Защита данных

Шифрование

- **Шифрование** – использование криптографических сервисов безопасности.
- **Процедура шифрования** – преобразование открытого текста сообщения в закрытый.
- Современные средства шифрования используют известные алгоритмы шифрования. Для обеспечения конфиденциальности преобразованного сообщения используются специальные параметры преобразования – ключи.

Шифрование

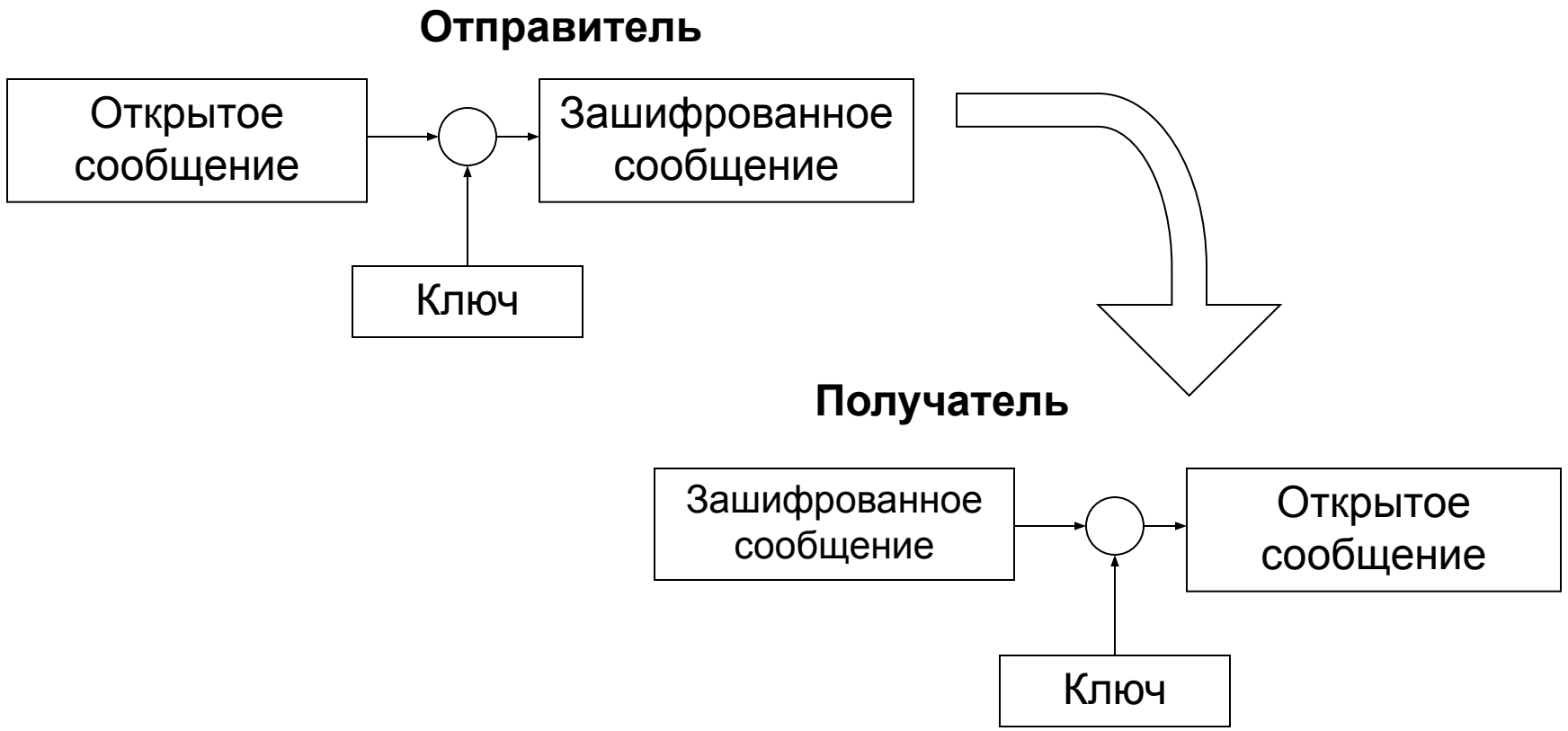
- Криптографические преобразования используются при реализации следующих сервисов безопасности:
  - Собственно шифрование (обеспечение конфиденциальности данных);
  - Контроль целостности;
  - Аутентификация.

Системы криптографической защиты информации

- Задача средств криптографической защиты информации — преобразование информационных объектов с помощью некоторого обратимого математического алгоритма.
- Процесс **шифрования** использует в качестве входных параметров объект – открытый текст и объект – ключ, а результат преобразования — объект – зашифрованный текст. При **дешифровании** выполняется обратный процесс.
- Криптографическому методу в ИС соответствует некоторый специальный алгоритм. При выполнении данного алгоритма используется уникальное числовое значение – **ключ**.
- Знание ключа позволяет выполнить обратное преобразование и получить открытое сообщения.
- Стойкость криптографической системы определяется используемыми алгоритмами и степенью секретности ключа.

Криптографические средства защиты данных

- Для обеспечения защиты информации в распределенных информационных системах активно применяются криптографические средства защиты информации.
- Сущность криптографических методов заключается в следующем:



Использование средств криптографической защиты для предотвращения угроз ИБ

- **Обеспечение конфиденциальности данных**. Использование криптографических алгоритмов позволяет предотвратить утечку информации. Отсутствие ключа у «злоумышленника» не позволяет раскрыть зашифрованную информацию;
- **Обеспечение целостности данных**. Использование алгоритмов несимметричного шифрования и хэширования делает возможным создание способа контроля целостности информации.
- **Электронная цифровая подпись.** Позволяет решить задачу отказа от информации.
- **Обеспечение аутентификации**. Криптографические методы используются в различных схемах аутентификации в распределенных системах (Kerberos, S/Key и др.).

Требования к системам криптографической защиты

- ***Криптографические требования***
  - Эффективность применения злоумышленником определяется **средней долей дешифрованной информации**, являющейся средним значением отношения количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию, и трудоемкостью дешифрования единицы информации, измеряемой Q числом элементарных опробований.
  - Под **элементарными опробованиями** понимается операция над двумя n-разрядными двоичными числами. При реализации алгоритма дешифрования может быть использован гипотетический вычислитель, объем памяти которого не превышает M двоичных разрядов. За одно обращение к памяти может быть записано по некоторому адресу или извлечено не более n бит информации. Обращение к памяти по трудоемкости приравнивается к элементарному опробованию.
  - За единицу информации принимается общий объем информации обработанной на одном средстве криптографической защиты в течении единицы времени. Атака злоумышленника является успешной, если объем полученной открытой информации больше некоторого заданного объема V.

Требования к системам криптографической защиты

- ***Требования надежности***.
- Средства защиты должны обеспечивать заданный уровень надежности применяемых криптографических преобразований информации, определяемый значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях.
- Регламентные работы (ремонт и сервисное обслуживание) средств криптографической защиты не должно приводить к ухудшению свойств средств в части параметров надежности.

Требования к системам криптографической защиты

- ***Требование по защите от несанкционированного доступа для средств криптографической информации в составе информационных систем.***
- В автоматизированных информационных системах, для которых реализованы программные или аппаратные средства криптографических защиты информации, при хранении и обработке информации должны быть предусмотрены следующие основные механизмы защиты:
  - идентификация и аутентификация пользователей и субъектов доступа;
  - управление доступом;
  - обеспечения целостности;
  - регистрация и учет.

Требования к системам криптографической защиты

- ***Требования к средствам разработки, изготовления и функционирования средств криптографической защиты информации.***
- Аппаратные и программные средства, на которых ведется разработка систем криптографической защиты информации, не должны содержать явных или скрытых функциональных возможностей, позволяющих:
  - модифицировать или изменять алгоритм работы средств защиты информации в процессе их разработки, изготовления и эксплуатации;
  - модифицировать или изменять информационные или управляющие потоки, связанные с функционированием средств;
  - осуществлять доступ посторонних лиц к ключам идентификационной и аутентификационной информации;
  - получать доступ к конфиденциальной информации средств криптографической защиты информации.

Способы шифрования

- Различают два основных способа шифрования:
  - **Симметричное шифрование**, иначе шифрование с закрытым ключом;
  - **Ассиметричное шифрование**, иначе шифрование с открытым ключом;

Шифрование с секретным ключом

- При симметричном шифровании процесс зашифровывания и расшифровывания использует некоторый *секретный ключ*.
- При симметричном шифровании реализуются два типа алгоритмов:
  - Поточное шифрование (побитовое)
  - Блочное шифрование (при шифровании текст предварительно разбивается на блоки, как правило не менее 64 бит)

Шифрование с секретным ключом

- Выделяют следующие общие принципы построения шифров:
  - электронная кодовая книга (режим простой замены);
  - сцепление блоков шифра (режим гаммирования с обратной связью);
  - обратная связь по шифротексту;
  - обратная связь по выходу (режим гаммирования).

Симметричное шифрование

- В процессе шифрования и дешифрования используется один и тот же параметр – секретный ключ, известный обеим сторонам
- Примеры симметричного шифрования:
  - ГОСТ 28147-89
  - DES
  - Blow Fish
  - IDEA
- Достоинство симметричного шифрования
  - Скорость выполнения преобразований
- Недостаток симметричного шифрования
  - Известен получателю и отправителю, что создает проблемы при распространении ключей и доказательстве подлинности сообщения

Симметричное шифрование

Алгоритм	Размер ключа	Длина блока	Число циклов	Основные операции
DES	56	64	16	Перестановка, подстановка, $\oplus$
FEAL	64, 128	64	<=4	Сложение по модулю 2^8, циклический сдвиг, $\oplus$
IDEA	128	64	8	Умножение по модулю $2^{16}+1$, сложение по модулю 2^{16}, $\oplus$
ГОСТ 28147-89	256	64	32	Сложение по модулю 2^{32}, подстановка, циклический сдвиг, $\oplus$
RC5	8t, t<=255	32, 64, 128	<= 255	Сложение по модулю 2^W, (W=1/2 длины блока), циклический сдвиг, $\oplus$
Blowfish	<=448	64	16	Сложение по модулю 2^{32}, подстановка, $\oplus$

Несимметричное шифрование

- В несимметричных алгоритмах шифрования ключи зашифровывания и расшифровывания всегда разные (хотя и связанные между собой).
- Ключ зашифровывания является несекретным (открытым), ключ расшифровывания – секретным.

Ассиметричное шифрование

- В криптографических преобразованиях используется два ключа. Один из них несекретный (открытый) ключ используется для шифрования. Второй, секретный ключ для расшифровывания.
- Примеры несимметричного шифрования:
  - RSA
  - Алгоритм Эль-Гамаля
- Недостаток асимметричного шифрования
  - низкое быстродействие алгоритмов (из-за длины ключа и сложности преобразований)
- Достоинства:
  - Применение асимметричных алгоритмов для решения задачи проверки подлинности сообщений, целостности и т.п.

Сравнение симметричных и несимметричных алгоритмов шифрования

- Преимущества симметричных алгоритмов:
  - Скорость выполнения криптографических преобразований
  - Относительная легкость внесения изменений в алгоритм шифрования
- Преимущества несимметричных алгоритмов
  - Секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа
  - Применение в системах аутентификации (электронная цифровая подпись)

Проверка подлинности

- Криптографические методы позволяют контролировать целостность сообщений, определять подлинность источников данных, гарантировать невозможность отказа от совершенных действий
- В основе криптографического контроля целостности лежат два понятия:
  - Хэш-функция;
  - Электронная цифровая подпись.

Проверка целостности сообщений

- Контроль целостности потока сообщений помогает обнаружить их повтор, задержку, переупорядочивание или утрату. Для контроля целостности сообщений можно использовать хэш-функцию.
- **Хэш-функция** – преобразование преобразующее строку произвольной длины в строку фиксированной длины и удовлетворяющее следующим свойствам:
  - Для каждого значения H(M) невозможно найти аргумент M – стойкость в смысле обращения;
  - Для данного аргумента M невозможно найти аргумент M’,что H(M) = H(M’) – стойкость в смысле возникновения коллизий.
- Хэш-функция используется:
  - Для создания сжатого образа сообщения, применяемого в ЭЦП;
  - Для защиты пароля;
  - Для построения кода аутентификации сообщений.

Контроль подлинности

- **Электронная цифровая подпись** выполняет роль обычной подписи в электронных документах для подтверждения подлинности сообщений – данные присоединяются к передаваемому сообщению, подтверждая подлинность отправителя сообщения.
- При разработке механизма цифровой подписи возникает три задачи:
  - создание подписи таким образом, чтобы ее невозможно было подделать;
  - возможность проверки того, что подпись действительно принадлежит указанному владельцу.
  - предотвращение отказа от подписи.

Алгоритм формирования электронной цифровой подписи

- При формировании цифровой подписи по классической схеме отправитель:
  - Применяет к исходному тексту хэш-функцию;
  - Дополняет хэш-образ до длины, требуемой в алгоритме создания ЭЦП;
  - Вычисляет ЭЦП по хэш-образу с использованием секретного ключа создания подписи.
- Получатель, получив подписанное сообщение, отделяет цифровую подпись от основного текста и выполняет проверку:
  - Применяет к тексту полученного сообщения хэш-функцию;
  - Дополняет хэш-образ до требуемой длины;
  - Проверяет соответствие хэш-образа сообщения полученной цифровой подписи с использованием открытого ключа проверки подписи.

Примеры алгоритмов формирования хэш-функции и ЭЦП

- В качестве распространенных алгоритмов хэширования можно указать:
  - MD5;
  - SHA;
  - ГОСТ Р34.11-94;
- Алгоритмы формирования электронной цифровой подписи:
  - RSA;
  - DSA;
  - ГОСТ Р34.10-94

Выбор алгоритмов аутентификации

- При выборе протоколов аутентификации, необходимо определить, какой тип аутентификации требуется – односторонняя или двусторонняя, наличие доверенной стороны и т.д.
- Параметры протокола аутентификации:
  - Тип алгоритма (симметричный, несимметричный);
  - Конкретный вид алгоритма;
  - Режим работы;
  - Процедура управления ключами;
  - Совместимость используемых алгоритмов.

Корпоративные системы

- **Контроль доступа к ресурсам**
- **Аутентификация, легализация пользователя**
- **Антивирусная защита в корпоративных системах**
- **Модель вероятностного контроля доступа к ресурсам**

- **Комплексный подход к реализации контроля доступа к ресурсам в корпоративных приложениях**

Локальные данные

- В **Windows** есть функция шифрования томов под названием **BitLocker**. Для защиты системного диска она требует наличия модуля TPM, который установлен далеко не во всех ПК или ноутбуках, но для прочих томов он не требуется.
- Также в Windows есть функция **BitLocker To Go** для защиты съёмных накопителей, которой тоже можно воспользоваться без аппаратного криптомодуля, а этого вполне достаточно для большинства пользователей.

Локальные данные

- В **Mac OS X** уже давно имеется встроенная система шифрования **FileVault**, а с версии 10.7 она позволяет защищать не только домашний каталог, но и сразу весь диск. Включить её можно в настройках системы в разделе «Защита и безопасность». Там же полезно будет отметить галочкой опцию защиты виртуальной памяти. При включении шифрования придётся задать мастер-пароль, если он ещё не задан, а также сохранить ключ восстановления.
- Впрочем, более универсальный метод — это использование зашифрованных образов диска.

Локальные данные

- **Ubuntu** ещё на этапе установки предлагает зашифровать домашний каталог пользователя. Одновременно с этим шифруется и раздел подкачки, что приводит к невозможности использования спящего режима. Если же вы отказались от шифрования при установке, то придётся настроить все вручную. При этом от защиты swap-раздела можно отказаться, что естественным образом снижает безопасность. Более удобный и защищённый, но и более сложный в настройке вариант — шифрование всего диска сразу.

Безопасное удаление

- **Единственный надёжный способ гарантированно удалить данные — это физическое уничтожение накопителя, на котором они находятся.** Для этого даже разработаны специальные процедуры, порой утончённо-извращённого садистского характера. А «виноваты» в этом различные технологии, которые используются в современных накопителях, — **остаточная намагниченность, TRIM-операции, равномерное распределение нагрузки, журналирование** и так далее. Суть их в целом сводится к тому, что данные зачастую помечаются как удалённые или готовые к удалению вместо того, чтобы быть действительно стёртыми. Поэтому были разработаны методики достаточно безопасного удаления **остаточной информации**, которые не столь радикальны, как полное уничтожение носителя.
- Функция безопасной очистки диска присутствует во многих редакторах разделов.

Прозрачное шифрование

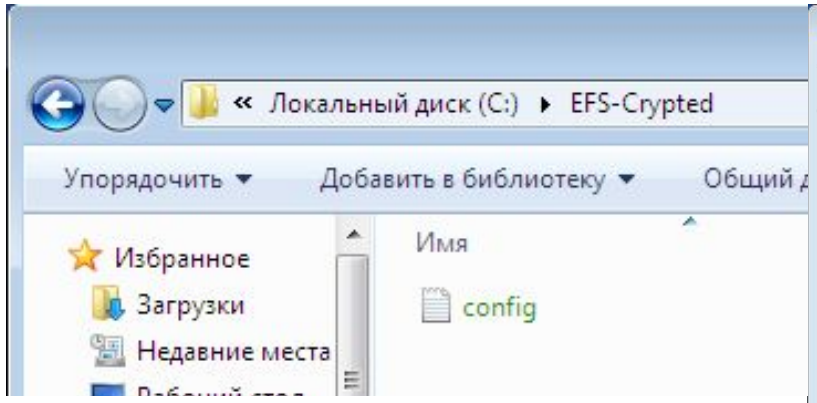
- В Windows (кроме Home-выпусков) традиционно для организации прозрачного шифрования используется шифрованная файловая система — EFS (Encrypting File System).
- EFS предназначена, чтобы один пользователь не мог получить доступ к файлам (зашифрованным) другого пользователя. Зачем нужно было создавать EFS, если NTFS поддерживает разграничение прав доступа? Хотя NTFS и является довольно безопасной файловой системой, но со временем появились различные утилиты (одной из первых была NTFSDOS, позволяющая читать файлы, находящиеся на NTFS-разделе, из DOS-окружения), игнорирующие права доступа NTFS. Появилась необходимость в дополнительной защите. Такой защитой должна была стать EFS.
  По сути, EFS является надстройкой над NTFS. EFS удобна тем, что входит в состав Windows и для шифрования файлов вам не нужно какое-либо дополнительное программное обеспечение — все необходимое уже есть в Windows. Для начала шифрования файлов не нужно совершать какие-либо предварительные действия, поскольку при первом шифровании файла для пользователя автоматически создается сертификат шифрования и закрытый ключ.
  Также преимуществом EFS является то, что при перемещении файла из зашифрованной папки в любую другую он остается зашифрованным, а при копировании файла в зашифрованную папку он автоматически шифруется.

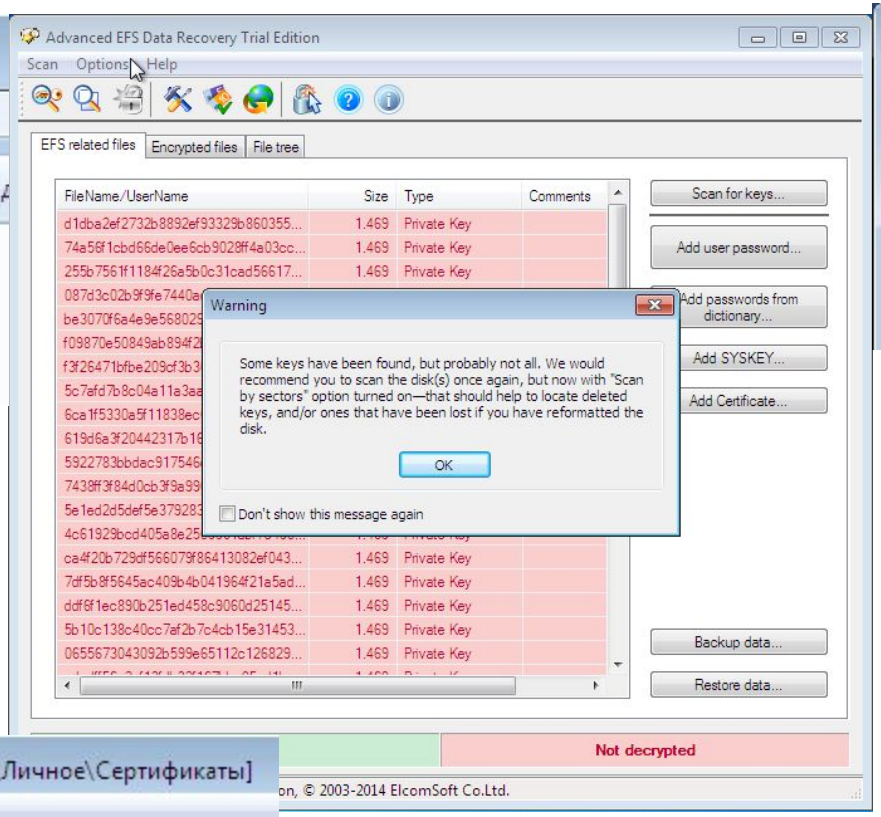
Прозрачное шифрование

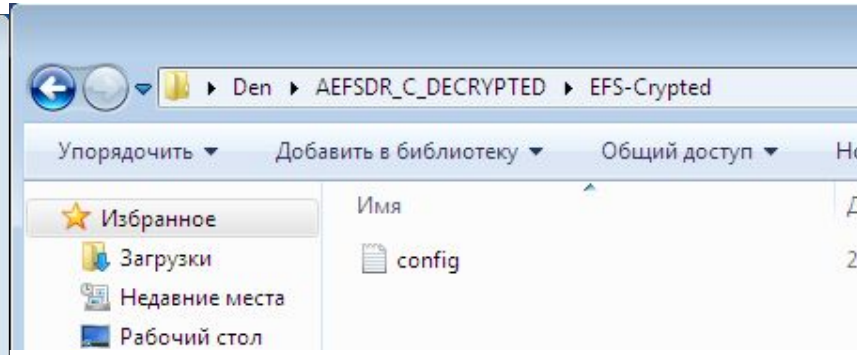
Такой подход, конечно же, очень удобен, и пользователю кажется, что от EFS одна только польза. Но это не так. С одной стороны, при неблагоприятном стечении обстоятельств, пользователь может вообще потерять доступ к зашифрованным файлам. Это может произойти в следующих случаях:

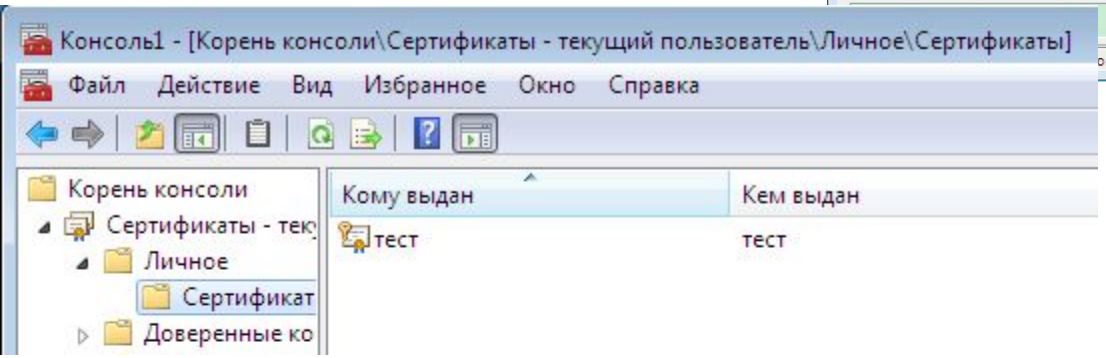
- Аппаратные проблемы, например, вышла из строя материнская плата, испорчен загрузчик, повреждены системные файлы из-за сбоя жесткого диска (bad sectors). В итоге жесткий диск можно подключить к другому компьютеру, чтобы скопировать с него файлы, но если они зашифрованы EFS, у вас ничего не выйдет.
- Система переустановлена. Windows может быть переустановлена по самым разнообразным причинам. В этом случае доступ к зашифрованным данным, понятно, будет потерян.
- Удален профиль пользователя. Даже если создать пользователя с таким же именем, ему будет присвоен другой ID, и расшифровать данные все равно не получится.
- Системный администратор или сам пользователь сбросил пароль. После этого доступ к EFS-данным также будет потерян.
- Некорректный перенос пользователя в другой домен. Если перенос пользователя выполнен неграмотно, он не сможет получить доступ к своим зашифрованным файлам.

Надёжно?


« Локальный диск (C:) ▸ EFS-Crypted
Упорядочить
Добавить в библиотеку
Общий
Избранное
Загрузки
Недавние места
Имя
config


Advanced EFS Data Recovery Trial Edition
Scan
Options
Help
EFS related files
Encrypted files
File tree
FileName/UserName
Size
Type
Comments
Scan for keys...
Add user password...
Add passwords from dictionary...
Add SYSKEY...
Add Certificate...
Backup data...
Restore data...
Warning
Some keys have been found, but probably not all. We would recommend you to scan the disk(s) once again, but now with "Scan by sectors" option turned on—that should help to locate deleted keys, and/or ones that have been lost if you have reformatted the disk.
OK
Don't show this message again
Not decrypted
© 2003-2014 ElcomSoft Co.Ltd.


Den ▸ AEFSDR_C_DECRYPTED ▸ EFS-Crypted
Упорядочить
Добавить в библиотеку
Общий доступ
Избранное
Загрузки
Недавние места
Рабочий стол
Имя
config


Консоль1 - [Корень консоли\Сертификаты - текущий пользователь\Личное\Сертификаты]
Файл
Действие
Вид
Избранное
Окно
Справка
Корень консоли
Сертификаты - тек
Личное
Сертификат
Доверенные ко
Кому выдан
Кем выдан
тест
тест

Утечка информации

- Она может быть перехвачена;
- Модификация информации (изменение исходного документа или сообщения либо его абсолютная подмена с последующей отсылкой адресату);
- Фальсификация авторства (если посылают любые данные от вашего имени);
- К серверу аппаратуры или линии связи может быть осуществлено незаконное подключение;
- Кто-то может замаскироваться под авторизованного пользователя и присвоить себе его данные и полномочия;
- Вводятся новые пользователи;
- После преодоления мер защиты носители информации и файлы могут быть скопированы;
- Неправильное хранение архивных данных;
- Некорректная работа обслуживающего персонала или пользователей;
- Внедрение компьютерного вируса;
- Недостатки вашей операционной системы или прикладных программных средств могут быть использованы против вас.

Средств защиты

- Средства аппаратного (или технического) характера;
- Программные меры защиты;
- Средства, которые относят к смешанному виду;
- Меры организационного или административного характера.

Средств защиты

Технические средства — электрические, электромеханические, электронные и др. типа устройства. *Преимущества* технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. *Слабые стороны* — недостаточная гибкость, относительно большие объём и масса, высокая стоимость.

Технические средства подразделяются на:

- аппаратные — устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с аппаратурой локальных сетей по стандартному интерфейсу (схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры);
- физические — реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения. Замки на дверях, решетки на окнах).

Средств защиты

Программные средства — программы, специально предназначенные для выполнения функций, связанных с защитой информации. А именно 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 файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Средств защиты

Смешанные аппаратно-программные средства

- **Смешанные аппаратно-программные средства** реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

Организационные средства

- **Организационные средства** 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, в том числе от общей организации работы в конкретном подразделении.
- В ходе развития концепции защиты информации специалисты пришли к выводу, что использование какого-либо одного из выше указанных способов защиты, не обеспечивает надежного сохранения информации. Необходим комплексный подход к использованию и развитию всех средств и способов защиты информации.

Важно помнить!

- **О Шифрование содержимого папок**
- При шифровании папки, внутри которой есть файлы или другие папки, Windows просит вас указать, нужно ли шифровать это содержимое. В большинстве случаев вы просто соглашаетесь. Если же вы в этом окне щелкнете на кнопке Нет (No), то текущее содержимое папки останется незашифрованным, однако новые файлы будут шифроваться.
- **О Зашифровано навсегда?**
- Невозможно гарантировать, что зашифрованный файл останется таковым навсегда. Например, некоторые приложения при редактировании и сохранении данных удаляют оригинальные файлы, а потом создают новые на том же месте. Если приложение не знает, что файл нужно шифровать, защита исчезает. Чтобы этого не происходило, необходимо шифровать родительскую папку, а не только сам файл.
- **О Защищено от других пользователей?**
- Если изменить владельца зашифрованного файла, то только предыдущий владелец создатель файла сможет расшифровать и просмотреть его, несмотря на то что файл ему уже не принадлежит. Это означает, что в некоторых случаях ни один пользователь не способен прочитать файл.

Важно помнить!

- **О Шифрование системных файлов**
- Поскольку доступ к определенным папкам, таким как \Windows и \Windows\System, нужен всем пользователям, шифрование файлов, системных папок и корневых каталогов любых дисков запрещено. Следовательно, единственный способ зашифровать подобные объекты — использовать шифрование всего диска, как рассказывается во врезке «Шифрование целого диска с помощью BitLocker».
- **О Шифрование и сжатие**
- Сжатие — еще одна возможность файловых систем NTFS — позволяет уменьшать количество места, которое занимают на диске файлы и папки. Принципы сжатия очень напоминают принципы шифрования. Однако для объекта нельзя одновременно использовать и шифрование, и сжатие; включите в окне Свойства (Properties) один параметр, и второй автоматически отключится.

Вы уверены, что ваши данные только ваши?