеристику.
2. В каких целях применяется компьютерная стеганография?
3. Опишите метод сокрытия информации с помощью потоков NTFS.
4. За счет чего достигается сокрытие информации в аудио- и видеофайлах?

22.1. Общие сведения

Кодирование – представление информации в альтернативном виде. По своей сути кодовые системы (или просто коды) аналогичны шифрам однозначной замены, в которых элементам кодируемой информации соответствуют кодовые обозначения. Отличие заключается в том, что в шифрах присутствует переменная часть (ключ), которая для определенного исходного сообщения при одном и том же алгоритме шифрования может выдавать разные шифртексты. В кодовых системах переменной части нет. Поэтому одно и то же исходное сообщение при кодировании, как правило, всегда выглядит одинаково¹. Другой отличительной особенностью кодирования является применение кодовых обозначений (замен) целиком для слов, фраз или чисел (совокупности цифр). Замена элементов кодируемой информации кодовыми обозначениями может быть выполнена на основе соответствующей таблицы (наподобие таблицы шифрозамен) либо определена посредством функции или алгоритма кодирования.

В качестве **элементов кодируемой информации** могут выступать:

- буквы, слова и фразы естественного языка;
- различные символы, такие как знаки препинания, арифметические и логические операции, операторы сравнения и т.д. Следует отметить, что сами знаки операций и операторы сравнения – это кодовые обозначения;
- числа;
- аудиовизуальные образы;
- ситуации и явления;
- наследственная информация;
- и т.д.

Кодовые обозначения могут представлять собой:

- буквы и сочетания букв естественного языка;
- числа;
- графические обозначения;
- электромагнитные импульсы;
- световые и звуковые сигналы;
- набор и сочетание химических молекул;
- и т.д.

Кодирование может выполняться в **целях**:

- удобства хранения, обработки и передачи информации (как правило, закодированная информация представляется более компактно, а также пригодна для обработки и передачи автоматическими программно-техническими средствами);
- удобства информационного обмена между субъектами;
- наглядности отображения;
- идентификации объектов и субъектов;
- сокрытия секретной информации;
- и т.д.

Кодирование информации бывает **одно-** и **многоуровневым**. Примером одноуровневого кодирования служат световые сигналы, подаваемые светофором (красный – стой, желтый – приготовиться, зеленый – вперед). В качестве многоуровневого кодирования можно привести представление визуального (графического) образа в виде файла фотографии. Вначале визуальная картинка разбивается на составляющие элементарные элементы (пиксели), т.е. каждая отдельная часть визуальной картинки кодируется элементарным элементом. Каждый элемент представляется (кодируется) в виде набора элементарных цветов (RGB: англ. red – красный, green – зеленый, blue – синий) соответствующей интенсивностью, которая в свою очередь представляется в виде числового значения. Впоследствии наборы чисел, как правило, преобразуются (кодируются) с целью более компактного представления информации (например, в форматах jpeg, png и т.д.). И наконец, итоговые числа представляются (кодируются) в виде электромагнитных сигналов для передачи по каналам связи или областей на носителе информации. Следует отметить, что сами числа при программной обработке представляются в соответствии с принятой системой кодирования чисел.

Кодирование информации может быть **обратимым** и **необратимым**. При обратимом кодировании на основе закодированного сообщения можно однозначно (без потери качества) восстановить кодируемое сообщение (исходный образ). Например, кодирование с помощью азбуки Морзе или штрихкода. При необратимом кодировании однозначное восстановление исходного образа невозможно. Например, кодирование аудиовизуальной информации (форматы jpg, mp3 или avi) или хеширование.

Различают **общедоступные** и **секретные** системы кодирования. Первые используются для облегчения информационного обмена, вторые – в целях сокрытия информации от посторонних лиц.

¹В некоторых секретных кодовых системах присутствуют элементы, позволяющие получать разные закодированные сообщения для определенного

исходного сообщения (аддитивные числа, многозначные замены, правила перешифрования).

22.2. Общедоступные кодовые системы

Применение кодов нашло широкое применение в общественной жизни. Как отмечалось выше, даже сами знаки арифметических и логических операций – это кодовые обозначения. В частности, знак «+» для операции сложения (а также знак «-») придумали в немецкой математической школе «коссистов» (т.е. алгебраистов). Они используются в «Арифметике» Иоганна Видмана, изданной в 1489 г. До этого сложение обозначалось буквой p (plus) или латинским словом et (союз «и»), а вычитание - буквой m (minus). У Видмана символ плюса заменяет не только сложение, но и союз «и» [17]. Если «копать еще глубже», то буква «A» - это кодовое обозначение для соответствующего звука.

В качестве других распространенных кодовых систем можно привести:

- дорожные знаки;
- обозначение химических элементов из периодической таблицы Дмитрия Ивановича Менделеева;
- знаки зодиака;
- сокращенные наименования дисциплин в расписании занятий студентов.

Ниже приводится описание других общедоступных кодовых систем в целях иллюстрации многообразия их назначения и способов представления кодовых обозначений [17].

Азбука Морзе - способ кодирования символов (букв алфавита, цифр, знаков препинания и др.) с помощью последовательности «точек» и «тире». За единицу времени принимается длительность одной точки. Длительность тире равна трём точкам. Пауза между элементами одного знака - одна точка (около 1/25 доли секунды), между знаками в слове - 3 точки, между словами - 7 точек. Назван в честь американского изобретателя и художника Сэмюэля Морзе.

Русская буква	Латинская буква	Код Морзе	Русская буква	Латинская буква	Код Морзе	Символ	Код Морзе
А	A	· —	Р	R	· — ·	1	· — — — —
Б	B	— · · ·	С	S	· · ·	2	· · — — —
В	W	· — —	Т	T	—	3	· · · — —
Г	G	— — ·	У	U	· · —	4	· · · · —
Д	D	— · ·	Ф	F	· · — ·	5	· · · · ·
Е (Ё)	E	·	Х	H	· · · ·	6	— · · · ·
Ж	V	· · · —	Ц	C	— · — ·	7	— — — · ·
З	Z	— — — ·	Ч	O	— — — ·	8	— — — — ·
И	I	· ·	Ш	CH	— — — —	9	— — — — ·
Й	J	· — — — —	Щ	Q	— — — · —	0	— — — — —
К	K	— · —	Ъ	N	— — · — —	Точка	· · · · ·
Л	L	· — · ·	Ы	Y	— · — — —	Запятая	· — · — — —
М	M	— —	Ь (Ъ)	X	— · · — —	—	· · — — — ·
Н	N	— ·	Э	E	· · — · ·	!	— — — · · — —
О	O	— — — —	Ю	U	· · — — —	@	· — — — · ·
П	P	· — — — ·	Я	A	· — — — —	Конец связи (end contact)	· · — — —

Рис.22.1. Фрагмент азбуки Морзе

Изначально азбука Морзе применялась для передачи сообщений в телеграфе. При этом точки и тире передавались в виде электрических сигналов, проходящих по проводам. В настоящий момент азбуку Морзе, как правило, используют в местах, где другие средства обмена информации недоступны (например, в тюрьмах).

Любопытный факт связан с изобретателем первой лампочки Томасом Альвой Эдисоном (1847-1931 гг.). Он плохо слышал и общался со своей женой, Мэри Стюэлл, с помощью азбуки Морзе. Во время ухода Эдисон сделал предложение, отстучав слова рукой, и она ответила тем же способом. Телеграфный код стал обычным средством общения для супругов. Даже когда они ходили в театр, Эдисон клал руку Мэри себе на колено, чтобы она могла «телеграфировать» ему диалоги актеров [44].

Код Бодо - цифровой 5-битный код. Был разработан Эмилем Бодо в 1870 г. для своего телеграфа. Код вводился прямо клавиатурой, состоящей из пяти клавиш, нажатие или ненажатие клавиши соответствовало передаче или непередаче одного бита в пятибитном коде. Существует несколько разновидностей (стандартов) данного кода (CCITT-1, CCITT-2, МТК-2 и др.) В частности МТК-2 представляет собой модификацию международного стандарта CCITT-2 с добавлением букв кириллицы.

Управляющие символы		
Двоичный код	Десятичный код	Назначение
01000	8	Возврат каретки
00010	2	Перевод строки
11111	31	Буквы латинские
11011	27	Цифры

00100	4	Пробел		
00000	0	Буквы русские		
Буквы, цифры и остальные символы				
Двоичный код	Десятичный код	Латинская буква	Русская буква	Цифры и прочие символы
00011	3	A	А	-
11001	25	B	Б	?
01110	14	C	Ц	:
01001	9	D	Д	Кто там?
00001	1	E	Е	3
01101	13	F	Ф	Э
11010	26	G	Г	Ш
10100	20	H	Х	Щ
00110	6	I	И	8
01011	11	J	Й	Ю
01111	15	K	К	(
10010	18	L	Л	)
11100	28	M	М	.
01100	12	N	Н	,
11000	24	O	О	9
10110	22	P	П	0
10111	23	Q	Я	1
01010	10	R	Р	4
00101	5	S	С	'
10000	16	T	Т	5
00111	7	U	У	7
11110	30	V	Ж	=
10011	19	W	В	2
11101	29	X	Ь	/
10101	21	Y	Ы	6
10001	17	Z	З	+

Рис.22.2. Стандарт кода Бодо МТК-2

На следующем рисунке показана телетайпная перфолента с сообщением, переданным с помощью кода Бодо.

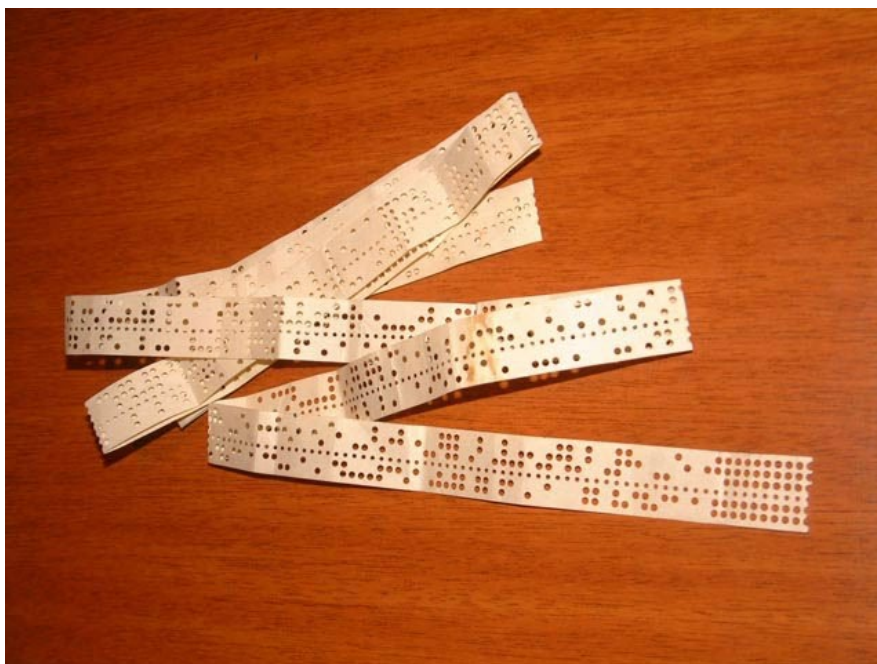


Рис. 22.3. Перфолента с кодом Бодо

Следует отметить два интересных факта, связанных с кодом Бодо.

1. Сотрудники телеграфной компании AT&T Гильберто Вернам и Мейджор Джозеф Моборн в 1917 г. предложили идею автоматического шифрования

телеграфных сообщений на основе кода Бодо. Шифрование выполнялось методом гаммирования по модулю 2.

2. Соответствие между английским и русским алфавитами, принятое в МТК-2, было использовано при создании компьютерных кодировок КОИ-7 и КОИ-8.

ASCII и Unicode.

ASCII (англ. American Standard Code for Information Interchange) - американская стандартная кодировочная таблица для печатных и управляющих символов. Изначально была разработана как 7-битная для представления 128 символов, при использовании в компьютерах на символ выделялось 8 бит (1 байт), где 8-ой бит служил для контроля целостности (бит четности). Позднее, с задействованием 8 бита для представления дополнительных символов (всего 256 символов), например букв национальных алфавитов, стала восприниматься как половина 8-битной. В частности на основе ASCII были разработаны кодировки, содержащие буквы русского алфавита: для операционной системы MS-DOS - cp866 (англ. code page – кодовая страница), для операционной системы MS Windows – Windows 1251, для различных операционных систем – КОИ-8 (код обмена информацией, 8 битов), ISO 8859-5 и другие.

Кодировка ASCII						Дополнительные символы					
Двоичный код	Десятичный код	Символ	Двоичный код	Десятичный код	Символ	Двоичный код	Десятичный код	Символ	Двоичный код	Десятичный код	Символ
00000000	0	NUL	01000000	64	@	10000000	128	Ђ	11000000	192	А
00000001	1	SOH	01000001	65	A	10000001	129	Ѓ	11000001	193	Б
00000010	2	STX	01000010	66	B	10000010	130	,	11000010	194	В
00000011	3	ETX	01000011	67	C	10000011	131	ѓ	11000011	195	Г
00000100	4	EOT	01000100	68	D	10000100	132	„	11000100	196	Д
00000101	5	ENQ	01000101	69	E	10000101	133	...	11000101	197	Е
00000110	6	ACK	01000110	70	F	10000110	134	ђ	11000110	198	Ж
00000111	7	BEL	01000111	71	G	10000111	135	‡	11000111	199	З
00001000	8	BS	01001000	72	H	10001000	136	€	11001000	200	И
00001001	9	HT	01001001	73	I	10001001	137	‰	11001001	201	Й
00001010	10	LF	01001010	74	J	10001010	138	Љ	11001010	202	К
00001011	11	VT	01001011	75	K	10001011	139	‹	11001011	203	Л
00001100	12	FF	01001100	76	L	10001100	140	Њ	11001100	204	М
00001101	13	CR	01001101	77	M	10001101	141	Ћ	11001101	205	Н
00001110	14	SO	01001110	78	N	10001110	142	Ќ	11001110	206	О
00001111	15	SI	01001111	79	O	10001111	143	Џ	11001111	207	П
00010000	16	DLE	01010000	80	P	10010000	144	ђ	11010000	208	Р
00010001	17	DC1	01010001	81	Q	10010001	145	‘	11010001	209	С
00010010	18	DC2	01010010	82	R	10010010	146	’	11010010	210	Т
00010011	19	DC3	01010011	83	S	10010011	147	“	11010011	211	У
00010100	20	DC4	01010100	84	T	10010100	148	”	11010100	212	Ф
00010101	21	NAK	01010101	85	U	10010101	149	•	11010101	213	Х
00010110	22	SYN	01010110	86	V	10010110	150	–	11010110	214	Ц
00010111	23	ETB	01010111	87	W	10010111	151	—	11010111	215	Ч
00011000	24	CAN	01011000	88	X	10011000	152		11011000	216	Ш
00011001	25	EM	01011001	89	Y	10011001	153	™	11011001	217	Щ
00011010	26	SUB	01011010	90	Z	10011010	154	љ	11011010	218	Ъ
00011011	27	ESC	01011011	91	[	10011011	155	›	11011011	219	Ы
00011100	28	FS	01011100	92	\	10011100	156	њ	11011100	220	Ь
00011101	29	GS	01011101	93	]	10011101	157	ќ	11011101	221	Э
00011110	30	RS	01011110	94	^	10011110	158	ћ	11011110	222	Ю
00011111	31	US	01011111	95	_	10011111	159	џ	11011111	223	Я
00100000	32		01100000	96	`	10100000	160		11100000	224	а
00100001	33	!	01100001	97	a	10100001	161	Ÿ	11100001	225	б
00100010	34	"	01100010	98	b	10100010	162	ŷ	11100010	226	в
00100011	35	#	01100011	99	c	10100011	163	Ј	11100011	227	г
00100100	36	\$	01100100	100	d	10100100	164	Ѡ	11100100	228	д
00100101	37	%	01100101	101	e	10100101	165	Ѓ	11100101	229	е
00100110	38	&	01100110	102	f	10100110	166	Ѕ	11100110	230	ж
00100111	39	'	01100111	103	g	10100111	167	§	11100111	231	з
00101000	40	(	01101000	104	h	10101000	168	Ё	11101000	232	и
00101001	41	)	01101001	105	i	10101001	169	©	11101001	233	й
00101010	42	*	01101010	106	j	10101010	170	€	11101010	234	к
00101011	43	+	01101011	107	k	10101011	171	«	11101011	235	л

00101100	44	,	01101100	108	l	10101100	172	¬	11101100	236	м
00101101	45	-	01101101	109	m	10101101	173	¬	11101101	237	н
00101110	46	.	01101110	110	n	10101110	174	®	11101110	238	о
00101111	47	/	01101111	111	o	10101111	175	İ	11101111	239	п
00110000	48	0	01110000	112	p	10110000	176	°	11110000	240	р
00110001	49	1	01110001	113	q	10110001	177	±	11110001	241	с
00110010	50	2	01110010	114	r	10110010	178	I	11110010	242	т
00110011	51	3	01110011	115	s	10110011	179	i	11110011	243	у
00110100	52	4	01110100	116	t	10110100	180	ı	11110100	244	ф
00110101	53	5	01110101	117	u	10110101	181	µ	11110101	245	х
00110110	54	6	01110110	118	v	10110110	182	¶	11110110	246	ц
00110111	55	7	01110111	119	w	10110111	183	·	11110111	247	ч
00111000	56	8	01111000	120	x	10111000	184	ë	11111000	248	ш
00111001	57	9	01111001	121	y	10111001	185	№	11111001	249	щ
00111010	58	:	01111010	122	z	10111010	186	є	11111010	250	ъ
00111011	59	;	01111011	123	{	10111011	187	»	11111011	251	ы
00111100	60	<	01111100	124		10111100	188	j	11111100	252	ь
00111101	61	=	01111101	125	}	10111101	189	S	11111101	253	э
00111110	62	>	01111110	126	~	10111110	190	s	11111110	254	ю
00111111	63	?	01111111	127	DEL	10111111	191	ï	11111111	255	я

Рис. 22.4. Кодовая страница Windows 1251

Unicode - стандарт кодирования символов, позволяющий представить знаки почти всех письменных языков. Стандарт был предложен в 1991 г. некоммерческой организацией «Консорциум Юникода» (англ. Unicode Consortium, Unicode Inc.). Применение этого стандарта позволяет закодировать большее число символов (чем в ASCII и прочих кодировках) за счет двухбайтового кодирования символов (всего 65536 символов). В документах Unicode могут соседствовать китайские иероглифы, математические символы, буквы греческого алфавита, латиницы и кириллицы.

Коды в стандарте Unicode разделены на несколько разделов. Первые 128 кодов соответствуют кодировке ASCII. Далее расположены разделы букв различных письменностей, знаки пунктуации и технические символы. В частности прописным и строчным буквам русского алфавита соответствуют коды 1025 (Ё), 1040-1103 (А-я) и 1105 (ё).

Шрифт Брайля - рельефно-точечный тактильный шрифт, предназначенный для письма и чтения незрячими людьми. Был разработан в 1824 г. французом Луи Брайлем (Louis Braille), сыном сапожника. Луи в возрасте трёх лет потерял зрение, в результате воспаления глаз, начавшегося от того, что мальчик поранился шпорным ножом (подобие шила) в мастерской отца. В возрасте 15 лет он создал свой рельефно-точечный шрифт, вдохновившись простотой «ночного шрифта» капитана артиллерии Шарля Барбье (Charles Barbier), который использовался военными того времени для чтения донесений в темноте.

Для изображения символов (в основном букв и цифр) в шрифте Брайля используются 6 точек, расположенных в два столбца, по 3 в каждом.

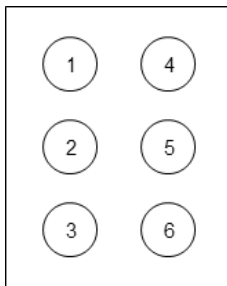


Рис. 22.5. Нумерация точек

Каждому символу соответствует свой уникальный набор выпуклых точек. Т.о. шрифт Брайля представляет собой систему для кодирования $2^6 = 64$ символов. Но присутствие в шрифте управляющих символов (например, переход к буквам или цифрам) позволяет увеличить количество кодируемых символов.

Управляющие символы			
Символ шрифта Брайля	Назначение		
.	Буквы		
⋮	Цифры		
Буквы, цифры и остальные символы			
Символ шрифта Брайля	Латинские буквы	Русские буквы	Цифры
.	A	А	1
⋮	B	Б	2
⋮⋮	C	Ц	3

⠠	D	Д	4
⠡	E	Е	5
⠢	F	Ф	6
⠣	G	Г	7
⠤	H	Х	8
⠥	I	И	9
⠦	J	Ж	0
⠧	K	К	
⠨	L	Л	
⠩	M	М	
⠪	N	Н	
⠬	O	О	
⠮	P	П	
⠯	Q	Ч	
⠰	R	Р	
⠱	S	С	
⠲	T	Т	
⠳	U	У	
⠴	V		
⠵	W	В	
⠶	X	Щ	
⠷	Y		
⠸	Z	З	
⠹		Ё	
⠺		Й	
⠻		Ш	
⠼		Ъ	
⠽		Ы	
⠾		Ь	
⠿		Э	
⠁		Ю	
⠂		Я	
⠃	Точка		
⠄	Запятая		
⠅	Восклицательный знак		
⠆	Вопросительный знак		
⠇	Точка с запятой		
⠈	Дефис		
	Пробел		

Рис. 22.6. Шрифт Брайля

Шрифт Брайля, в последнее время, стал широко применяться в общественной жизни и быту в связи с ростом внимания к людям с ограниченными возможностями.



Рис. 22.7. Надпись "Sochi 2014" шрифтом Брайля на золотой медали Параолимпийских игр 2014г.

Штрихкод - графическая информация, наносимая на поверхность, маркировку или упаковку изделий, представляющая собой последовательность черных и белых полос либо других геометрических фигур в целях ее считывания техническими средствами.

В 1948 г. Бернард Сильвер (Bernard Silver), аспирант Института Технологии Университета Дрекслея в Филадельфии, услышал, как президент местной продовольственной сети просил одного из деканов разработать систему, автоматически считывающую информацию о продукте при его контроле. Сильвер рассказал об этом друзьям - Норману Джоозефу Вудланду (Norman Joseph Woodland) и Джордину Джохэнсону (Jordin Johanson). Втроем они начали исследовать различные системы маркировки. Их первая работающая система использовала ультрафиолетовые чернила, но они были довольно дороги, а кроме того, со временем выцветали.

Убеденный в том, что система реализуема, Вудланд покинул Филадельфию и переехал в Флориду в квартиру своего отца для продолжения работы. 20 октября 1949 г. Вудланд и Сильвер подали заявку на изобретение, которая была удовлетворена 7 октября 1952 г. Вместо привычных нам линий патент содержал описание штрихкодовой системы в виде концентрических кругов.

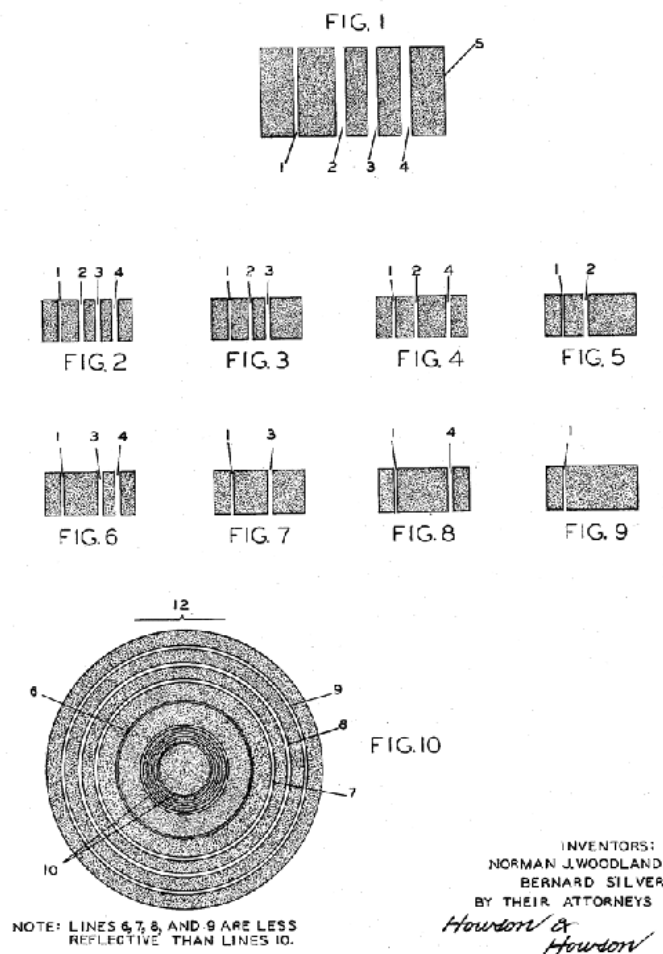


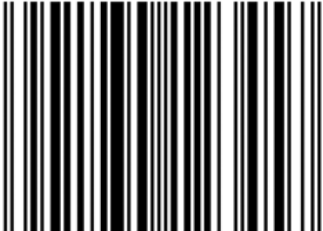
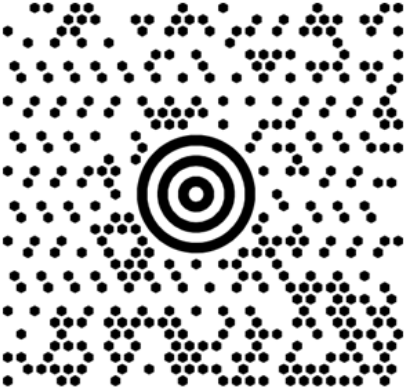
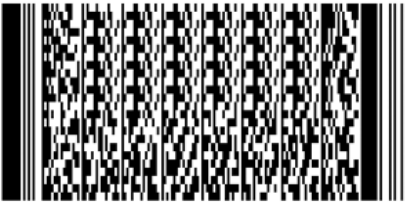
Рис. 22.8. Патент системы Вудланда и Сильвера с концентрическими кругами, предшественниками современных штрихкодов

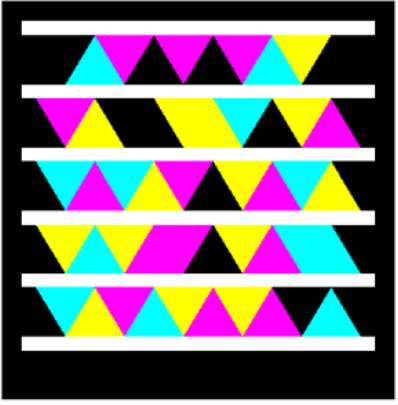
Впервые штрихкоды начали официально использоваться в 1974 г. в магазинах г. Трой, штат Огайо [44]. Системы штрихового кодирования нашли широкое применение в общественной жизни: торговля, почтовые отправления, финансовые и судебные уведомления, учет единиц хранения, идентификация личностей, контактная информация (веб-ссылки, адреса электронной почты, телефонные номера) и т.д.

Различают линейные (читаемые в одном направлении) и двумерные штрихкоды. Каждая из разновидностей различается как размерами графического изображения, так и объемами представленной информации. В следующей таблице приведены примеры некоторых разновидностей штрихкода.

Таблица 22.1. Разновидности штрихкодов

Наименование	Пример штрих-кода	Примечания
Линейные		
Universal Product Code, UPC (универсальный код товара)		Американский стандарт штрихкода, предназначенный для кодирования идентификатора товара и производителя. Имеются разновидности: - UPC-E – кодируются 8 цифр; - UPC-A – кодируется 13 цифр.
European Article Number, EAN (европейский номер товара)		Европейский стандарт штрихкода, предназначенный для кодирования идентификатора товара и производителя. Имеются разновидности: - EAN-8 – кодируются 8 цифр; - EAN 13 – кодируется 13 цифр; - EAN-128 – кодируется любое количество букв и цифр, объединенных в регламентированные группы. ГОСТ ИСО/МЭК 15420-2001 «Автоматическая идентификация. Кодирование штриховое. Спецификация символики EAN/UPC (EAN/ЮПиСи)».

	 5 901234 123457 > (EAN-13)	
Code 128 (Код 128)		Включает в себя 107 символов. Из которых 103 символа данных, 3 стартовых, и 1 остановочный символ. Для кодирования всех 128-ми символов ASCII предусмотрено три комплекта символов - А, В и С, которые могут использоваться внутри одного штрихкода. EAN-128 кодирует информацию по алфавиту Code 128 ГОСТ 30743-2001 (ИСО/МЭК 15417-2000) «Автоматическая идентификация. Кодирование штриховое. Спецификация символики Code 128 (Код 128)».
Двумерные		
DataMatrix (матричные данные)		Максимальное количество символов, которые помещаются в один код - 2048 байт. ГОСТ Р ИСО/МЭК 16022-2008 «Автоматическая идентификация. Кодирование штриховое. Спецификация символики Data Matrix».
QR-код (англ. quick response - быстрый отклик)		Квадраты в углах изображения позволяют нормализовать размер изображения и его ориентацию, а также угол, под которым сенсор относится к поверхности изображения. Точки переводятся в двоичные числа с проверкой контрольной суммы. Максимальное количество символов, которые помещаются в один QR-код: - цифры - 7089; - цифры и буквы (латиница) - 4296; - двоичный код - 2953 байт; - иероглифы - 1817.
MaxiCode (максикод)		Размер - дюйм на дюйм (1 дюйм = 2.54 см). Используется для грузоотправительных и грузоприемных систем. Может вместить в себя столько же символов, что Code128. ГОСТ Р 51294.6-2000 «Автоматическая идентификация. Кодирование штриховое. Спецификация символики MaxiCode (Максикод)».
PDF147 (англ. Portable Data File — переносимый файл данных)		Применяется при идентификации личности, учете товаров, при сдаче отчетности в контролирующие органы и других областях. Поддерживает кодирование до 2710 символов и может содержать до 90 строк.

Microsoft Tag (метка Microsoft)		Разработан для распознавания при помощи фотокамер, встроенных в мобильные телефоны. Может вместить в себя столько же символов, что Code128. Предназначен для быстрой идентификации и получения на устройство заранее подготовленной информации (веб-ссылки, произвольного текста длиной до 1000 символов, телефонного номера и т.п.), привязанной к коду и хранящейся на сервере компании Microsoft. Содержит 13 байт плюс один дополнительный бит для контроля четности.
--	--	--

Представление чисел в двоичном виде (в компьютере). Как известно, информация, хранящаяся и обрабатываемая в компьютерах, представлена в двоичном виде. **Бит** (англ. **binary digit** - двоичное число; также игра слов: англ. **bit** - кусочек, частица) - единица измерения количества информации, равная одному разряду в двоичной системе счисления. С помощью бита можно закодировать (представить, различать) два состояния (0 или 1; да или нет). Увеличивая количество битов (разрядов), можно увеличить количество кодируемых состояний. Например, для байта (англ. **byte**), состоящего из 8 битов, количество кодируемых состояний составляет $2^8 = 256$.

Числа кодируются в т.н. форматах с фиксированной и плавающей запятой.

1. Формат с фиксированной запятой, в основном, применяется для целых чисел, но может применяться и для вещественных чисел, у которых фиксировано количество десятичных знаков после запятой. Для целых чисел подразумевается, что «запятая» находится справа после младшего бита (разряда), т.е. вне разрядной сетки. В данном формате существуют два представления: беззнаковое (для неотрицательных чисел) и со знаком.

Для **беззнакового** представления все разряды отводятся под представление самого числа. Например, с помощью байта можно представить беззнаковые целые числа от 0_{10} до 255_{10} ($00000000_2 - 11111111_2$) или вещественные числа с одним десятичным знаком от 0.0_{10} до 25.5_{10} ($00000000_2 - 11111111_2$). Для **знакового** представления, т.е. положительных и отрицательных чисел, старший разряд отводится под знак (0 – положительное число, 1 – отрицательное).

Различают прямой, обратный и дополнительный коды записи знаковых чисел.

В **прямом** коде запись положительного и отрицательного числа выполняется так же, как и в беззнаковом представлении (за исключением того, что старший разряд отводится под знак). Таким образом, числа 5_{10} и -5_{10} записываются, как 00000101_2 и 10000101_2 . В прямом коде имеются два кода числа 0: «положительный ноль» 00000000_2 и «отрицательный ноль» 10000000_2 .

При использовании **обратного** кода отрицательное число записывается в виде инвертированного положительного числа (0 меняются на 1 и наоборот). Например, числа 5_{10} и -5_{10} записываются, как 00000101_2 и 11111010_2 . Следует отметить, что в обратном коде, как и в прямом, имеются «положительный ноль» 00000000_2 и «отрицательный ноль» 11111111_2 . Применение обратного кода позволяет вычитать одно число из другого, используя операцию сложения, т.е. вычитание двух чисел $X - Y$ заменяется их суммой $X + (-Y)$. При этом используются два дополнительных правила:

- вычитаемое число инвертируется (представляется в виде обратного кода);
- если количество разрядов результата получается больше, чем отведено на представление чисел, то крайний левый разряд (старший) отбрасывается, а к результату добавляется 1_2 .

В следующей таблице приведены примеры вычитания.

Таблица 22.2. Примеры вычитания двух чисел с использованием обратного кода

$X - Y$	$5 - 5$	$6 - 5$	$5 - 6$	$5 - (-6)$
X_2	00000101	00000110	00000101	00000101
Y_2	00000101	00000101	00000110	11111001
Замена сложением	$5 + (-5)$	$6 + (-5)$	$5 + (-6)$	$5 + 6$
Обратный код для вычитаемого ($-Y_2$)	11111010	11111010	11111001	00000110
Сложение	$\begin{array}{r} 00000101 \\ + 11111010 \\ \hline 11111111 \end{array}$	$\begin{array}{r} 00000110 \\ + 11111010 \\ \hline 100000000 \end{array}$	$\begin{array}{r} 00000101 \\ + 11111001 \\ \hline 11111110 \end{array}$	$\begin{array}{r} 00000101 \\ + 00000110 \\ \hline 00001011 \end{array}$
Отбрасывание старшего разряда и добавление 1_2	не требуется	$\begin{array}{r} 00000000 \\ + 00000001 \\ \hline 00000001 \end{array}$	не требуется	не требуется
Результат	-0	1	-1	11

Несмотря на то, что обратный код значительно упрощает вычислительные процедуры, а соответственно и быстродействие компьютеров, наличие двух «нулей» и другие условности привели к появлению **дополнительного** кода. При представлении отрицательного числа его модуль вначале инвертируется, как в обратном коде, а затем к инверсии сразу добавляется 1_2 .

В следующей таблице приведены некоторые числа в различном кодовом представлении.

Таблица 22.3. Представление чисел в различных кодах

Десятичное представление	Код двоичного представления (8 бит)		
	прямой	обратный	дополнительный
127	01111111	01111111	01111111
6	00000110	00000110	00000110
5	00000101	00000101	00000101
1	00000001	00000001	00000001
0	00000000	00000000	00000000
-0	10000000	11111111	---
-1	10000001	11111110	11111111
-5	10000101	11111010	11111011
-6	10000110	11111001	11111010
-127	11111111	10000000	10000001
-128	---	---	10000000

При представлении отрицательных чисел в дополнительных кодах второе правило несколько упрощается - если количество разрядов результата получается больше, чем отведено на представление чисел, то только отбрасывается крайний левый разряд (старший).

Таблица 22.4. Примеры вычитания двух чисел с использованием дополнительного кода

X – Y	5 – 5	6 – 5	5 – 6	5 – (-6)
X ₂	00000101	00000110	00000101	00000101
Y ₂	00000101	00000101	00000110	11111010
Замена сложением	5 + (-5)	6 + (-5)	5 + (-6)	5 + 6
Дополнительный код для вычитаемого (-Y ₂)	11111011	11111011	11111010	00000110
Сложение	$\begin{array}{r} 00000101 \\ + 11111011 \\ \hline 00000000 \end{array}$	$\begin{array}{r} 00000110 \\ + 11111011 \\ \hline 100000001 \end{array}$	$\begin{array}{r} 00000101 \\ + 11111010 \\ \hline 11111111 \end{array}$	$\begin{array}{r} 00000101 \\ + 00000110 \\ \hline 00001011 \end{array}$
Отбрасывание старшего разряда и добавление 1 ₂	не требуется	00000001	не требуется	не требуется
Результат	-0	1	-1	11

Можно возразить, что представление чисел в дополнительных кодах требует на одну операцию больше (после инверсии всегда требуется сложение с 1₂), что может и не потребоваться в дальнейшем, как в примерах с обратными кодами. В данном случае срабатывает известный «принцип чайника». Лучше сделать процедуру линейной, чем применять в ней правила «Если А то В» (даже если оно одно). То, что с человеческой точки зрения кажется увеличением трудозатрат (вычислительной и временной сложности), с точки зрения программно-технической реализации может оказаться эффективней.

Еще одно из преимуществ дополнительного кода перед обратным заключается в возможности представления в единице информации на одно число (состояние) больше, за счет исключения «отрицательного нуля». Поэтому, как правило, диапазон представления (хранения) для знаковых целых чисел длиной один байт составляет от +127 до -128.

2. Формат с плавающей запятой, в основном, используется для вещественных чисел. Число в данном формате представляется в экспоненциальном виде

$$X = e^n * m, \quad (22.1)$$

где e - основание показательной функции;

n - порядок основания;

eⁿ - характеристика числа;

m - мантисса (лат. mantissa - прибавка) – множитель, на который надо умножить характеристику числа, чтобы получить само число.

Например, число десятичное число 350 может быть записано, как 3.5 * 10², 35 * 10¹, 350 * 10⁰ и т.д. В **нормализованной научной записи**, порядок **n** выбирается такой, чтобы абсолютная величина **m** оставалась не меньше единицы, но строго меньше десяти (1 ≤ |m| < 10). Таким образом, в нормализованной научной записи число 350 выглядит, как 3.5 * 10². При отображении чисел в программах, учитывая, что основание равно 10, их записывают в виде **m E ± n**, где E означает «*10ⁿ» («...умножить на десять в степени...»). Например, число 350 – 3.5E+2, а число 0.035 – 3.5E-2.

Так как числа хранятся и обрабатываются в компьютерах в двоичном виде, то для этих целей принимается e = 2. Одной из возможных форм двоичного представления чисел с плавающей запятой является следующая.

b _{n±}	b _{n7}	b _{n6}	b _{n5}	b _{n4}	b _{n3}	b _{n2}	b _{n1}	b _{m±}	b _{m15}	b _{m14}	b _{m13}	b _{m12}	b _{m11}	b _{m10}	b _{m9}	b _{m8}	b _{m7}	b _{m6}	b _{m5}	b _{m4}	b _{m3}	b _{m2}	b _{m1}
знак	величина							знак	величина														
порядок								мантисса															

Рис. 22.9. Двоичный формат представления чисел с плавающей запятой

Биты b_{n±} и b_{m±}, означающие знак порядка и мантиссы, кодируются аналогично числам с фиксированной запятой: для положительных чисел «0», для отрицательных – «1». Значение порядка выбирается таким образом, чтобы величина целой части мантиссы в десятичном (и соответственно в двоичном)

0	.3671875
x	2
0	.734375
x	2
1	.46875
x	2
0	.9375
x	2
1	.875
x	2
1	.75
x	2
1	.5
x	2
1	.0

0	0	0	0	1	0	0	0	0	0	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
знак +	величина 2 ⁸							знак +	величина (1) + 0.3671875																	
порядок								мантисса																		

$b_{n\pm}$	b_{ni}	...	b_{nl}	b_{mj}	...	b_{ml}
знак мантиссы	порядок			величина мантиссы		

Формат	single	double
Общий размер, бит (байт)	32 (4)	64 (8)
Число бит для порядка	8	11
Число бит для мантиссы (без учета знакового бита)	23	52
Величина порядка	$2^{128} \dots 2^{-127}$ $(\pm 3.4 * 10^{38} \dots 1.7 * 10^{-38})$	$2^{1024} \dots 2^{-1023}$ $(\pm 1.8 * 10^{308} \dots 9.0 * 10^{-307})$
Смещение порядка	127	1023
Диапазон представления чисел (без учета знака)	$\pm 1.4 * 10^{-45} \dots 3.4 * 10^{38}$	$\pm 4.9 * 10^{-324} \dots 1.8 * 10^{308}$
Количество значащих цифр числа (не более)	8	16

[illegible]

знак мантиссы +	порядок 2^8 ($8 = 135 - 127$)	величина мантиссы (1) + 0.3671875
-----------------------	--------------------------------------	--------------------------------------

Рис. 22.13. Двоичный вид числа 350 по стандарту IEEE

К другим особенностям стандарта IEEE относится возможность представления специальных чисел. К ним относятся значения NaN (англ. Not a Number - не число) и +/-INF (англ. Infinity - бесконечность), получающихся в результате операций типа деления на ноль. Также сюда попадают денормализованные числа, у которых мантисса меньше единицы.

В заключение по числам с плавающей запятой несколько слов о пресловутой «ошибке округления». Т.к. в двоичной форме представления числа хранится только несколько значащих цифр, она не может «покрыть» все многообразие вещественных чисел в заданном диапазоне. В результате, если число невозможно точно представить в двоичной форме, оно представляется ближайшим возможным. Например, если к числу типа double «0.0» последовательно добавлять «1.7», то можно обнаружить следующую «картину» изменения значений.

```
0.0
1.7
3.4
5.1
6.8
8.5
10.2
11.899999999999999
13.599999999999998
15.299999999999997
16.999999999999996
18.699999999999996
20.399999999999995
22.099999999999994
23.799999999999994
25.499999999999993
27.199999999999992
28.899999999999999
30.599999999999999
32.299999999999999
33.999999999999999
35.699999999999996
37.4
39.1
40.800000000000004
42.500000000000001
44.200000000000001
45.900000000000001
47.6000000000000016
...
```

Рис. 22.14. Результат последовательного добавления числа 1.7 (Java 7)

Другой нюанс обнаруживается при сложении двух чисел, у которых значительно отличается порядок. Например, результатом сложения $10^{10} + 10^{-10}$ будет 10^{10} . Даже если последовательно триллион (10^{12}) раз добавлять 10^{-10} к 10^{10} , то результат останется прежним 10^{10} . Если же к 10^{10} добавить произведение $10^{-10} * 10^{12}$, что с математической точки зрения одно и то же, результат станет 10000000100 ($1.0000000100 * 10^{10}$).

Генетический код - свойственная всем живым организмам кодированная аминокислотная последовательность белков. Кодирование выполняется при помощи нуклеотидов³, входящих в состав ДНК (дезоксирибонуклеиновой кислоты). ДКН - макромолекула, обеспечивающая хранение, передачу из поколения в поколение и реализацию генетической программы развития и функционирования живых организмов. Пожалуй, самый главный код в истории человечества.

В ДНК используется четыре азотистых основания - аденин (А), гуанин (G), цитозин (С), тимин (Т), которые в русскоязычной литературе обозначаются буквами А, Г, Ц и Т. Эти буквы составляют алфавит генетического кода. В молекулах ДНК нуклеотиды выстраиваются в цепочки и, таким образом, получают последовательности генетических букв.

Белки практически всех живых организмов построены из аминокислот всего 20 видов. Эти аминокислоты называют каноническими. Каждый белок представляет собой цепочку или несколько цепочек аминокислот, соединенных в строго определенной последовательности. Эта последовательность определяет строение белка, а, следовательно, все его биологические свойства. Синтез белков (т.е. реализация генетической информации в живых клетках) осуществляется на основе информации, заложенной в ДНК. Для кодирования каждой из 20 аминокислот, а также сигнала «стоп», означающего конец белковой последовательности, достаточно трех последовательных нуклеотидов (триплета).

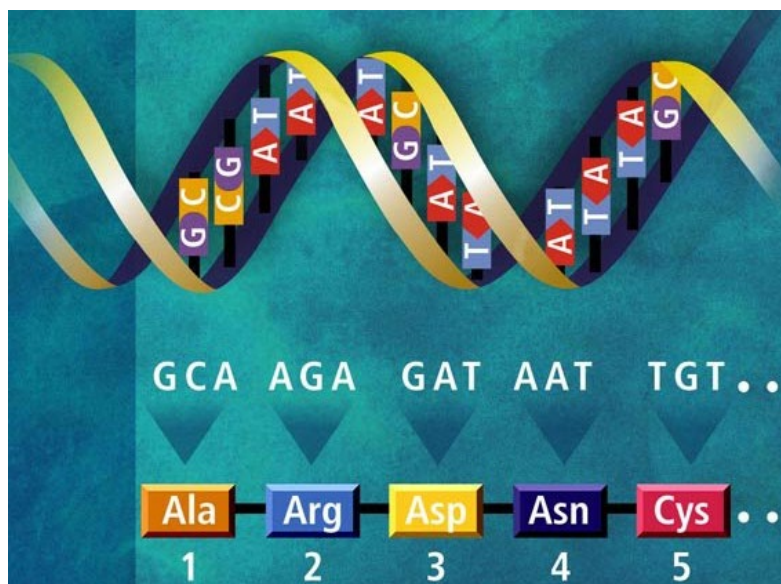


Рис. 22.15. Фрагмент ДНК

²IEEE (англ. Institute of Electrical and Electronics Engineers) - институт инженеров по электротехнике и электронике.

³Содержит азотистое основание, соединенное с сахаром, и фосфорную кислоту.

22.3. Секретные кодовые системы

Секретные коды, как и шифры, предназначены для обеспечения конфиденциальности информации. Изначально секретные кодовые системы представляли собой стеганографическую систему, в основе которой лежало подобие жаргонного кода. Они возникли в целях сокрытия имен реальных людей, упоминавшихся в переписке. Это были небольшие списки, в которых в были записаны скрываемые имена, а напротив них - кодовые замены (подстановки). Официальные коды для сокрытия содержания донесений, которыми пользовались папские эмиссары и послы средиземноморских городов-государств, найденные в ранних архивах Ватикана, датируются XIV в. По мере возрастания потребности в безопасности переписки, у представителей городов-государств появились более обширные перечни, которые включали в себя не только кодовые замены имен людей, но и стран, городов, видов оружия, провианта и т.д. В целях повышения защищенности информации к перечням были добавлены шифралфавиты для кодирования слов, не вошедших в перечень, а также правила их использования, базирующиеся на различных стеганографических и криптографических методах. Такие сборники получили название **«номенклаторы»**. С XV и до середины XIX в. они были основной формой обеспечения конфиденциальности информации [43].

Вплоть до XVII столетия в номенклаторах слова открытого текста и их кодовые замены шли в алфавитном порядке, пока французский криптолог Антуан Россиньоль не предложил использовать более стойкие номенклаторы, состоящие из двух частей. В них существовало два раздела: в одном перечислялись в алфавитном порядке элементы открытого текста, а кодовые элементы были перемешаны. Во второй части в алфавитном порядке шли перечни кодов, а перемешанными были уже элементы открытого текста.

Изобретение телеграфа и азбуки Морзе, а также прокладка трансатлантического кабеля в середине XIX в. значительно расширило сферы применения секретных кодов. Помимо традиционных областей их использования (в дипломатической переписке и в военных целях) они стали широко использоваться в коммерции и на транспорте. Секретные кодовые системы того времени в своем названии содержали слово **«код»** («Код Госдепартамента (1867 г.)», «Американский код для окопов», «Речные коды : Потомак», «Черный код») или **«шифр»** («Шифр Госдепартамента (1876 г.)», «Зеленый шифр»). Следует отметить, что, несмотря на наличие в названии слова «шифр», в основу этих систем было положено кодирование.

609			609		
Code word P	Code No 609	Message or true reading	Code word P	Code No 609	Message or true reading
Promotes	00	Russia	Propels	50	Russia – Continued
Promoting	01	Agreement between Russia and	Propend	51	Subject of Russia
Promotion	02	Agreement with Russia	Propended	52	Subjects of Russia
Promotions	03	Ambassador from Russia	Propendent	53	The Czar of Russia
Promotive	04	Ambassador of Russia	Propending	54	The Emperor of Russia
Prompt	05	Ambassador to Russia	Propends	55	The Empire of Russia
Prompted	06	And Russia	Propense	56	The Empress of Russia
Prompter	07	Army of Russia	Propension	57	The Government of Russia
Prompters	08	Authorities of Russia	Propensely	58	The trade of Russia
Promptest	09	Authority of Russia	Propension	59	To Russia
Prompting	10	By Russia	Propensity	60	To the Government of Russia
Promptings	11	Cabinet of Russia	Proper	61	Treaty between Russia and
Promptly	12	Charge d'affaires of Russia	Properate	62	Treaty with Russia
Promptness	13	Commerce of Russia	Properly	63	Vessel of Russia
Prompts	14	Consul of Russia	Properness	64	Vessels of Russia
Promulgate	15	Consul-general of Russia	Properties	65	War vessel of Russia
Pronate	16	Consuls of Russia	Property	66	War vessels of Russia
Pronation	17	Convention between Russia and	Prophesied	67	With Russia
Pronator	18	Convention with Russia	Prophesies	68	With the Government of Russia
Prone	19	Czar of Russia	Prophecy	69	Russian
Pronely	20	Embassy of Russia	Prophet	70	And the Russian
Proneness	21	Emperor of Russia	Prophetess	71	And the Russian Government
Prong	22	Empire of Russia	Prophetic	72	From the Russian Government
Pronged	23	Empress of Russia	Prophetize	73	Russian agreement
Pronghorn	24	Flag of Russia	Prophets	74	Russian Ambassador
Prongs	25	Forces of Russia	Propine	75	Russian Ambassador (by name)
Pronity	26	From Russia	Propined	76	Russian army
Pronoun	27	From the Government of Russia	Propines	77	Russian authorities
Pronounce	28	Government of Russia	Propining	78	Russian authority
Pronounced	29	Head of the Government (by whatever title)	Propitious	79	Russian cabinet
Pronouncer	30	Her Majesty the Empress of Russia	Proplastic	80	Russian capital
Pronounces	31	His Majesty the Emperor of Russia	Propodial	81	Russian charge d'affaires
Pronouns	32	Imperial Government of Russia	Propone	82	Russian commerce
Pronubial	33	In Russia	Proponed	83	Russian company
Pronuncial	34	Legation of Russia	Proponent	84	Russian consul
Proof	35	Minister for foreign affairs of Russia	Propones	85	Russian consul-genera,l
Proofless	36	Minister for foreign affairs of Russia (by name)	Proponing	86	Russian consuls
Proofs	37	Minister from Russia	Proportion	87	Russian convention
Prop	38	Minister of Russia	Proposal	88	Russian Czar
Propagable	39	Minister of Russia at	Proposals	89	Russian embassy
Propaganda	40	Minister to Russia	Propose	90	Russian Emperor
Propagate	41	Naval vessel of Russia	Proposed	91	Russian Empire
Propagated	42	Naval vessels of Russia	Proposer	92	Russian Empress
Propagates	43	Navy of Russia	Proposers	93	Russian flag
Propagator	44	Of Russia	Proposes	94	Russian forces
Propel	45	People of Russia	Proposing	95	Russian funds
Propelled	46	Policy of Russia	Propound	96	Russian Government
Propeller	47	Possessions of Russia	Propounded	97	Russian lagation
Propellers	48	Secretary of embassy of Russia	Propounder	98	Russian minister
Propelling	49	Secretary of legation of Russia	Propounds	99	Russian minister (by name)
			Propped		Russian minister at

Рис. 22.16. Фрагмент «Шифра Госдепартамента (1899 г.)»

Разработчики кодов, как и составители шифров, нередко добавляли дополнительные степени защиты, чтобы затруднить взлом своих кодов. Такой процесс называется **перешифрованием**. В итоге секретные кодовые системы сочетали в себе, как стеганографические, так и криптографические способы обеспечения конфиденциальности информации. Наиболее популярные из них приведены в следующей таблице.

Таблица 22.6. Способы обеспечения конфиденциальности информации в секретных кодовых системах

Способ	Тип	Примечания	Примеры (кодируемое слово – кодовое обозначение)
Замена слова (словосочетания) другим словом произвольной длины	стеганографический	Аналог - жаргонный код. Для одного кодируемого слова могли использоваться несколько кодовых обозначений.	1. Номенклатор города Сиены (XV в.): Cardinales (кардинал) – Florenus; Antonello da Furlì (Антолло да Фурли) – Forte. 2. Шифр Госдепартамента 1899 г.: Russia (Россия) – Promotes; Cabinet of Russia (Правительство России) – Promptings. 3. Код руководителя службы связи (1871 г.): 10:30 – Anna, Ida; 13th (тринадцатый) – Charles, Mason.
Замена слова (словосочетания) символьной строкой фиксированной длины	стеганографический	Аналог - жаргонный код.	1. Американский код для окопов (1918 г.): Patrol (патруль) – RAL; Attack (атака) – DIT. 2. Код Госдепартамента А-1 (1919 г.): Diplomat (дипломат) – BUJON; Diplomatic corps (дипломатический корпус) – BEDAC.
Замена слова (словосочетания) числом	стеганографический	Аналог - жаргонный код. Для одного кодируемого слова могли использоваться несколько кодовых обозначений.	1. Номенклатор Бенджамина Толмаджа (1779 г.): Defense (оборона) – 143; Attack (атака) – 38. 2. Код вещания для торговых судов союзников во Второй мировой войне (BAMS): остров – 36979; порт – 985.
Замена слова (словосочетания) набором цифр фиксированной длины	стеганографический	Аналог - жаргонный код.	1. Американский код для окопов (1918 г.): Patrol (патруль) – 2307; Attack (атака) – 1447. 2. Американский служебный радиокод № 1 (1918 г.): Oil (масло) – 001; Bad (плохой) – 642.
Замена букв	криптографический	Аналоги – шифр однозначной замены, омофонический шифр, полиалфавитный шифр. В качестве кодового обозначения могли использоваться буквы, числа, графические обозначения. Применялась для слов,	1. Номенклатор города Сиены (XV в.): q –  ; s –  . 2. Номенклатор Джеймса Мэдисона (1781 г.): o – 527; p – 941. 3. Американский код для окопов (1918 г.): a – 1332 .. 2795 или CEW .. ZYR. Содержал также 30 алфавитов шифрозамен для перешифрования кодовых

		отсутствующих в списке кодируемых.	обозначений.
Замена сочетания букв	криптографический	Аналог – полиграммный шифр замены. В качестве кодового обозначения могли использоваться буквы, числа, графические обозначения.	1. Номенклатор города Сиены (XV в.): bb –  ; tt –  . 2. Номенклатор X-Y-Z (1737 г.): ce – 493; ab – 1194.
Использование пустых знаков	стеганографический	Аналог – пустышечный шифр. Ничего назначавшие (лат. nihil importantes) символы использовались для запутывания криптоаналитиков.	1. Номенклатор города Сиены (XV в.):  ,  . 2. Речные коды : Потомак (1918 г.): ASY.
Использование аддитивных чисел	криптографический	Аналог – полиалфавитный шифр. Аддитивное число, добавляемое к числовому кодовому обозначению, служило в качестве переменной части кода (ключа).	Шифр Госдепартамента 1876 г.: правило «Horse» (лошадь) в начале сообщения означало, что при кодировании последующих кодовых обозначений использовалось аддитивное число 203; «Hawk» (ястреб) - 100.
Перестановка букв (цифр) в кодовых обозначениях	криптографический	Аналог – шифр блочной одинарной перестановки.	Телеграфный код для обеспечения секретности при передаче телеграмм (1870 г.): одно из правил предписывало перестановку последних трех цифр в цифровом кодовом обозначении, состоящем из пяти цифр.
Перестановка кодовых обозначений	криптографический	Аналог – шифр перестановки.	Шифр Госдепартамента 1876 г.: правило «Tiger» (тигр) в начале сообщения означало, что раскодированное сообщение надо читать с последнего слова по первое (задом-наперед); «Tapir» (тапир) – меняя местами каждую пару слов (т.е. первое и второе, третье и четвертое и т.д.).

Сочетание различных способов кодирования и перешифровки в кодовой системе было обычной практикой у разработчиков кодов и стало применяться практически с самого начала их появления. Так, еще в номенклатуре, использовавшемся в г. Сиена в XV в., помимо кодовых замен слов, применялись шифралфавиты для замены букв, их удвоенных сочетаний и пустых знаков. Наибольшего расцвета эта практика получила в конце XIX – начале XX вв. В частности в «Шифре Госдепартамента 1876 г.» (англ. Red Book – Красная книга), состоящем из 1200 страниц, и его дополнении «Неподдающийся декодированию код: дополнение к шифру Госдепартамента» применялись:

- кодовые обозначения в виде слов и чисел;
- 30 шифралфавитов для замены букв;
- 50 правил перешифрования, включая аддитивные числа, перестановки кодовых обозначений и их частей.

В дополнении к «Шифру Госдепартамента 1899 г.» (англ. Blue Book – Синяя книга) были описаны еще 25 дополнительных правил перешифрования: изменение направления чтения и записи, прибавление или вычитание чисел, замена кодовых чисел другими кодовыми числами.

Разработчики кодов, чтобы закодировать сообщение, могут не только создавать с самого начала новые коды, но и воспользоваться уже имеющимися текстами. Т.н. **книжные коды** по своей сути аналогичны книжному шифру. В отличие от них замене подлежит не буква, а все слово целиком. Таким образом, кодовая замена представляет собой тройку чисел «страница.строка.слово». В книжных шифрах, как и в кодовых системах, рассмотренных выше, нашли широкое применение различные способы перешифровки. В частности, аддитивные числа, перестановки цифр и повторные замены.

Несомненным преимуществом книжного кода является то, что исключается необходимость использовать вызывающие подозрение кодовые книги — обнаружение таковой может привести к провалу агента. В то же время саму книгу можно потерять или ее могут украсть, в результате чего окажется скомпрометированной вся система.

Вопросы для самопроверки

1. Назовите основные отличия кодовых систем от криптографических.
2. Дайте характеристику общедоступным кодовым системам.
3. Перечислите основные способы обеспечения конфиденциальности информации в секретных кодовых системах.

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской Федерации (от 12.12.1993 г.).
2. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» (№ 149-ФЗ от 27.07.2006 г.).
3. Доктрина информационной безопасности Российской Федерации (№ Пр-1895 от 06.09.2000 г.).
4. Федеральный закон Российской Федерации «О государственной тайне» (№ 5485-1 от 06.10.1997 г.).
5. Указ Президента РФ «Перечень сведений конфиденциального характера» (№ 188 06.03.1997 г.).
6. Федеральный закон Российской Федерации «О персональных данных» (№ 152 от 27.07.2006 г.).
7. Федеральный закон Российской Федерации «Об электронной цифровой подписи» (№ 1-ФЗ от 26.12.2001 г.).
8. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер – М.: ТРИУМФ, 2002. – 816 с.
9. Введение в криптографию / Под. ред. В.В. Яценко. – СПб.: Питер, 2001. – 288 с.
10. Коутинхо, С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. – М.: Постмаркет, 2001. – 328 с.
11. Барычев, С. Основы современной криптографии / С. Барычев, Р. Серов. – М.: 2001. – 152 с.
12. Яковлев, В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учебник для вузов ж.-д. транспорта / В.В. Яковлев, А.А. Корниенко. – М.: УМК МПС России, 2002. – 328 с.
13. Кан, Д. Взломщики кодов / Д. Кан – М.: Центрполиграф, 2000. – 594 с.
14. Бабаш, А.В. Криптография. Под. ред. В.П. Шерстюка, Э.А. Применко / А.В. Бабаш, Г.П. Шанкин – М.: СОЛОН-ПРЕСС, 2007. – 512 с.
15. Алферов, А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин – М.: Гелиос АРВ, 2002. – 480 с.
16. National Institute of Standards and Technology (NIST). FIPS Pub 46-3 (Federal information processing standards publication): Data Encryption Standard (DES). Oct. 1999. csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.
17. Википедия. ru.wikipedia.org.
18. Галатенко, В.А. Основы информационной безопасности. www.intuit.ru.
19. Галатенко, В.А. Информационная безопасность: основные стандарты и спецификации. www.intuit.ru.
20. Басалова, Г.В. Основы криптографии. www.intuit.ru.
21. Ботт, Э. Эффективная работа: Безопасность Windows / Э. Ботт, К. Зихерт. – СПб.: Питер, 2003. – 682 с.
22. Малюк, А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В.

Пазинин, Н.С. Погожин. – М.: Горячая линия - Телеком, 2001. – 148 с.

23. Фомичев, В.М. Дискретная математика и криптология / В.М. Фомичев. – М.: ДИАЛОГ-МИФИ, 2003. – 400 с.

24. Винокуров, А.Ю. Традиционные криптографические алгоритмы. www.enlight.ru/crypto/algorithms/algs.htm.

25. CryptoBloG. Прикладные методы защиты информации. crypto-blog.ru.

26. Скудис, Э. Противостояние хакерам / Эд Скудис. – М.: ДМК Пресс, 2003. – 512 с.

27. Андреев, А.Г. и др. Microsoft Windows 2000 Professional. Русская версия / Под. ред. А.Н. Чекмарева и Д.Б. Вишнякова - СПб.: БВХ - Санкт-Петербург, 2000. – 752 с.

28. Барсуков, В.С. Безопасность: технологии, средства, услуги. / В.С. Барсуков - М.: КУДИЦ - ОБРАЗ, 2001. – 496 с.

29. Гордиенко, И. ID-cards: о старый, новый дивный мир! Компьютерра - 1999. - №10 (288).

30. Берд, К. Война — это мир, паспорт — это свобода. www.computerra.ru.

31. Кохно, В.О. Информационные системы медицинского страхования на основе пластиковых карт

32. Макаров, О. Отдай голос машине: голоса из урны. Популярная механика – 2012. – № 113

33. ЦИК РФ. cikrf.ru.

34. Кнут, Д.Э. Искусство программирования, т.2. Получисленные алгоритмы / Д.Э. Кнут - М.: Издательский дом «Вильямс», 2000. – 832 с.

35. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты / А.А. Петров - М.: ДМК, 2000. – 448 с.

36. Портал ОАО «Универсальная электронная карта». www.uecard.ru.

37. Palacios, M.A. and etc. InfoBiology by printed arrays of microorganism colonies for timed and on-demand release of messages. www.pnas.org/content/early/2011/09/19/1109554108.

38. Шелков, В.А. История "микроточки". Специальная техника и связь – 2012. – № 3.

39. Получение микроизображения (микроточки). www.photohistory.ru/Mikrot-manuf.html.

40. Малюк, А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С. В. Пазинин, Н. С. Погожин - М.: Горячая линия-Телеком, 2001. – 148 с.

41. Риджуэй, А. Целую книгу закодировали в ДНК. Наука в фокусе - 2012 - №11 (013).

42. www.technologyreview.com/view/515016/one-time-pad-reinvented-to-make-electronic-copying-impossible.

43. Риксон, Фред Б. Коды, шифры, сигналы и тайная передача информации / Фред Б. Риксон - М.: АСТ: Астрель, 2011. – 656 с.

44. Мир математики. Т.2: Жуан Гомес. Математики, шпионы и хакеры. Кодирование и криптография. - М.: Де Агостини, 2014. - 144 с.

45. RFIDjournal.com

46. Мошенский, С.З. Эволюция векселя / С.З. Мошенский. - Ровно: «Планета-друк», 2005. – 446 с.

47. Автономов, А.С. Сравнительное избирательное право / А.С. Автономов, Ю.А. Веденеев, В.В. Луговой. - М.: Издательство НОРМА, 2003. — 208 с.

48. Автономов, А.С. Зарубежное избирательное право / А.С. Автономов, Ю.А. Веденеев, О.В. Дегтярева, В.В. Луговой, В.И. Лысенко. - М.: Издательство НОРМА, 2003. — 288 с.

49. Веденеев, Ю.А. Очерки по истории выборов и избирательного права / Ю.А. Веденеев, И.В. Зайцев, В.Е. Кораблин, В.В. Луговой, В.В. Тылкин. - Калуга : Калужский обл. фонд возрождения историко-культурных и духовных традиций «Символ», 2002. - 692 с.

50. Морозова, О.С. Обязательное голосование: мировой опыт и особенности избирательных практик. Каспийский регион: политика, экономика, культура - 2013. - № 3 (36).

51. Чуров, В.Е. Российский опыт использования технических средств в ходе региональных и муниципальных выборов 2008–2011 годов / В.Е. Чуров, Н.Е. Конкин, Г.И. Райков, А.В. Иванченко. — М.: РЦОИТ, 2011. — 328 с.

52. Мир математики. Т.3: Энрике Грасиан. Простые числа. Долгая дорога к бесконечности. - М.: Де Агостини, 2014. - 144 с.

53. Мир математики. Т.21: Ламберто Гарсия дель Сид. Замечательные числа: Ноль, 666 и другие бестии. - М.: Де Агостини, 2014. - 160 с.

54. Мир математики. Т.31: Хоакин Наварро. Тайная жизнь чисел. Любопытные разделы математики. - М.: Де Агостини, 2014. - 160 с.

55. Fujioka, A., Okamoto, T., and Ohta, K. A Practical Secret Voting Scheme for Large Scale Elections. In Proceedings of the Workshop on the theory and Application of Cryptographic Techniques: Advances in Cryptology (December 13 - 16, 1992). J. Seberry and Y. Zheng, Eds. Lecture Notes In Computer Science, vol. 718. Springer-Verlag, London, 244-251.

56. Cranor, L. and Cytron, R., 1997. Sensus: A Security-Conscious Electronic Polling System for the Internet. Proc. of the Hawaii International Conference on System Sciences. Wailea, Hawaii.

57. Federal Information Processing Standards Publication 197. Announcing the ADVANCED ENCRYPTION STANDARD (AES). November 26, 2001. nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

58. ГОСТ 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf.

59. ГОСТ 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. www.tc26.ru/standard/gost/GOST_R_3413-2015.pdf.

60. Bitcoin Developer Reference. bitcoin.org/en/developer-reference.

61. Bitcoin Wiki. en.bitcoin.it/wiki/Main_Page.

62. Технологии криптовалют. www.intuit.ru/studies/courses/3643/885/info.

63. J. von Neumann. Various techniques used in connection with random digits. Collected Works, vol. 5, pp. 768–770, Pergamon Press, 1963. also: in Monte Carlo Method, National Bureau of Standards Series, Vol. 12, pp. 36-38, 1951.

64. Круглов, П. Поиск генераторов истинных случайных чисел [Электронный ресурс]. — Режим доступа: habr.com/ru/company/mailru/blog/408181 (дата обращения: 10.12.2019).

65. Intel Digital Random Number. Software Implementation Guide. - Intel Corporation. August 7, 2012. - 35 p.

66. R.C. Fairfield, R.L. Mortenson, K.B. Coulthart. 1985. An LSI random number generator (RNG). In

Proceedings of CRYPTO 84 on Advances in cryptology, G R Blakley and David Chaum (Eds.). Springer-Verlag New York, Inc., New York, NY, USA, 203-230.

67. David H. Bailey, Peter B. Borwein, Simon Plouffe. On the Rapid Computation of Various Polylogarithmic Constants // Mathematics of Computation. – 1997. – Т. 66, вып. 218. – С. 903–913