	До	После
Знания о материале		
Полезность материала		

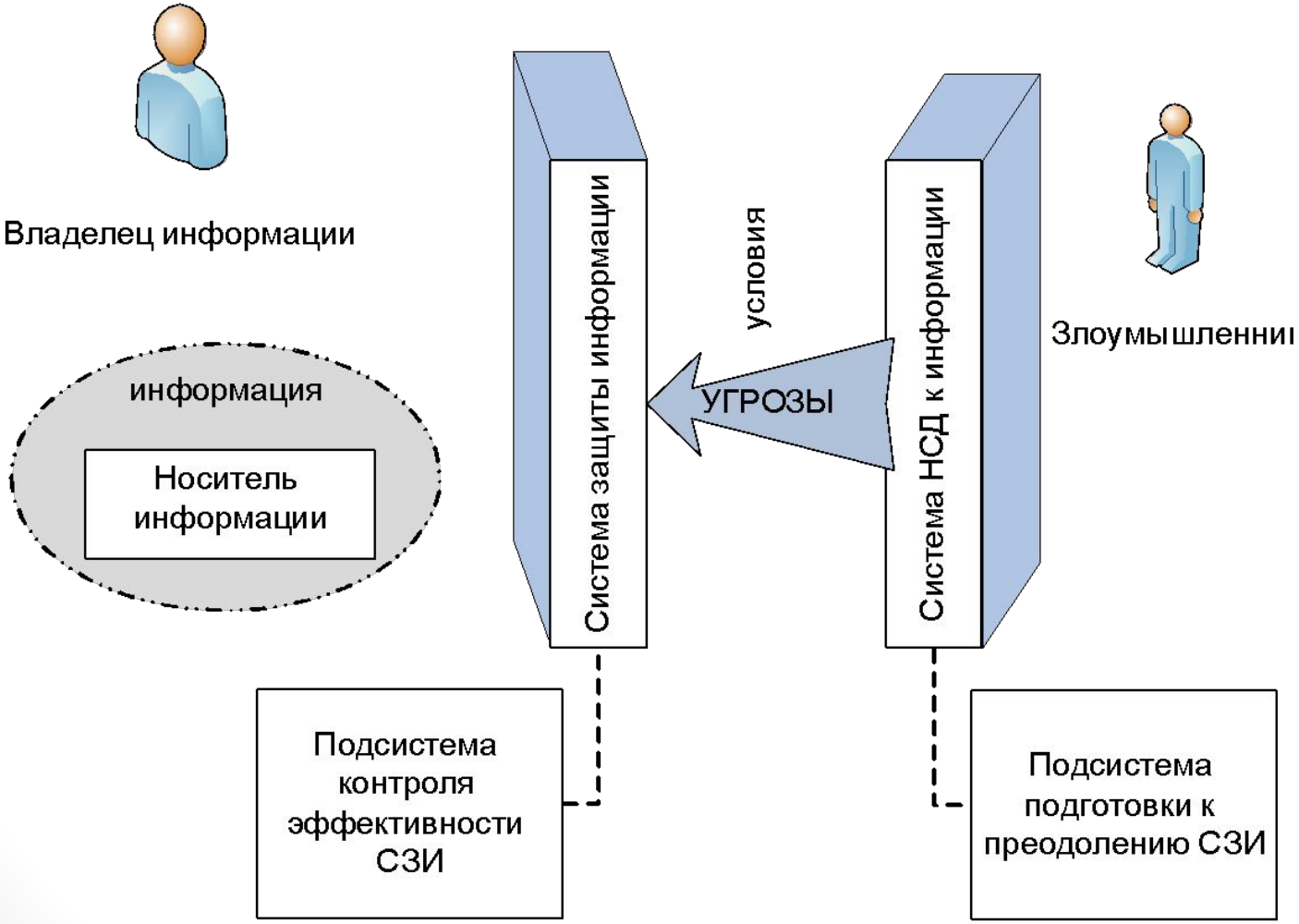
Организационные и технические способы и средства защиты информации. Шифровальная (криптографическая) защита информации. Электронная подпись.

лекция

Учебные вопросы

1. Политика информационной безопасности.
2. Способы и средства защиты информации.
3. Доступ, аудит и технический контроль на средствах вычислительной техники.
4. Защита информации при работе ведомственных сетей и сетей общего пользования.
5. Антивирусная защита информации.
6. Защита информации от утечки по техническим каналам.
7. Шифрование (криптография).
8. Электронная подпись.

Модель защиты информации




Субъект, имеющий легальный доступ к информации
Защищаемая информация
Носители защищаемой информации
Угрозы защищаемой информации
Способы и средства защиты информации, включая контроль
Характеристики субъекта, имеющего легальный доступ к информации
Мониторинг ценности защищаемой информации
Учёт этапов жизненного цикла носителя защищаемой информации
Ранжирование угроз защищаемой информации по степени опасности
Выбор достаточных способов и средств защиты от угроз за минимальную цену

1. Политика информационной безопасности


ОБЪЕКТЫ УГРОЗ:
Сведения о составе, состоянии и деятельности
ИСТОЧНИКИ УГРОЗ:
1.конкуренты;
2.преступники
ЦЕЛИ:
1.ознакомление;
2.модификация;
3.уничтожение
СПОСОБЫ ДОСТУПА:
1.за счет разглашения;
2.за счет утечки;
3.за счет НСД
НАПРАВЛЕНИЯ ЗАЩИТЫ:
1.правовая;
2.организационная;
3.инженерно-техническая
Информация
ИСТОЧНИКИ ИНФОРМАЦИИ:
1. персонал;
2.документы;
3.тех. средства;
4.тех. носители;
5.продукция;
6.отходы
СРЕДСТВА ЗАЩИТЫ:
1.физические;
2.аппаратные;
3.программные;
4.криптографические
СПОСОБЫ ЗАЩИТЫ:
1.упреждение;
2.предотвращение;
3.пресечение;
4.противодействие
УГРОЗЫ:
1.целостности;
2.конфиденциальности;
3.доступности;
4.полноте;

Политика информационной безопасности - совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые направлены на защиту ценной информации.

Назначение Политики информационной безопасности:

— формулирование целей и задач информационной безопасности организации;

— определение правил организации работы в компании для минимизации рисков информационной безопасности и повышения эффективности бизнеса.

Примерное содержание политики информационной безопасности

- 1. Общие положения
- 1.1. Цель и назначение настоящей Политики
- 1.2. Область применения настоящей Политики
- 2. Требования и рекомендации
- 2.1. Ответственность за информационные активы
- 2.2. Контроль доступа к информационным системам
- 2.2.1. Общие положения
- 2.2.2. Доступ третьих лиц к системам Компании
- 2.2.3. Удаленный доступ
- 2.2.4. Доступ к сети Интернет
- 2.3. Защита оборудования
- 2.3.1. Аппаратное обеспечение
- 2.3.2. Программное обеспечение
- 2.4. Рекомендуемые правила пользования электронной почтой
- 2.5. Сообщение об инцидентах информационной безопасности, реагирование и отчетность
- 2.6. Помещения с техническими средствами информационной безопасности
- 2.7. Управление сетью
- 2.7.1. Защита и сохранность данных
- 2.8. Разработка систем и управление внесением изменений

2. Способы и средства защиты информации

Основные способы защиты информации:

- организационные;
- физические;
- управление доступом;
- криптографические;
- антивирусная защита
- защита технических каналов утечки информации;
- правовые.

К **организационным способам защиты** относятся мероприятия организационного характера по выполнению правил обращения с информацией ограниченного доступа.

Физические способы защиты основаны на создании физических препятствий для злоумышленника, преграждающих ему путь к защищаемой информации (строгая пропускная система на территорию и в помещения с аппаратурой или с носителями информации).

Несмотря на богатый опыт по применению таких способов следует признать, что они эффективны только от "внешних" злоумышленников и не защищают информацию от тех лиц, которые обладают правом входа в помещение.

Под **управлением доступом** понимается способ защиты информации регулированием использования всех ресурсов системы (технических, программных, элементов баз данных).

В автоматизированных системах информационного обеспечения должны быть регламентированы порядок работы пользователей и персонала, право доступа к отдельным файлам в базах данных и т.д.

В сетях ЭВМ наиболее эффективными являются криптографические способы защиты информации.

Если физические способы защиты могут быть преодолены путем, например, дистанционного наблюдения, подключения к сети или подкупа персонала, законодательные не всегда сдерживают злоумышленника, а управление доступом не гарантирует от проникновения изощренных "хакеров", то криптографические методы характеризуются наибольшей степенью "прочности"

К правовым методам обеспечения информационной безопасности РФ относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности РФ.

3. Доступ, аудит и технический контроль на средствах вычислительной техники.

ДОСТУП К ИНФОРМАЦИИ

Проверка пользователя на предмет
способности доверить тайну

Бумажные носители информации:
Учёт тетрадей, книг, их листов
Специальные требования по хранению, перемещению и работе с ними:
Контроль

Электронные носители информации:
Специальные требования по определению подлинности пользователя, определение и предоставление прав работы с документами, аудит и т.п.

Доступ в автоматизированную информационную систему

включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы, (под идентификацией понимается присвоение каждому объекту персонального идентификатора (имени, кода, пароля и т.п.) и опознание (аутентификация - установление подлинности) субъекта или объекта по предъявленному идентификатору;

- проверку полномочий, заключающуюся в проверке соответствия времени, ресурсов и процедур установленному регламенту;

Управление доступом:

- разрешение и создание условий работы в пределах (и только в пределах) установленного регламента;
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий.

Самым распространенным методом установления подлинности является **метод паролей**.
Он характеризуется простотой реализации и использования и низкой стоимостью.

Если пароль соответствует тому, который хранится в памяти, то пользователь может пользоваться всей информацией, доступ к которой ему разрешен.

Различаются несколько типов паролей:

- простой пароль;
- пароль однократного использования;
- пароль на основе метода «запрос-ответ»;
- пароль на основе определенного алгоритма

Простой пароль

Схема простого пароля очень легка для использования: пользователь только вводит с клавиатуры пароль после запроса, а компьютерная программа (или специальная микросхема) сравнивает его с хранящимся в памяти ЭВМ эталоном.

Преимущество этого метода - нет необходимости записи пароля.

Недостаток - относительно простой метод, защита легко снимается. Рекомендуется использовать этот метод в случаях, когда защищаются данные с небольшим значением и стоимостью.

Создание простых паролей

Однажды в студёную зимнюю пору
Я из лесу вышел. Был сильный мороз.

OvszpYilvbsm

Пароль однократного использования

В схеме однократного пароля пользователю выдается список из N паролей, которые хранятся в памяти ЭВМ (обычно в зашифрованном виде). После использования пароль уничтожается в памяти, вычеркивается из списка. При этом перехват пароля становится бессмысленным - его значение не повторяется.

Преимущество данного метода - он обеспечивает большую степень безопасности, но он является и более сложным.

Метод не свободен от недостатков. Во-первых, необходимо где-то хранить список паролей, запоминать его практически невозможно. В случае ошибки в процессе передачи пользователь оказывается в затруднительном положении: он не знает, следует ли ему передать тот же самый пароль или послать следующий. Во-вторых, возникают чисто административные трудности: список может занимать достаточно большой объем памяти в ЭВМ, его необходимо постоянно изменять и т.д.

Метод "запрос - ответ"

В методе "запрос-ответ" пользователь должен дать правильные ответы на набор вопросов, который хранится в памяти ЭВМ и управляется операционной системой. Иногда пользователям задается большое количество вопросов и от них требуют ответы на те, которые они сами выберут.

Достоинство данного метода состоит в том, что пользователь может выбрать вопросы, а это дает весьма хорошую степень безопасности в процессе включения в работу.

Пароль на основе алгоритма

Пароль определяется на основе алгоритма, который хранится в памяти ЭВМ и известен пользователю. Это часто называют процедурой "рукопожатия". Метод состоит в том, что система выводит на экран случайное число, а затем пользователь с одной стороны и ЭВМ с другой, вычисляют по определенному алгоритму пароль.

Процедуры в режиме "рукопожатия" обеспечивают большую степень безопасности, чем многие другие схемы, но вместе с тем являются более сложными и требующими дополнительных затрат времени для пользователя.

Пароль на основе "персонального физического ключа"

В памяти ЭВМ хранится таблица, в которой записаны как пароли в зашифрованном виде, так и их открытый вариант. Кроме того, лицам, допущенным к работе в системе, выдается специальная магнитная карточка, на которую занесена информация, управляющая процессом шифрования. Процедура допуска требует, чтобы пользователь вставил карточку в специальное считывающее устройство и ввел свой пароль в открытом виде.

После этого пароль кодируется с использованием информации, записанной на магнитной карточке, и ищется соответствующая точка входа в таблицу паролей. В случае, если закодированный пароль соответствует хранящемуся эталону, подлинность пользователя считается установленной.

Недостатки паролей:

1). Обычно задаются слишком длинные пароли. Будучи не в состоянии их запомнить, пользователи записывают пароли на клочках бумаги, в записные книжки и т.д. После этого пароль теряет все свои привлекательные черты и становится уязвимым.

2). Пользователи склонны к выбору тривиальных паролей, которые просто подбираются после немногочисленных попыток.

3). Процесс ввода пароля в систему поддается наблюдению даже в том случае, если отсуствует режим "эхо" - вводимые символы не отражаются на экране. Вводя пароль необходимо убедиться в том, что никто не стоит за вашей спиной.

4). Таблица паролей, которая входит обычно в состав программного обеспечения операционной системы, может быть изменена, что часто и происходит. Необходимо кодировать таблицу паролей! Ключ алгоритма декодирования должен находиться только у лица, отвечающего за безопасность информации.

5). Известны случаи, когда в систему вносится "троянский конь", перехватывающий вводимые пароли и записывающий их в отдельный файл. Необходима большая осторожность при работе с но выми программными продуктами.

При работе с паролями рекомендуется применение следующих правил и мер предосторожности:

- пароли не следует печатать или отображать на экран;

- пароли нужно менять часто. Чем больший период времени используется один и тот же пароль, тем больше вероятность того, что он будет раскрыт;

- каждый пользователь хранит свой пароль и не позволяет посторонним узнать его;

- пароли всегда должны быть зашифрованы и их безопасность должна обеспечиваться недорогими и эффективными средствами;

- длину пароля необходимо выбрать правильно: чем больше длина пароля, тем большую безопасность будет обеспечивать система, так как потребуются большие усилия для отгадывания пароля.

Регистрация и аудит на средствах вычислительной техники

Защитные свойства регистрации и аудита в информационных системах

Механизм регистрации основан на подотчетности системы обеспечения безопасности, которая фиксирует все события, касающиеся безопасности, в том числе, такие как:

- **вход и выход субъектов доступа;**
- **запуск и завершение программ;**
- **выдача печатных документов;**
- **попытки доступа к защищаемым ресурсам;**
- **изменение полномочий субъектов доступа;**
- **изменение статуса объектов доступа и т.д.**

Аудит – это анализ накопленной информации, проводимый оперативно в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

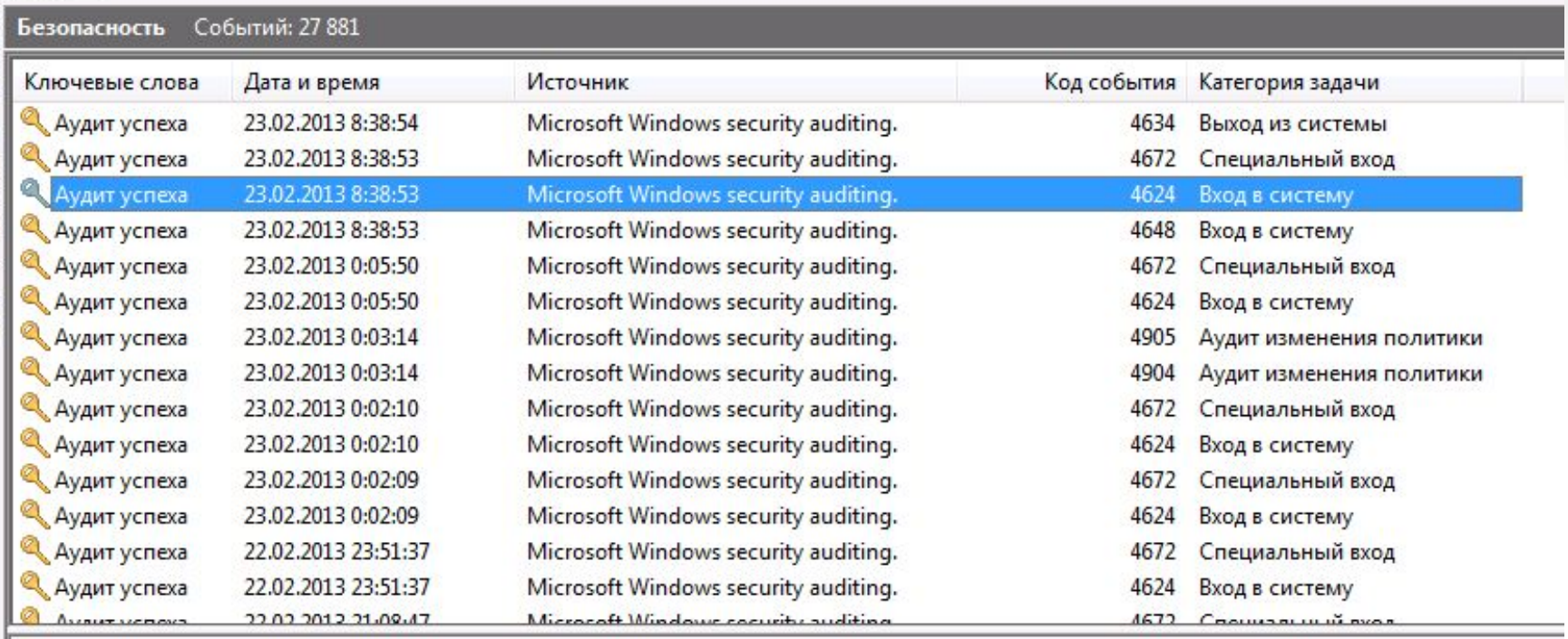
Реализация механизмов регистрации и аудита позволяет решать следующие задачи информационной безопасности:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Практическими средствами регистрации и аудита являются:

- ✔ различные системные утилиты и прикладные программы;
- ✔ регистрационный (системный или контрольный) журнал.

Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.



Безопасность Событий: 27 881

Ключевые слова	Дата и время	Источник	Код события	Категория задачи
Аудит успеха	23.02.2013 8:38:54	Microsoft Windows security auditing.	4634	Выход из системы
Аудит успеха	23.02.2013 8:38:53	Microsoft Windows security auditing.	4672	Специальный вход
Аудит успеха	23.02.2013 8:38:53	Microsoft Windows security auditing.	4624	Вход в систему
Аудит успеха	23.02.2013 8:38:53	Microsoft Windows security auditing.	4648	Вход в систему
Аудит успеха	23.02.2013 0:05:50	Microsoft Windows security auditing.	4672	Специальный вход
Аудит успеха	23.02.2013 0:05:50	Microsoft Windows security auditing.	4624	Вход в систему
Аудит успеха	23.02.2013 0:03:14	Microsoft Windows security auditing.	4905	Аудит изменения политики
Аудит успеха	23.02.2013 0:03:14	Microsoft Windows security auditing.	4904	Аудит изменения политики
Аудит успеха	23.02.2013 0:02:10	Microsoft Windows security auditing.	4672	Специальный вход
Аудит успеха	23.02.2013 0:02:10	Microsoft Windows security auditing.	4624	Вход в систему
Аудит успеха	23.02.2013 0:02:09	Microsoft Windows security auditing.	4672	Специальный вход
Аудит успеха	23.02.2013 0:02:09	Microsoft Windows security auditing.	4624	Вход в систему
Аудит успеха	22.02.2013 23:51:37	Microsoft Windows security auditing.	4672	Специальный вход
Аудит успеха	22.02.2013 23:51:37	Microsoft Windows security auditing.	4624	Вход в систему

Событие 4624, Microsoft Windows security auditing.

Общие | Подробности

Вход с учетной записью выполнен успешно.

Субъект:
ИД безопасности: система
Имя учетной записи: BPN-ПК$

Имя журнала: Безопасность
Источник: Microsoft Windows security
Дата: 23.02.2013 8:38:53
Код события: 4624
Категория задачи: Вход в систему
Уровень: Сведения
Ключевые слова: Аудит успеха
Пользов.: Н/Д
Компьютер: bpn-ПК
Код операции: Сведения
Подробности: Веб-справка журнала

Под **подозрительной активностью** понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям). Например, подсистема аудита, отслеживая процедуру входа (регистрации) пользователя в систему подсчитывает количество неудачных попыток входа. В случае превышения установленного порога таких попыток подсистема аудита формирует сигнал о блокировке учетной записи данного пользователя.

Регистрация и учет событий в информационной системе являются обязательными элементами защищенной информационной системы, позволяющими обеспечить важное для информационной безопасности свойство информационной инфраструктуры: подотчетность.

В параметрах регистрации событий доступа к объектам информационной системы должны фиксироваться:
дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
идентификатор субъекта доступа;
спецификация защищаемого файла;
имя программы (процесса, задания, задачи), осуществляющей доступ к файлу,
вид запрашиваемой операции (чтение, запись, удаление, выполнение,

Администрирование процессов регистрации событий, связанных с безопасностью информационной системы, включает три этапа:
сбор и хранение информации о событиях;
защита содержимого журнала регистрации;
анализ содержимого журнала регистрации.

Регистрация событий в информационной системе является сильным психологическим средством, напоминающим потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям – за возможные критические ошибки.
В свою очередь, эффективный аудит событий в информационной системе позволяет своевременно предупредить возможные инциденты информационной безопасности.

4. Защита информации при работе с ведомственных сетей и сетей общего пользования

Программные средства защиты

включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки – ограниченная функциональность сети, использование части ресурсов рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Организационные средства защит

складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия).

Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки – высокая зависимость от субъективных факторов.

Инструментальные средства анализа сетевого трафика

Системы обнаружения вторжений (IDS)

Обнаружение вторжений – это активный процесс, при котором происходит обнаружение хакера при его попытках проникнуть в систему. В идеальном случае такая система лишь выдаст сигнал тревоги при попытке проникновения. Обнаружение вторжений помогает при превентивной идентификации активных угроз посредством оповещений и предупреждений о том, что злоумышленник осуществляет сбор информации, необходимой для проведения атаки.

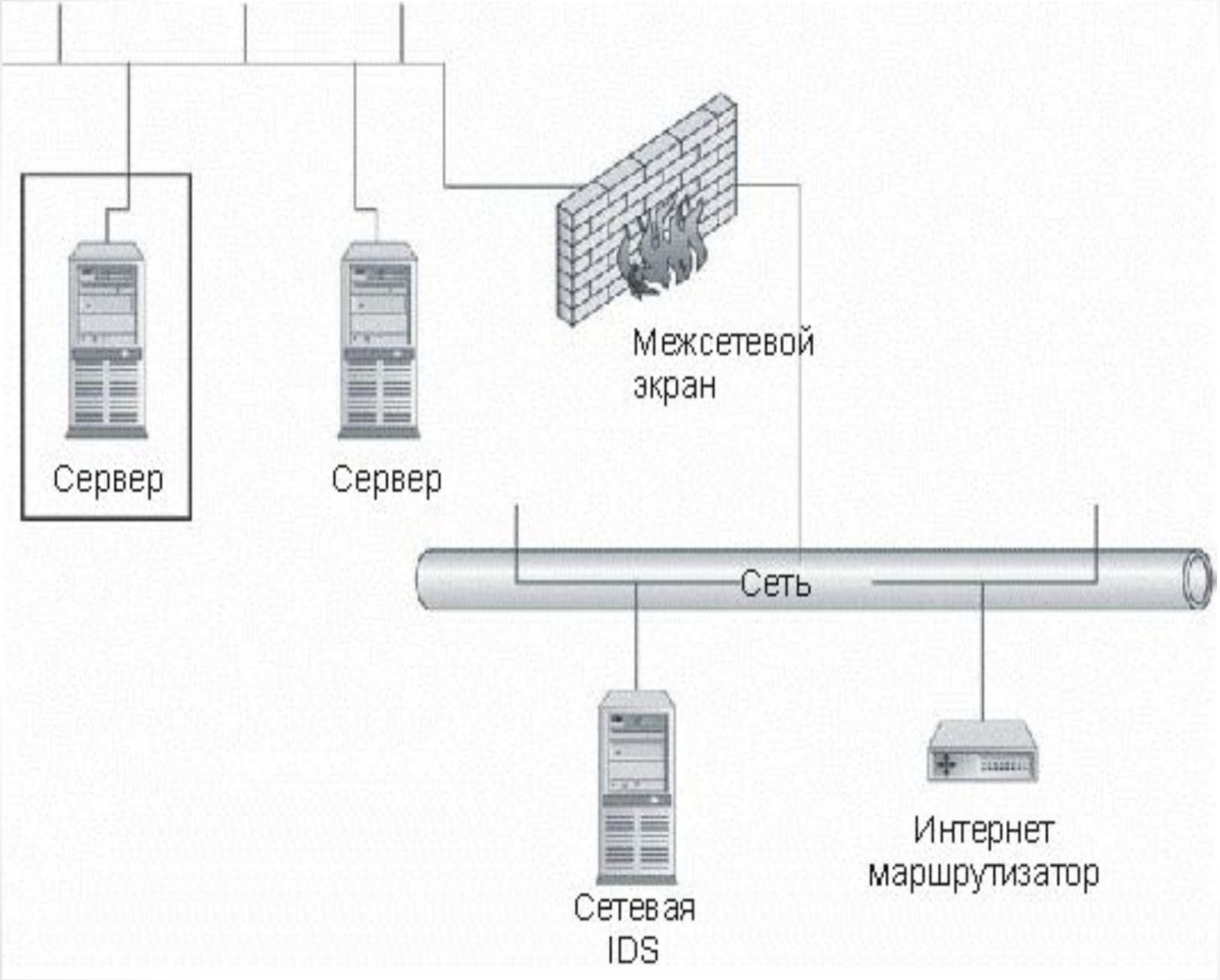
Определение типов систем обнаружения вторжений

Существуют два основных типа IDS: узловые (HIDS) и сетевые (NIDS).
Система HIDS располагается на отдельном узле и отслеживает признаки атак на данный узел.
Система NIDS находится на отдельной системе, отслеживающей сетевой трафик на наличие признаков атак, проводимых в подконтрольном сегменте сети.

Узловые IDS (HIDS) представляют собой систему датчиков, загружаемых на различные сервера организации и управляемых центральным диспетчером.

Датчики отслеживают различные типы событий и предпринимают определенные действия на сервере либо передают уведомления.

Датчики HIDS отслеживают события, связанные с сервером, на котором они загружены. Сенсор HIDS позволяет определить, была ли атака успешной, если атака имела место на той же платформе, на которой установлен датчик.


Сервер
Сервер
Межсетевой
экран
Сеть
Сетевая
IDS
Интернет
маршрутизатор

Существует пять основных типов датчиков HIDS:

- Анализаторы журналов.
- Датчики признаков.
- Анализаторы системных вызовов.
- Анализаторы поведения приложений.
- Контролеры целостности файлов.

Анализаторы журналов

Процесс выполняется на сервере и отслеживает соответствующие файлы журналов в системе.

Если встречается запись журнала, соответствующая некоторому критерию в процессе датчика HIDS, предпринимается установленное действие.

В большинстве случаев анализаторы журналов не способны предотвратить осуществляемую атаку на систему.

Датчики признаков

Датчики этого типа представляют собой наборы определенных признаков событий безопасности, сопоставляемых с входящим трафиком или записями журнала. Различие между датчиками признаков и анализаторами журналов заключается в возможности анализа входящего трафика.

Датчик признаков HIDS является полезным при отслеживании авторизованных пользователей внутри информационных систем.

Анализаторы системных вызовов

Анализаторы системных вызовов осуществляют анализ вызовов между приложениями и операционной системой для идентификации событий, связанных с безопасностью.

Когда приложению требуется выполнить действие, его вызов операционной системы анализируется и сопоставляется с базой данных признаков. Эти признаки являются примерами различных типов поведения, которые являют собой атакующие действия, или объектом интереса для администратора IDS.

HIDS данного типа могут предотвращать атаки.

Анализаторы поведения приложений

В анализаторах поведения датчик проверяет вызов на предмет того, разрешено ли приложению выполнять данное действие.

Например, веб-серверу обычно разрешается принимать сетевые соединения через порт 80, считывать файлы в веб-каталоге и передавать эти файлы по соединениям через порт 80. Если веб-сервер попытается записать или считать файлы из другого места, датчик обнаружит несоответствующее норме поведение сервера и заблокирует действие.

Контролеры целостности файлов

Контролеры целостности файлов отслеживают изменения в файлах. Это осуществляется посредством использования криптографической контрольной суммы или цифровой подписи файла. Конечная цифровая подпись файла будет изменена, если произойдет изменение хотя бы малой части исходного файла (это могут быть атрибуты файла, такие как время и дата создания). Алгоритмы, используемые для выполнения этого процесса, разрабатывались с целью максимального снижения возможности для внесения изменений в файл с сохранением прежней подписи.

Сетевые IDS

NIDS представляет собой программный процесс, работающий на специально выделенной системе.

NIDS переключает сетевую карту в системе в неразборчивый режим работы, при котором сетевой адаптер пропускает весь сетевой трафик (а не только трафик, направленный на данную систему) в программное обеспечение NIDS. После этого происходит анализ трафика с использованием набора правил и признаков атак для определения того, представляет ли этот трафик какой-либо интерес. Если это так, то генерируется соответствующее событие.

На данный момент большинство систем NIDS базируется на признаках атак.

Чаще всего при применении NIDS используются две сетевые карты

Среди преимуществ использования NIDS можно выделить следующие моменты.

- NIDS можно полностью скрыть в сети таким образом, что злоумышленник не будет знать о том, что за ним ведется наблюдение.
- Одна система NIDS может использоваться для мониторинга трафика с большим числом потенциальных систем-целей.
- NIDS может осуществлять перехват содержимого всех пакетов, направляющихся на систему-цель.

Среди недостатков данной системы необходимо отметить следующие аспекты:

- Система NIDS может только выдавать сигнал тревоги, если трафик соответствует предустановленным правилам или признакам.
- NIDS может упустить нужный интересуемый трафик из-за использования широкой полосы пропускания или альтернативных маршрутов.
- Система NIDS не может определить, была ли атака успешной.
- Система NIDS не может просматривать зашифрованный трафик.
- В коммутируемых сетях требуются специальные конфигурации, без которых NIDS будет проверять не весь трафик.

Инструментальные средства тестирования системы защиты

Систему защиты корпоративной сети целесообразно считать достаточно надежной только при условии постоянного тестирования.

В идеале администратор безопасности должен собирать информацию о возможных атаках, систематизировать ее и периодически осуществлять проверки системы защиты путем моделирования возможных атак.

Брандмауэры

Брандмауэром (firewall) называется стена, сделанная из негорючих материалов и препятствующая распространению пожара.

В сфере компьютерных сетей брандмауэр (БМ) представляет собой барьер, защищающий от виртуального пожара – попыток злоумышленников вторгнуться в сеть.

Брандмауэр способствует реализации политики безопасности, которая определяет разрешенные службы, типы доступа к ним и является реализацией этой политики.

Брандмауэр представляет собой систему или комбинацию систем, позволяющих разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую.

Как правило, эта граница проводится между локальной сетью и Internet, хотя ее можно провести и внутри локальной сети предприятия.

Основная цель системы брандмауэра – управление доступом к защищаемой сети.

Он реализует политику сетевого доступа, вынуждая проходить все соединения с сетью через брандмауэр, где они могут быть проанализированы, а затем разрешены либо отвергнуты.

Виртуальные сети

Ряд брандмауэров позволяет также организовывать виртуальные корпоративные сети (Virtual Private Network), т.е. объединить несколько локальных сетей, включенных в Internet в одну виртуальную сеть.

VPN позволяют организовать прозрачное для пользователей соединение локальных сетей, сохраняя секретность и целостность передаваемой информации с помощью шифрования.

При этом при передаче по INTERNET шифруются не только данные пользователя, но и сетевая информация – сетевые адреса, номера портов и т.д.

Межсетевые экраны и их организация

Межсетевой экран – это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных.

Межсетевой экран представляет собой средство защиты, которое пропускает определенный трафик из потока данных.

5. Антивирусная защита информации

Основная особенность компьютерных вирусов, заключающаяся в возможности их самопроизвольного внедрения в различные объекты операционной системы, присуща многим программам, которые не являются вирусами, но именно эта особенность является обязательным (необходимым) свойством компьютерного вируса. К более полной характеристике современного компьютерного вируса следует добавить способность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети или файлы, системные области компьютера и прочие выполняемые объекты.

Определение вируса, содержащееся в ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»:

Компьютерный вирус – вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы.

Вредоносная программа – программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

Несмотря на все усилия разработчиков антивирусного программного обеспечения, до сегодняшнего дня нет 100% надежных антивирусных средств, а противостояние «вирусописателей» и их оппонентов будет постоянным.

Исходя из этого, необходимо понимать, что нет достаточных программных и аппаратных средств защиты от вирусов, а надежная защита от вирусов может быть обеспечена комплексным применением этих средств и, что немаловажно, соблюдением элементарной «компьютерной гигиены».

По деструктивным возможностям вирусы можно разделить на:
безвредные, т.е. никак не влияющие на работу компьютера;
неопасные, влияние которых ограничивается уменьшением свободной памяти на диске;
опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожению данных, стиранию необходимой для работы компьютера информации, записанной в системных областях памяти, и даже повреждению аппаратных средств компьютера.

К «вредным программам», помимо вирусов, относятся: «троянские программы» (логические бомбы) и утилиты скрытого администрирования удаленных компьютеров.

К «троянским» программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий. Например, уничтожение информации на дисках при каждом запуске или по определенному графику.

Программы – «злые шутки» используются для устрашения пользователя: о заражении вирусом или о каких либо предстоящих действиях с этим связанных, т.е. сообщают о несуществующих опасностях, вынуждая пользователя к активным действиям.

Например, к «злым шуткам» относятся программы, которые «пугают» пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения.

Утилиты скрытого администрирования являются разновидностью «логических бомб» («троянских программ»), которые используются злоумышленниками для удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. При запуске такая программа устанавливает себя в систему и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях программы в системе. Чаще всего ссылка на такую программу отсутствует в списке активных приложений.

В результате пользователь не знает о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером все, что в них заложено автором: принимать/отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т.д.

Эти программы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т.п.

Вирусы могут удалить или зашифровать важные данные (фото, видео, рабочие файлы) без возможности восстановления

Вирусы могут заблокировать доступ к сайтам или перенаправить на подставной

Вирусы могут заблокировать доступ к Windows и потребовать денег для разблокировки

Мошенники могут взломать вашу почту, аккаунт соц. сети и использовать их в своих целях

Мошенники могут украсть ваши деньги из платежных систем, банковских карт

Мошенники могут украсть ваши персональные данные и использовать их в своих целях

Вирусы могут установить рекламные баннеры на рабочий стол и в браузеры

Вирусы могут испортить аппаратную часть компьютера (процессор, CD/DVD привод, жесткий диск, оперативную память, видеокарту)

Вирусы могут использовать ресурсы Вашего компьютера для интернет-атак на сайты

Одним из наиболее эффективных способов борьбы с вирусами является использование антивирусного программного обеспечения. **Антивирусная программа** – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

«Ложное срабатывание» – детектирование вируса в незараженном объекте (файле, секторе или системной памяти).

«Пропуск вируса» – недетектирование вируса в зараженном объекте.

«Сканирование по запросу» – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.

«Сканирование на лету» – постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т.п.). В этом режиме антивирус постоянно активен, он присутствует в памяти «резидентно» и проверяет

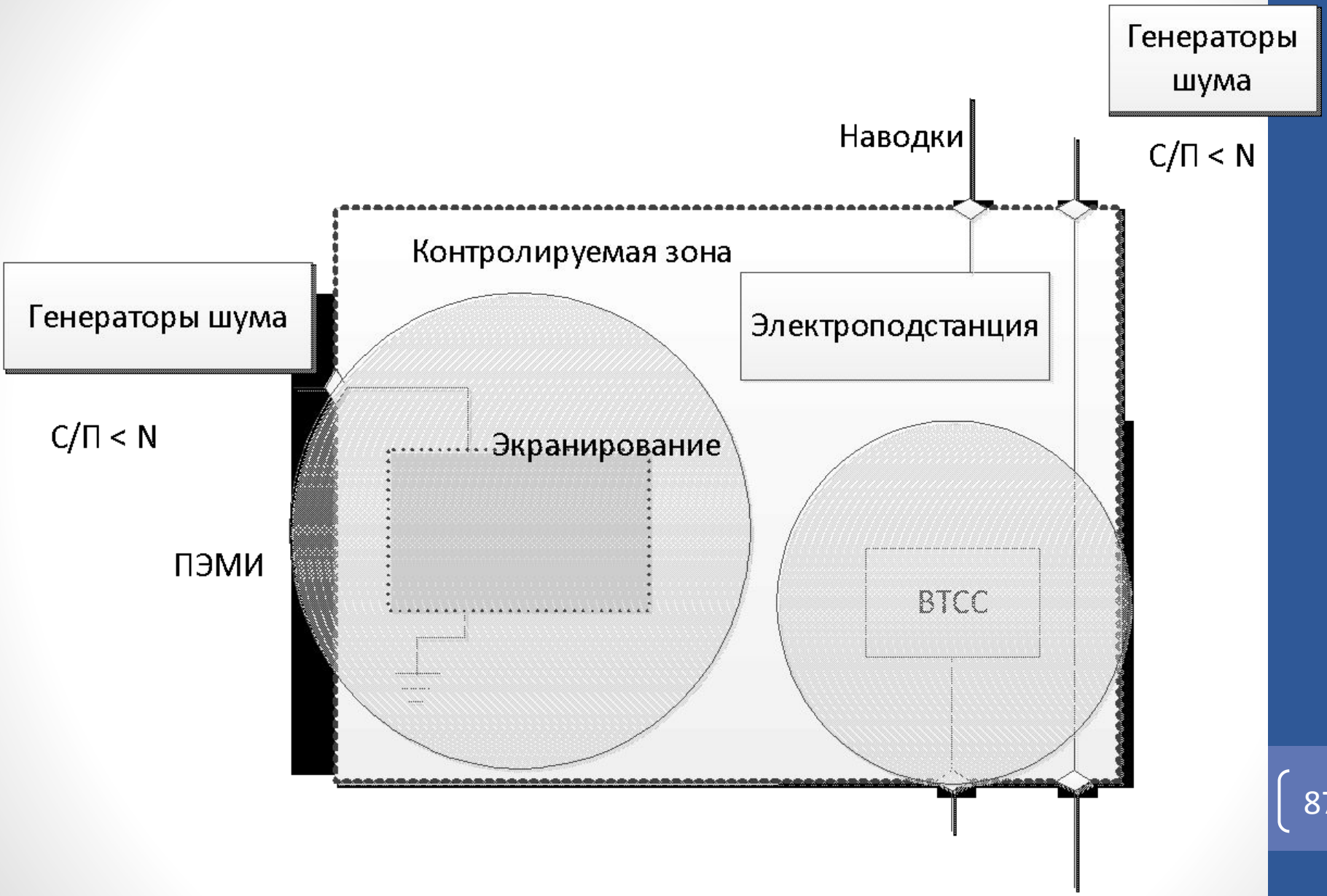
Самыми популярными и эффективными антивирусными программами являются ***антивирусные сканеры***, ***CRC-сканеры (ревизоры)***.

Существуют также ***антивирусы блокировщики и иммунизаторы.***

Принцип работы ***антивирусных сканеров*** основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов.
Для поиска известных вирусов используются так называемые «***маски***».
Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса.

Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы.
Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфных (изменяющих форму) вирусов.

6. Защита информации от утечки по техническим каналам


Генераторы шума
С/П < N
Наводки
Генераторы шума
С/П < N
Контролируемая зона
Электроподстанция
Экранирование
ПЭМИ
ВТСС

Технические (аппаратные) средства

Различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи *защиты информации*. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др.

Вторую – генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные *каналы утечки информации* или позволяющих их обнаружить.

Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны – недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

Необходимо постоянно осуществлять контроль функционирования системы информационной безопасности, анализ уязвимостей и новых угроз, а также степени опасности существующих угроз информационной безопасности.

Непрерывное совершенствование и развитие системы информационной безопасности возможно только на основе непрерывного контроля и анализа функционирующей системы информационной безопасности.

7. Шифрование (криптография)

Основные понятия шифрования

Шифрование представляет собой сокрытие информации от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней. Пользователи называются авторизованными, если у них есть соответствующий ключ для дешифрования информации.

Целью любой системы шифрования является максимальное усложнение получения доступа к информации неавторизованными лицами, даже если у них есть зашифрованный текст и известен алгоритм, использованный для шифрования. Пока неавторизованный пользователь не обладает ключом, секретность и целостность информации не нарушается.

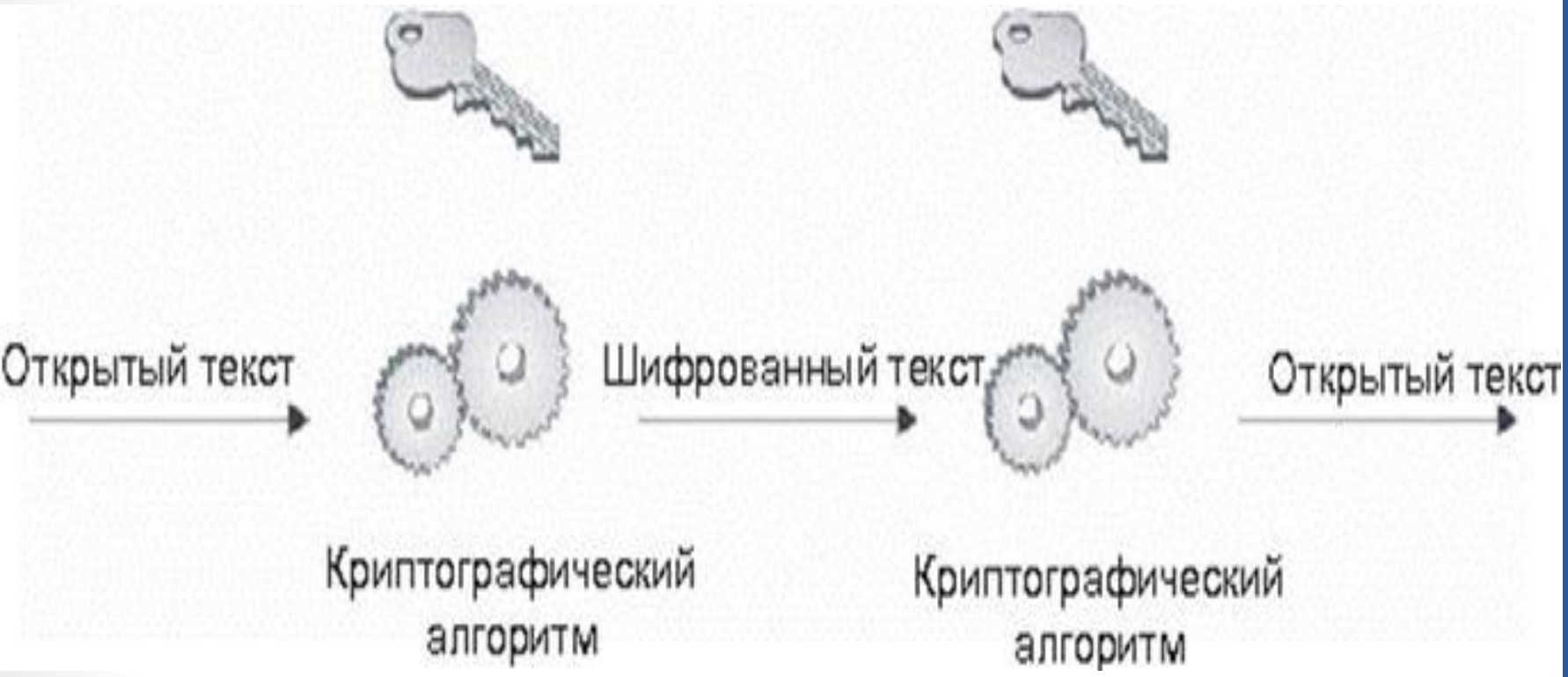
С помощью шифрования обеспечиваются три состояния безопасности информации:

- *Конфиденциальность*. Шифрование используется для сокрытия информации от неавторизованных пользователей при передаче или при хранении.
- *Целостность*. Шифрование используется для предотвращения изменения информации при передаче или хранении.
- *Идентифицируемость*. Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

- *Обычный текст* – информация в исходном виде. Также называется открытым текстом.
- *Шифрованный текст* – информация, подвергнутая действию алгоритма шифрования.
- *Алгоритм* – метод, используемый для преобразования открытого текста в шифрованный текст.
- Ключ – Входные данные, посредством которых с помощью алгоритма происходит преобразование открытого текста в шифрованный или обратно.
- Шифрование – Процесс преобразования открытого текста в шифр.
- Дешифрование – Процесс преобразования шифра в открытый текст.

- Криптография – наука о сокрытии информации с помощью шифрования.
- Криптограф – лицо, занимающееся криптографией.
- Криптоанализ – искусство анализа криптографических алгоритмов на предмет наличия уязвимостей.
- Криптоаналитик – лицо, использующее криптоанализ для определения и использования уязвимостей в криптографических алгоритмах.

«Простейшие методы шифрования текста»


Открытый текст
Криптографический алгоритм
Шифрованный текст
Криптографический алгоритм
Открытый текст

Хитроумный способ шифрования был изобретён в древней Спарте во времена Ликурга (V век до н.э.).

Для зашифровывания текста использовалась Сциталла - жезл цилиндрической формы, на который наматывалась лента из пергамента. Вдоль оси цилиндра построчно записывался текст, лента сматывалась с жезла и передавалась адресату, имеющему Сциталлу такого же диаметра.

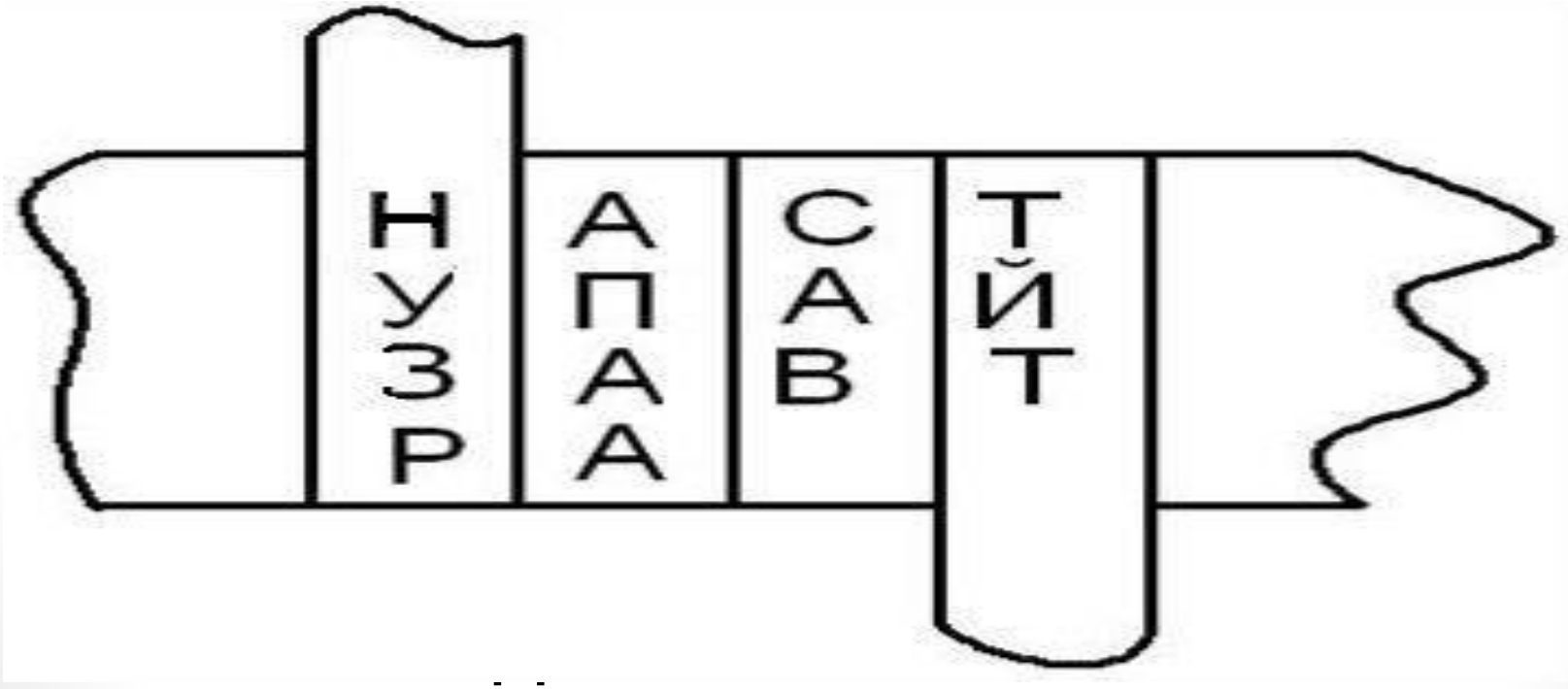
Этот способ осуществлял перестановку букв сообщения. Ключом шифра служил диаметр Сциталлы.

АРИСТОТЕЛЬ придумал метод вскрытия такого шифра. Он изобрёл дешифровальное устройство «Антисциталла».

Проверь себя

Расшифруйте сообщение, переданное спартанцу в V век до н. э.

НУЗРАПААСАВТЙТ



Греческий писатель ПОЛИБИЙ использовал систему сигнализации, которая применялась как метод шифрования. С его помощью можно было передавать абсолютно любую информацию. Он записывал буквы алфавита в квадратную таблицу и заменял их координатами.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I\J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Устойчивость этого шифра была велика. Основная причина - возможность постоянно менять в квадрате последовательность букв.

Проверь себя

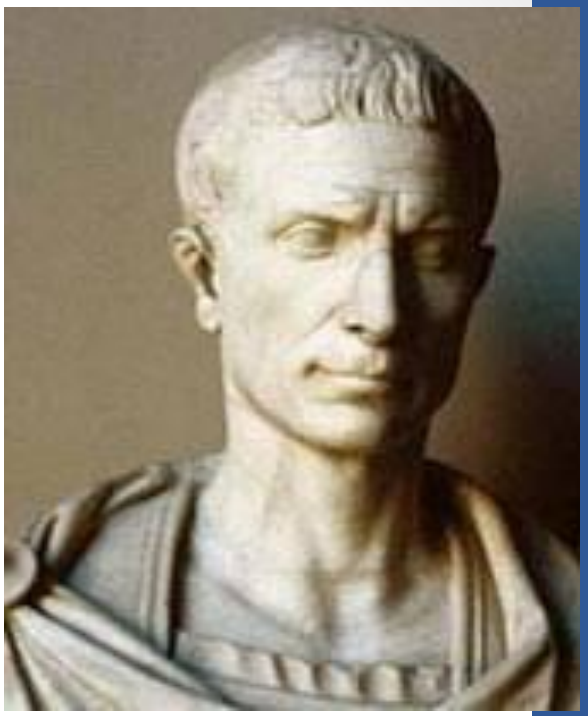
Расшифруйте сообщение,

6364433216626436111234421142546441645224443634326564116442556 6

Я умею работать с шифром! А ты?

Алгоритм шифрования:
первая цифра кода – номер строки,
вторая – номер столбца.

Особую роль в сохранении тайны сыграл способ шифрования, предложенный ЮЛИЕМ ЦЕЗАРЕМ и описанный им в «Записках о галльской войне» (1 век до н.э.) Ключом в шифре Цезаря является величина сдвига на 3.



Закодируем слово КОД

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

Получаем слово НСЖ

Проверь себя

Расшифруйте сообщение

ТУЛЫИО, ЦЕЛЖЗО,ТСДЗЖЛО!

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

Алгоритм шифрования: читать четвертую букву вместо первой.

Существует несколько модификаций шифра Цезаря. Один из них алгоритм шифра Гронсфельда (созданный в 1734 году бельгийцем Хосе де Бронкхором, графом де Гронсфельд, военным и дипломатом). Шифрование заключается в том, что величина сдвига не является постоянной, а задается ключом (гаммой).

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

При заданном ключе 317413327121 из шифротекста НСПУУСЁТЖХКА получает

Криптография

Для того, кто передаёт шифровку, важна её устойчивость к дешифрованию. Эта характеристика шифра называется **криптостойкостью**. Повысить криптостойкость позволяют шифры много алфавитной или многозначной замены. В таких шифрах каждому символу открытого алфавита ставятся в соответствие не один, а несколько символов шифровки.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

Научные методы в криптографии впервые появились в арабских странах. Арабского происхождения и само слово шифр (от арабского «цифра»). Арабы первыми стали заменять буквы цифрами с целью защиты исходного текста. Первая книга, специально посвящённая описанию некоторых шифров, появилась в 855г., она называлась «Книга о большом стремлении человека разгадать загадки древней письменности».

Итальянский математик и философ ДЖЕРОЛАМО КАРДАНО написал книгу "О тонкостях", в которой имеется часть, посвященная криптографии.

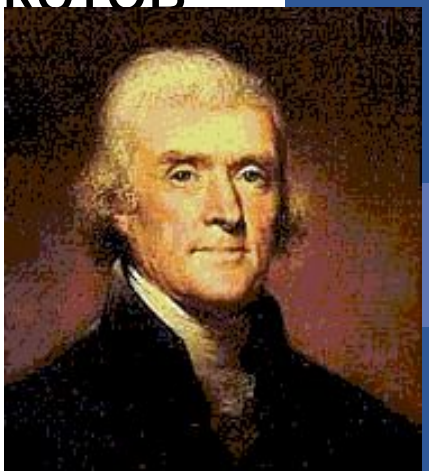
Кардано дает "доказательство" стойкости шифров, основанное на подсчете числа ключей, предлагает использовать открытый текст в качестве ключа, и новый шифр, "Решетка Кардано". Решётка представляет собой лист из твердого материала, в котором через неправильные интервалы сделаны прямоугольные вырезы высотой для одной строчки и различной длины. На лист накладывали эту решетку и записывали в вырезы секретное сообщение. Оставшиеся м заполнялись произвольным текстом.

Увлекались тайнописью и в России. Используемые шифры - такие же, как в западных странах - значковые, замены, перестановки.

Датой появления криптографической службы в России считают 1549 год, момента образования "посольского приказа", в котором имелось "цифирное отделение". Петр I полностью реорганизовал криптографическую службу, создав "Посольскую канцелярию".

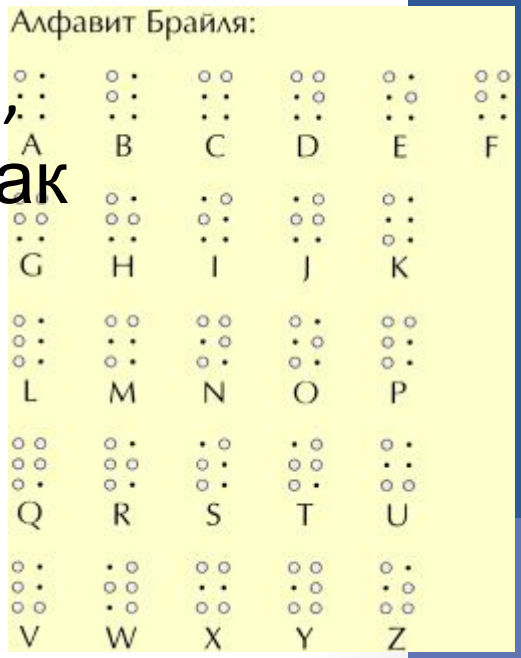
Много новых идей в криптографии принес XIX век. ТОМАС ДЖЕФФЕРСОН создал шифровальную систему, занимающую особое место в истории криптографии - "дисковый шифр". Этот шифр реализовывался с помощью специального устройства - шифратора Джефферсона.

В 1817 г. ДЕСИУС УОДСВОРТ сконструировал принципиально новое шифровальное устройство, Нововведение состояло в том, что он сделал алфавиты открытого и шифрованного текстов различных длин.



Способов кодирования информации можно привести много.

Капитан французской армии ШАРЛЬ БАРБЬЕ разработал в 1819 году систему кодирования ecriture noctrume – ночное письмо. В системе применялись выпуклые точки и тире, недостаток системы её сложность, так как кодировались не буквы, а звуки. ЛУИ БРАЙЛЬ усовершенствовал систему, разработал собственный шифр. Основы этой системы используются и сейчас.



СЭМЮЕЛЬ МОРЗЕ разработал в 1838 году систему кодирования символов с помощью точки и тире.

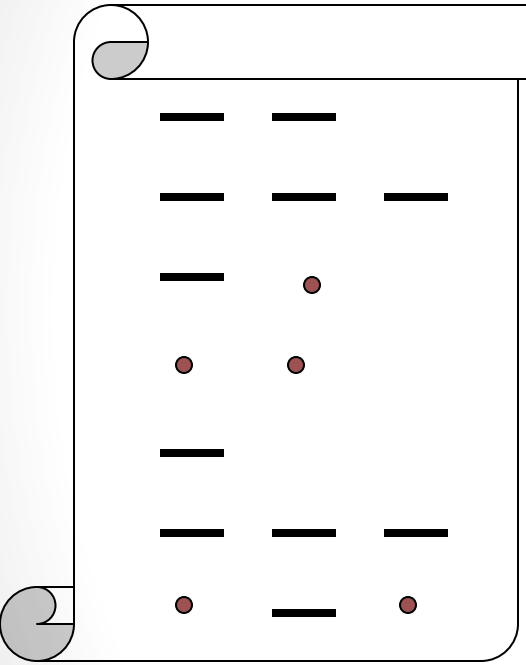
Он является изобретателем телеграфа (1837год) – устройства в котором использовалась эта система. Самое важное в этом изобретении – двоичный код,- использование для кодирования букв только двух символов.

А ·–	Б –···	В ·––	Г ––·	Д –··
Е ·	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 ·–·–		

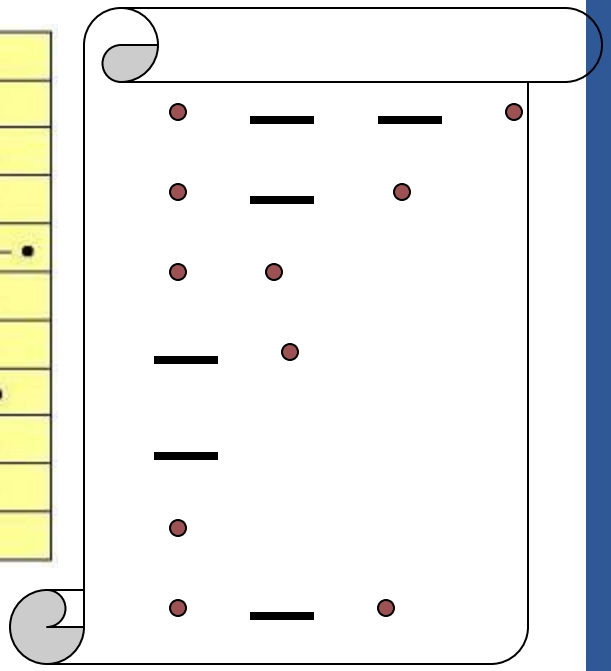
1 ·––––	2 ··–––	3 ···––	4 ····–
5 ·····	6 –····	7 ––···	8 –––··
9 ––––·	0 –––––		

Проверь себя

Расшифруйте сообщение, используя азбуку Морзе



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



В конце XIX века криптография начинает приобретать черты точной науки, а не только искусства, ее начинают изучать в военных академиях. В одной из них был разработан свой собственный военно-полевой шифр, получивший название "Линейка Сен-Сира".

В 80-х годах XIX века ОГЮСТ КЕРКГОФФС издал книгу "Военная криптография" объемом всего в 64 страницы, но они обессмертили его имя в истории криптографии. В ней сформулированы шесть конкретных требований к шифрам. Все эти требования актуальны и в наши дни.

Во второй половине XX века, вслед за развитием элементной базы вычислительной техники, появились электронные шифраторы. Сегодня они составляют подавляющую долю средств шифрования, удовлетворяя все возрастающим требованиям по надежности и скорости шифрования. В семидесятых годах был принят и опубликован первый стандарт шифрования данных (DES), "легализовавший" принцип Керкгоффса в криптографии; после работы американских математиков У. ДИФФИ и М. ХЕЛЛМАНА родилась "новая криптография"— **криптография с открытым ключом.**

8. Электронная подпись

Электронная подпись: алгоритмы, открытый и секретный ключи, сертификаты

Электронная подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствии искажения в электронном документе.

Открытый и закрытый ключи в электронной подписи

Электронная подпись функционирует на основе криптоалгоритмов с асимметричными (открытыми) ключами и инфраструктуры открытых ключей. В криптосистемах на основе асимметричных ключей для шифрования и дешифрования используется пара ключей – *секретный* и *публичный ключи*, уникальные для каждого пользователя, и *цифровой сертификат*.

Основные термины, применяемые при работе с ЭП:

закрытый ключ – это некоторая информация, обычно длиной 256 бит, хранится в недоступном другим лицам месте на смарт-карте, touch memory. Работает закрытый ключ только в паре с открытым ключом.

Открытый ключ – используется для проверки ЭП получаемых документов-файлов технически это некоторая информация длиной 1024 бита. Открытый ключ работает только в паре с закрытым ключом.

На открытый ключ выдается сертификат, который автоматически передается вместе с письмом, подписанным ЭП. Необходимо обеспечить наличие своего открытого ключа у всех, с кем предполагается обмениваться подписанными документами. Можно также удостовериться о личности, подписавшей электронной подписью документ, который получен, просмотрев его сертификат. Дубликат открытого ключа направляется в Удостоверяющий центр, где создана библиотека открытых ключей ЭП. В библиотеке Удостоверяющего центра обеспечивается регистрация и надежное хранение открытых ключей во избежание попыток подделки или внесения искажений.

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

В процессе формирования электронного ключа (электронный ключ ЭП), данные о его владельце сохраняются в отдельный файл. Этот файл и является сертификатом ключа подписи.

Выделяют также ***квалифицированный сертификат ключа*** проверки электронной подписи – сертификат, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Сертификат содержит следующую информацию:

- даты начала и окончания срока его действия;
- ФИО – для физических лиц, наименование и место нахождения – для юридических лиц или иная информация, позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи;
- ключ проверки электронной подписи;
- наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;
- наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи;
- иная информация для проверки сертификата ЭП, предусмотренная частью 2 статьи 17 ФЗ №63, – для квалифицированного сертификата.

Сертификат ключа подписи выдается, как правило, на 1 год и по истечении данного срока становится недействительным.

Для того чтобы продолжить работать в системе электронной документации, следует продлить сертификат.

При любом изменении реквизитов владельца ключа (смена руководителя организации, названия и т. д.), а также компрометации закрытого ключа требуется отозвать действующий сертификат и получить новый сертификат ключа проверки электронной подписи.

Удостоверяющий центр (УЦ) – это юридическое лицо (или индивидуальный предприниматель), которые обеспечивают изготовление сертификатов открытых ключей и управление (аннулирование, приостановление, возобновление) ими, а также выполняет иные функции, установленные законодательством Российской Федерации.

Задачи Удостоверяющего центра:

- ✔ изготовление сертификата ключа проверки электронной подписи. УЦ выдает такие сертификаты лицам, обратившимся за их получением (заявителям);
- ✔ устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- ✔ аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;
- ✔ выдает по обращению заявителя средства электронной подписи, содержащие
  - ✔ ключ электронной подписи и
  - ✔ ключ проверки электронной подписи
- ✔ или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

- ✔ ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей, в т.ч. включающий в себя информацию о сертификатах ключей проверки ЭП, и информацию о датах прекращения действия или аннулирования сертификатов и об основаниях таких прекращений или аннулирований;
- ✔ устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в т.ч. и через Интернет;
- ✔ создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;
- ✔ проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;
- ✔ осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;
- ✔ осуществляет иную связанную с использованием

Комплект для применения электронной подписи при выдаче ее удостоверяющим центром выглядит следующим образом:

Закрытый и открытый ключи.
Как правило, записаны на защищенном портативном устройстве (флеш-карта, токен или др. цифровой носитель), обеспечивающем хранение конфиденциальной информации.

Сертификат ключа подписи.
Это документ (на бумажном или электронном носителе), который подтверждает принадлежность ключей владельцу сертификата.

Дистрибутив программы Крипто-Про CSP, позволяющей осуществлять криптографические операции в операционных системах Microsoft.

Надежность ЭП

Технология изготовления подписи обеспечивает полноценную защиту электронных документов, их целостность и неоспоримое авторство.

Подделка электронной подписи практически невозможна. При ее формировании используются специальные схемы криптосистем. Расшифровка здесь не то что затруднительна, но практически нереализуема. Это, пожалуй, одно из главных преимуществ электронной подписи перед ее аналогами на бумажных документах, которые подделать сейчас значительно проще.

Виды ЭП

Согласно Федеральному закону №63-ФЗ, электронная подпись делится на три вида:

- ✔ Простая электронная подпись;
- ✔ Усиленная неквалифицированная электронная подпись;
- ✔ Усиленная квалифицированная электронная подпись.

Квалифицированная электронная подпись

Наиболее надежный вид ЭП – квалифицированная электронная подпись.

Она является равноценной заменой рукописной подписи и печати организации/ИП, проставляемых на бумажных документах.

В большинстве случаев, заменяет собственноручную подпись уполномоченного лица и печать, т.к. имеет ту же юридическую силу, как и реквизиты бумажного документа.

Главное назначение квалифицированной электронной подписи – защита электронных документов от подделки.

Также она используется для идентификации лица, подписавшего документ, и для защиты документа от просмотра и изменения третьими лицами.

Простая электронная подпись с помощью использования кодов, паролей или других средств подтверждает сам факт, что эта подпись была создана определенным лицом. Важная особенность, что с ее помощью нельзя проверить, был ли документ изменен с момента его подписания.

Обычно такая подпись используется при оформлении электронных сообщений, направляемых в органы государственной власти, местного самоуправления или должностным лицам.

Усиленная неквалифицированная электронная подпись позволяет не только определить автора документа, но и обнаружить факт внесения изменений в электронный документ после его подписания. Подпись создается использованием средств электронной подписи.

Процесс обмена сообщением:

- отправитель получает у удостоверяющего центра секретный ключ;
- используя этот ключ, формирует электронную цифровую подпись и отправляет письмо;
- получатель при помощи публичного (общедоступного) ключа и цифрового сертификата, полученного у удостоверяющего центра, устанавливает авторство документа и отсутствие

Схема выработки ЭП при асимметричном шифровании

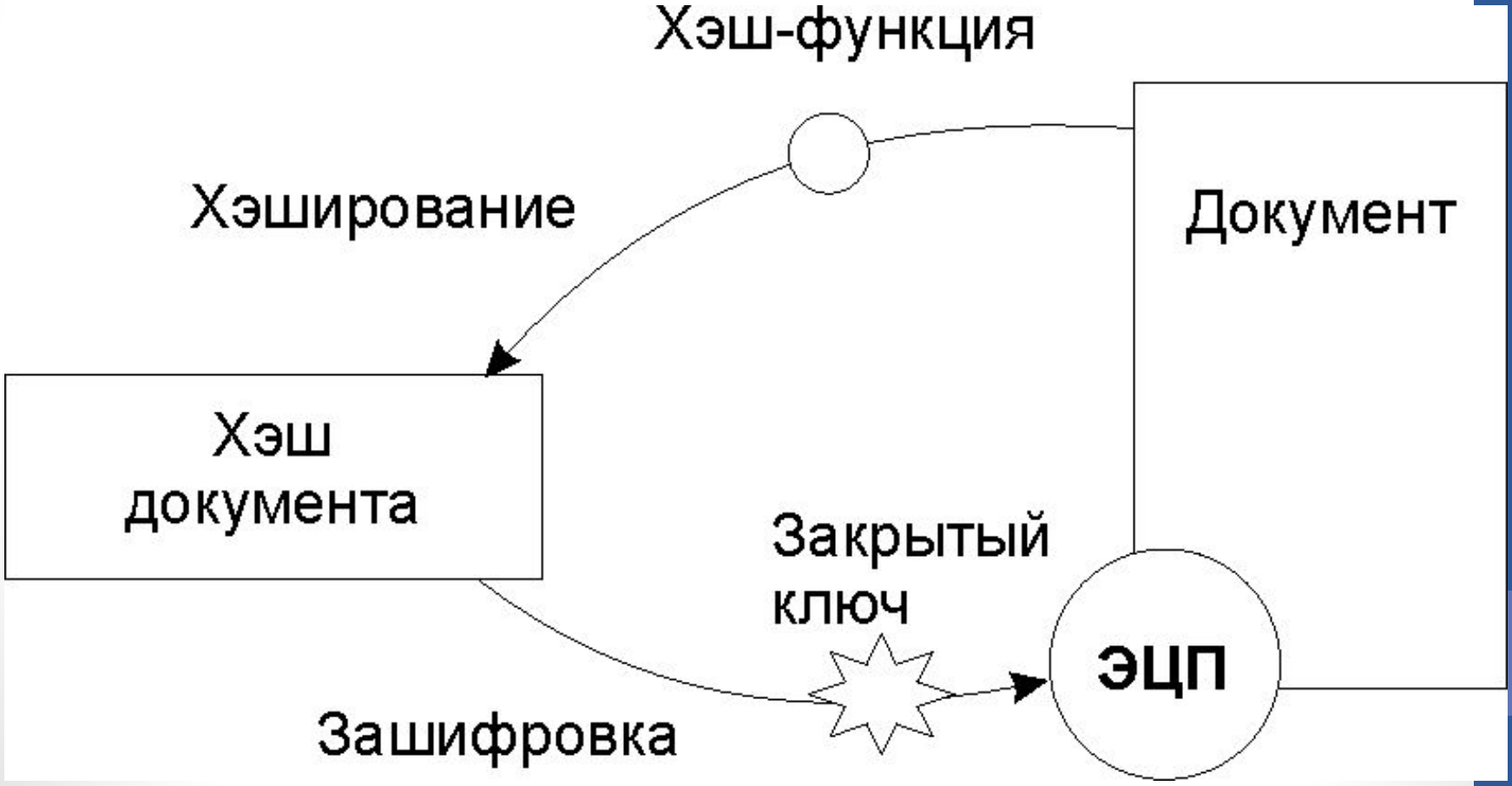
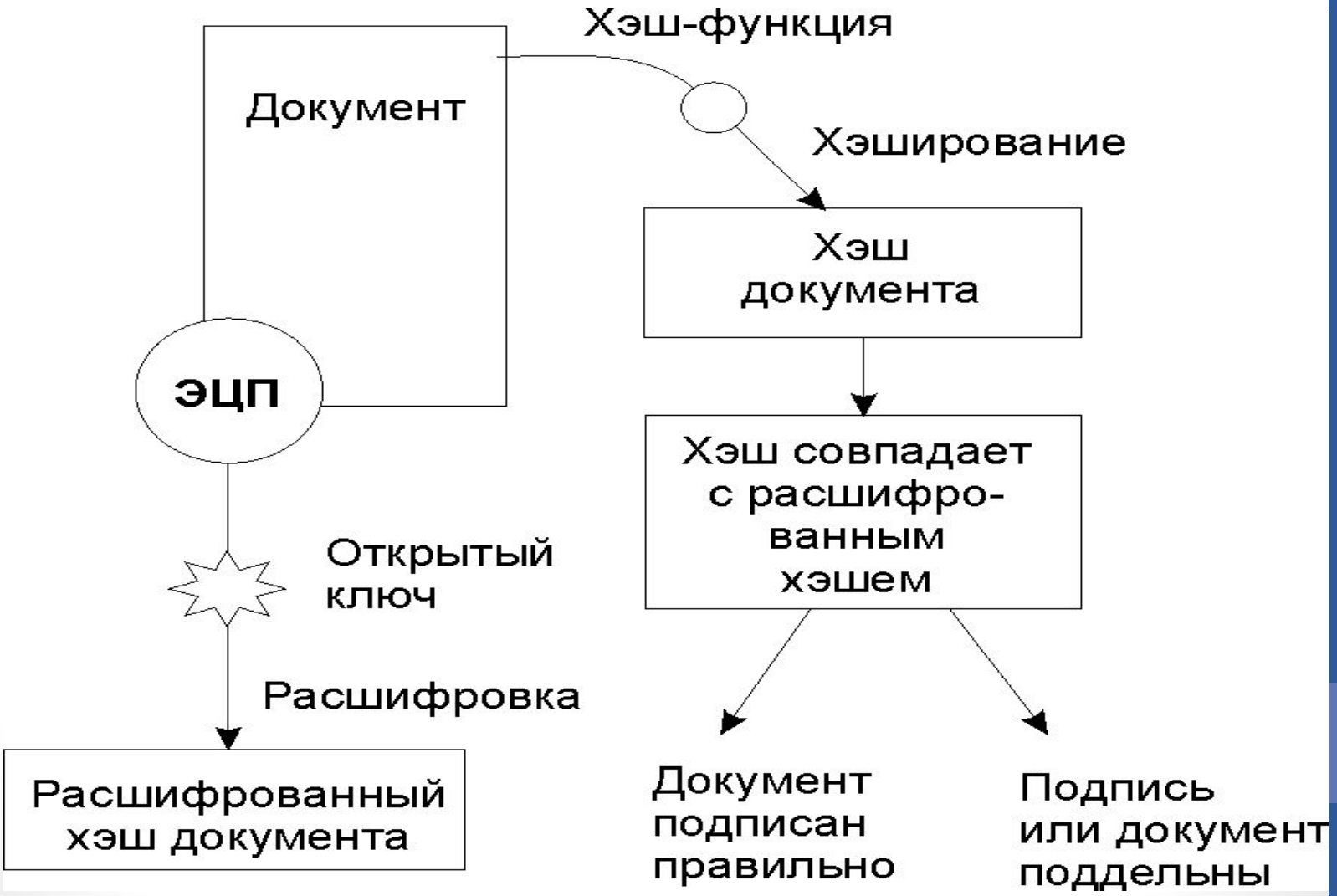


Схема проверки ЭП при асимметричном шифровании



Хеширование или **хэширование** - (англ. hashing) — преобразование массива входных данных произвольной длины в выходную) битовую строку фиксированной длины, выполняемое определенным алгоритмом.

Функция, реализующая алгоритм и выполняющая преобразование, называется «***хеш-функцией***» или «***функцией свёртки***».

Разновидности электронной подписи

Можно выделить 3 основных типа электронной подписи в зависимости от формы ее расположения:

Присоединенная ЭП. При ее формировании создается специальный отдельный файл электронной подписи, где находятся данные подписываемого документа. Этот процесс можно сравнить с опечатыванием конверта.

У этого типа подписи свои достоинства и недостатки:

К достоинству можно отнести простоту манипулирования с подписанными данными, так как все они содержатся вместе с подписями в одном файле, который можно копировать, пересылать и т. д.

К недостаткам – невозможность прочитать и использовать содержимое файла без применения специальных средств криптографической защиты.

Отсоединенная ЭП. В данном случае файл подписи формируется отдельно от подписываемого документа, который никак не изменяется. Поэтому подписанный файл можно читать, не прибегая к средствам криптографической защиты информации. А для проверки используются и файл с ЭП, и подписанный документ.

Однако, и здесь есть свой недостаток – необходимость хранения подписываемой информации в виде нескольких файлов, что весьма осложняет применение подписи.

ЭП внутри данных. ЭП такого типа значительно зависит от приложения, в котором используется (в частности внутри документов Microsoft Word или Acrobat Reader).
Вне приложения, создавшего электронную подпись, без знания структуры его данных проверить подлинность частей данных, подписанных электронной подписью достаточно сложно.

КриптоПро – линейка шифровальных программ - так называемых криптопровайдеров. Они используются во многих программах российских разработчиков для генерации электронной подписи (ЭП), работы с сертификатами, организации структуры PKI (открытых ключей) и т. д.

Компания КРИПТО-ПРО создана в 2000 году и в настоящее время занимает лидирующее положение по распространению средств криптографической защиты информации и электронной подписи.

«Крипто-Про» имеет лицензии ФСБ, ФАПСИ и Гостехкомисии, которые дают право осуществлять разработку, производство, распространение и сопровождению криптографических средств, предоставлять услуги по шифрованию информации.

Компания аккредитована ФАПСИ аттестационным центром в области криптографической защиты информации.

Один из наиболее популярных продуктов компании – КриптоПро CSP, разработанный в соответствии с криптографическим интерфейсом Microsoft - Cryptographic Service Provider (CSP), по согласованному с ФАПСИ техническому заданию.

КриптоПро CSP может использоваться для создания ключей шифрования и ключей электронной подписи, для шифрования, обеспечения целостности и подлинности

Электронный документооборот

	**Ключ директора** Применяется в информационных системах, использующих квалифицированный сертификат, изготовленный в соответствии с требованиями Федерального закона от 06.04.2011г. №63-ФЗ	4 000 р. Оформить заявку
	**Профессионал** Обладает всеми свойствами сертификата «Ключ директора», выдается на уполномоченное лицо	4 000 р. Оформить заявку
	**Росреестр** Сертификат предназначен для работы на портале Росреестра rosreestr.ru	3 000 р. Оформить заявку
	**Зеленый коридор** Сертификат предназначен для документооборота в рамках внешнеэкономической деятельности (ВЭД) между участниками ВЭД и органами Федеральной таможенной службы (ФТС России)	2 000 р. Оформить заявку