Нижегородская академия МВД России
Кафедра математики, информатики и информационных технологий

ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Лекция №4

План лекции

1. Парольная защита
2. Программные методы защиты данных
3. Вредоносные программы и борьба с ними

Парольная защита

1. Пароль должен быть секретным:

- недопустимо отображение пароля на экране;
- записанный пароль нельзя хранить в местах, доступных неавторизованным лицам;
- файл паролей должен иметь надежную криптографическую защиту;
- пароль следует хранить на внешнем носителе;
- на предложение программ запомнить пароль нужно всегда отвечать отказом

Парольная защита

2. Пароль должен быть длинным: не менее 8 символов
3. Пароль должен быть трудно угадываемым: недопустимо совпадение пароля с логином, использование в качестве пароля имени, фамилии, даты рождения, номеров телефонов пользователя и т.д.

Парольная защита

4. Пароль не должен представлять собой распространенные слова, имена, названия
5. Пароль должен быть сложным
6. Пароль должен регулярно меняться
7. Пароль должен значительно отличаться от паролей, использовавшихся ранее

Парольная защита

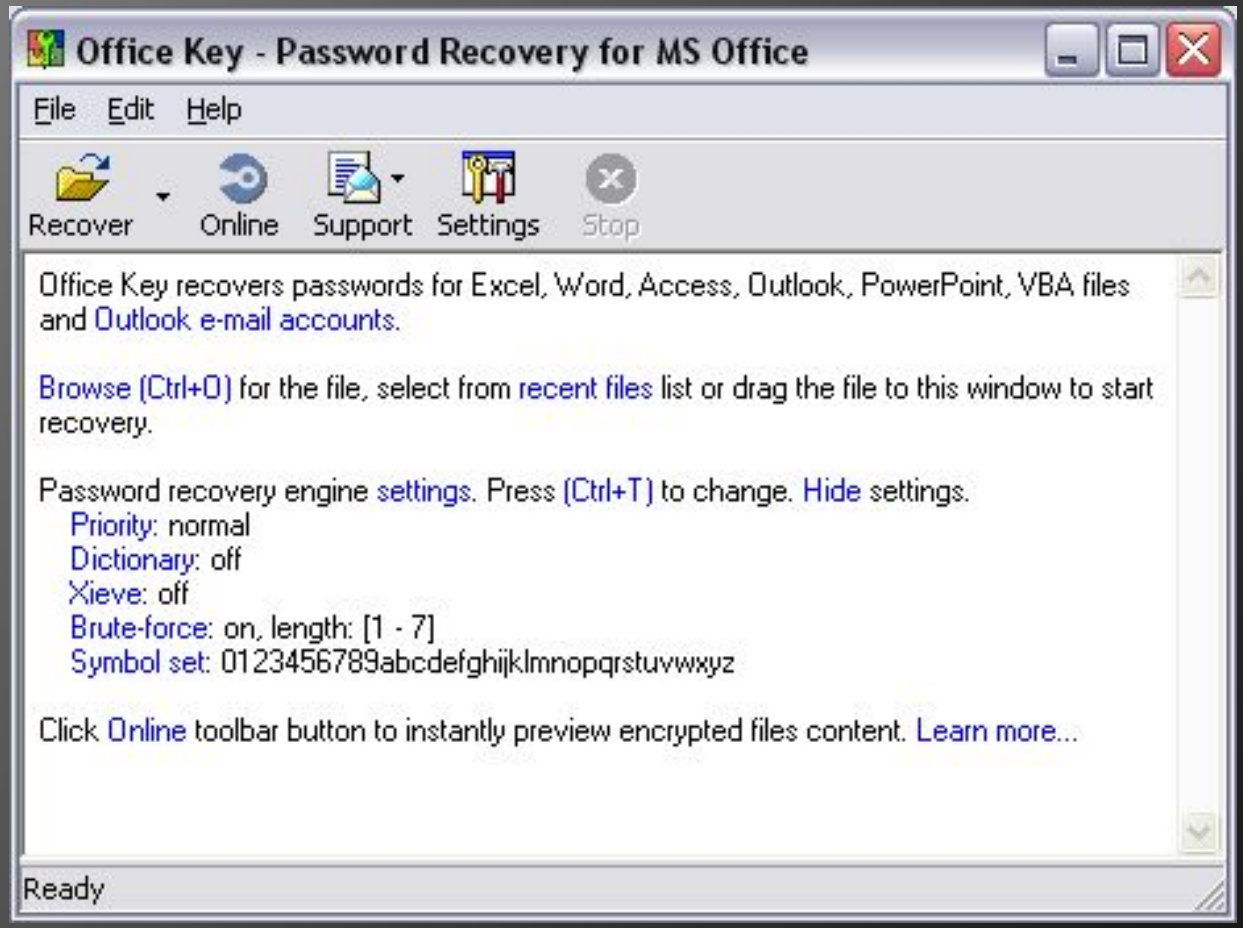
8. Подсказки к паролям не должны использоваться
9. Пароль не должен передаваться по недостаточно надежно защищенным каналам связи
10. Пароль должен немедленно заменяться, если есть подозрения, что он мог быть раскрыт

Взлом парольной защиты

- Узнавание пароля
- Угадывание пароля
- Словарная атака
- Метод прямого перебора
- Использование программных закладок
- Удаленный доступ к компьютеру
- Непосредственный доступ к компьютеру
- Перехват паролей тех. средствами

Подбор пароля

Passware Kit (Passware, www.LostPassword.com)



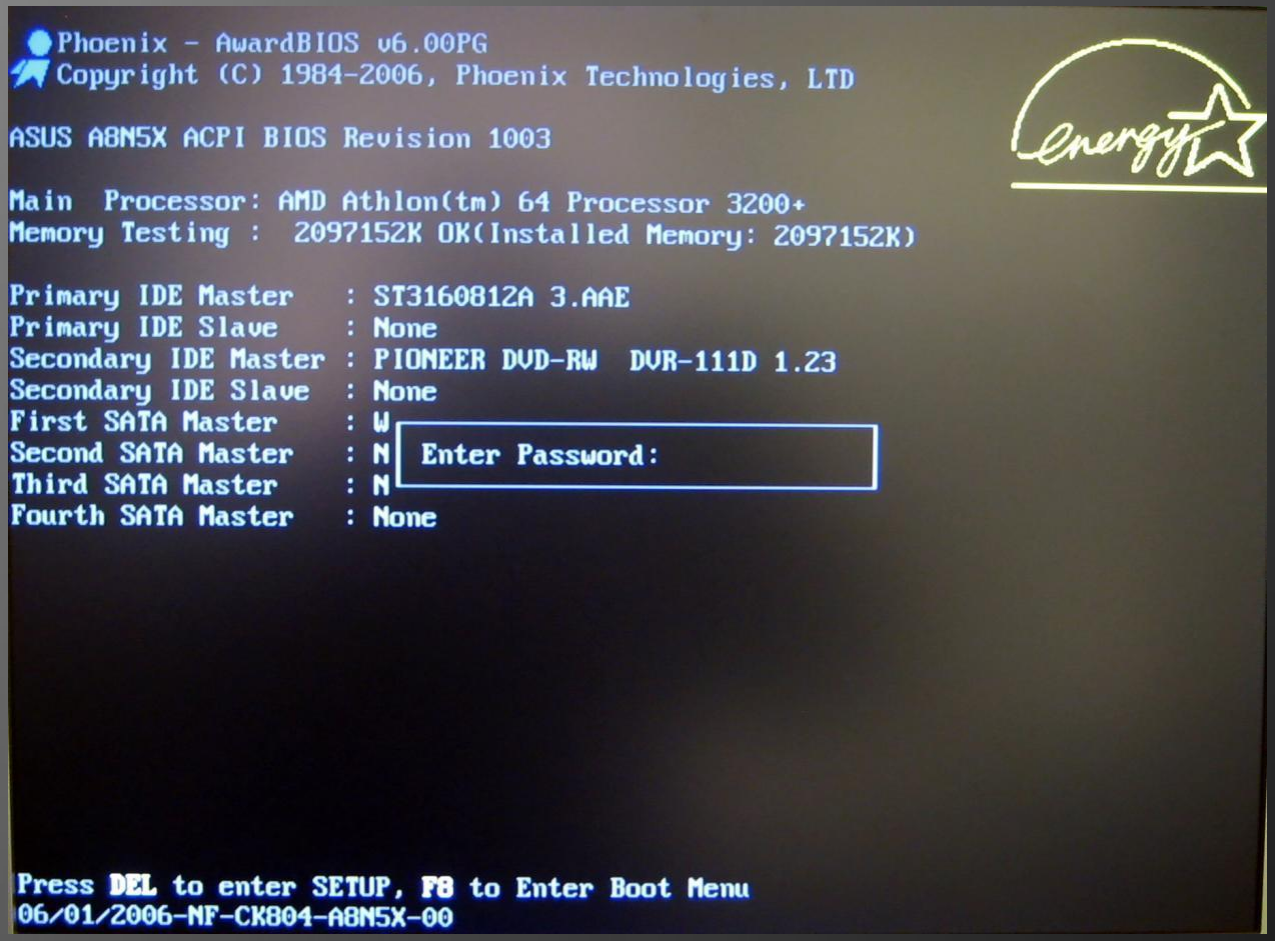
Программные методы защиты информации

1. Защита на уровне доступа к ресурсам
2. Защита на уровне данных
3. Защита информации нестандартными методами и средствами

Защита на уровне доступа к ресурсам

1. защита доступа на уровне BIOS
2. доступ к операционной системе
3. защита доступа к разделам носителя данных (НЖД)

ЗАЩИТА НА УРОВНЕ BIOS



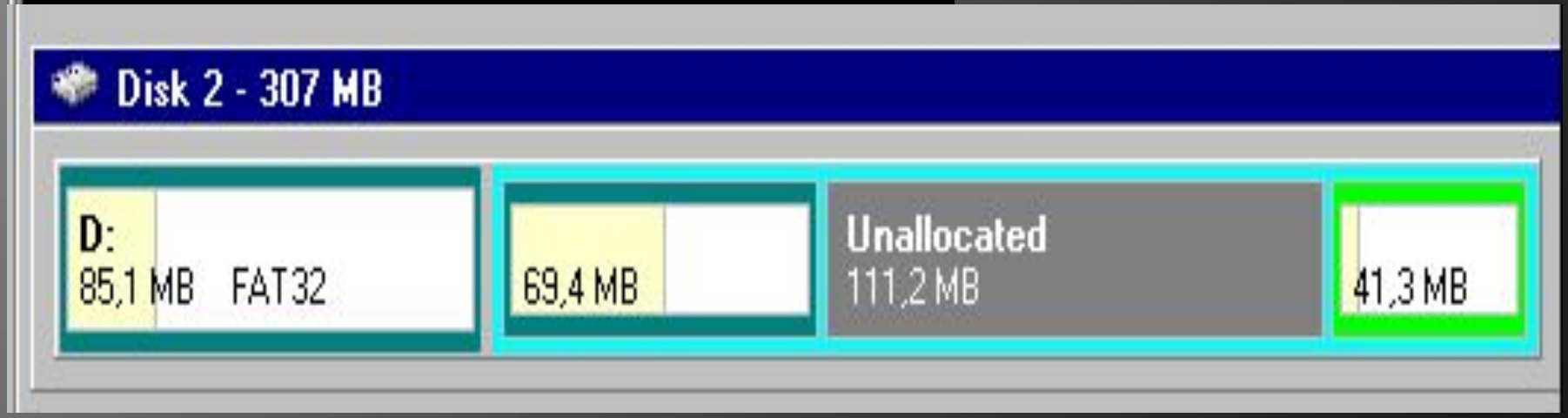
Защита учетной записи пользователя (доступ к ОС)

Защита доступа к разделам НЖД

- защита доступа паролем
- создание скрытых разделов
- удаление раздела
- шифрование раздела

Защита доступа к разделам НЖД

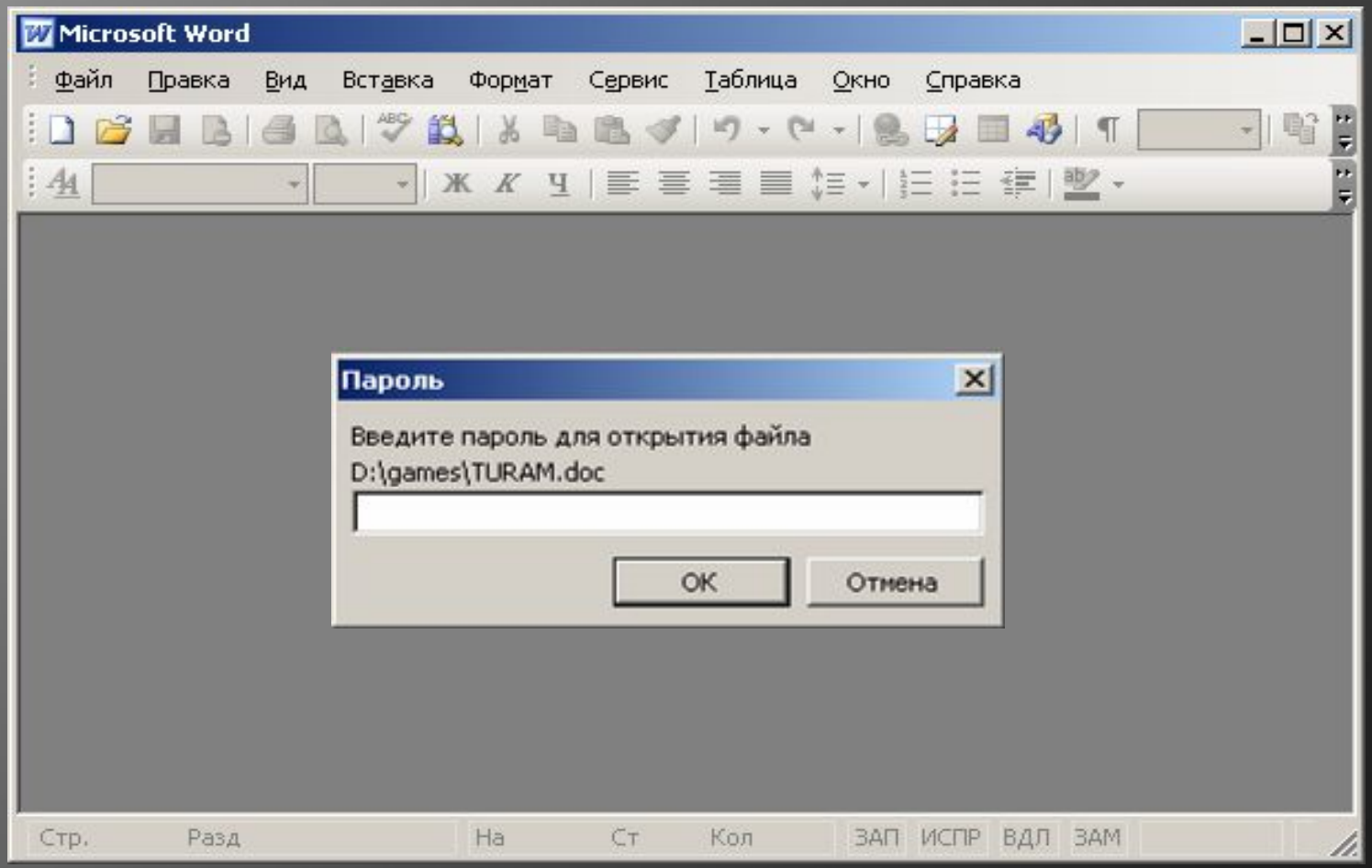
```
Non-System disk or disk error

Replace and strike any key when ready
_
```



Защита на уровне доступа к данным

- защита файлов пользовательским паролем
- шифрование данных
- сокрытие информации

Защита файлов пользовательским паролем



КРИПТОГРАФИЯ

Шифрование информации

Криптография - преобразование составных частей информации с помощью специальных алгоритмов

Методы криптографии:

Перестановка ***Замена***

Гаммирование ***Комбинированные методы***

Алгоритмы шифрования:

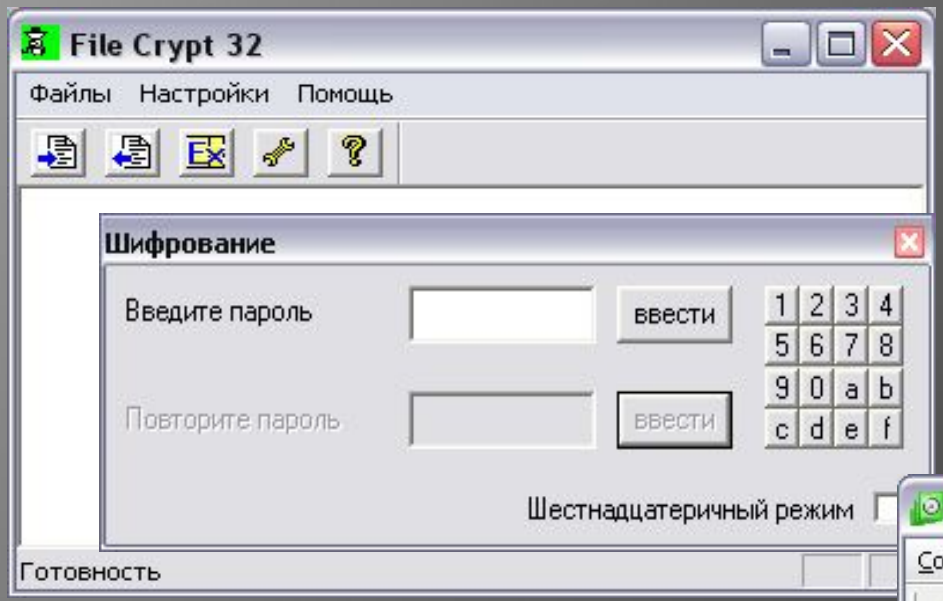
С закрытым ключом С открытым ключом

Пример перестановки

1	2	3	4	5
П	Р	И	М	Е
Р	_	П	Е	Р
Е	С	Т	А	Н
О	В	К	И	_

ПРЕОР_СВИПТКМЕАИЕРН

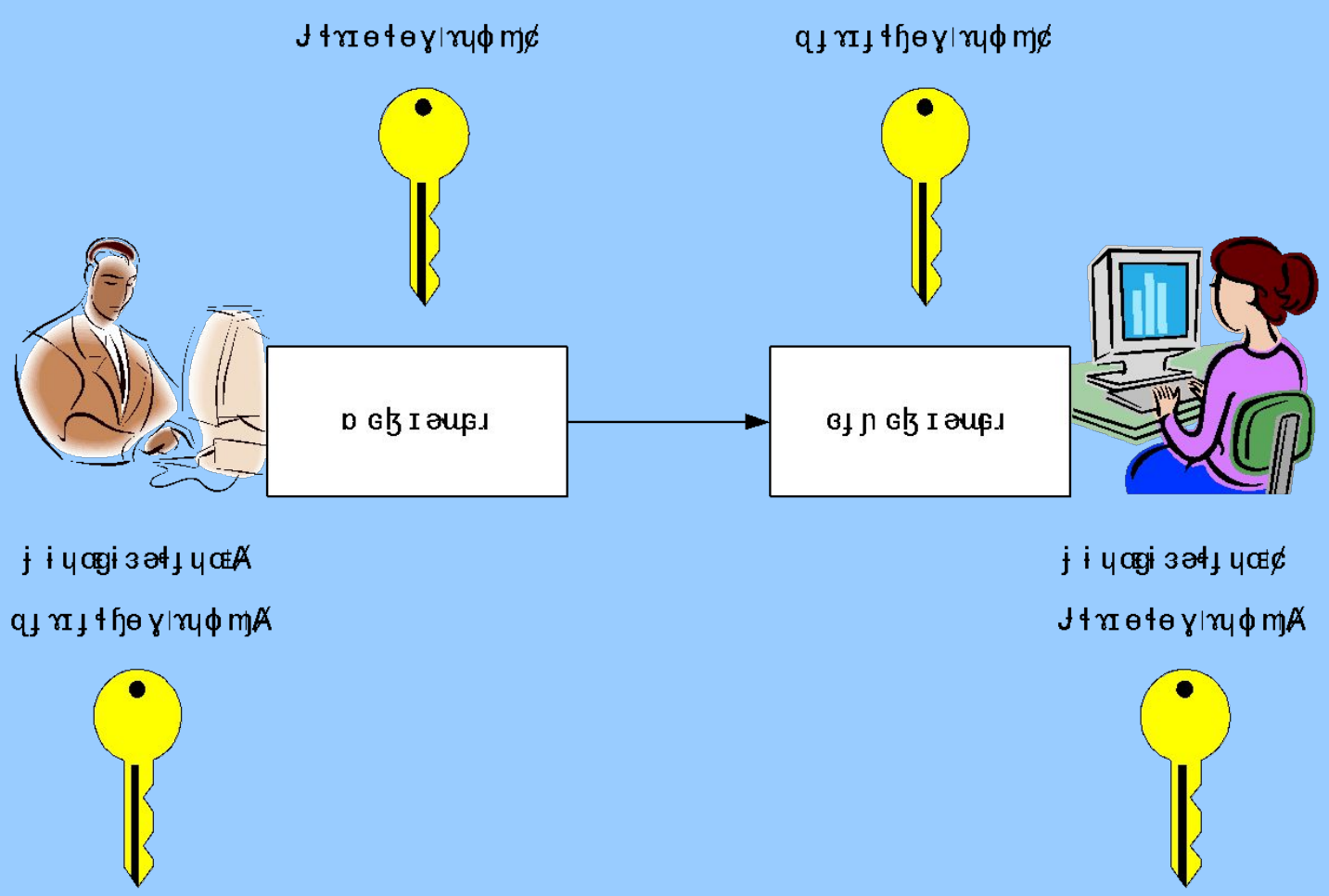
Шифрование с закрытым ключом



защита отдельных файлов (*FileCrypt32*)

криптодиски (*BestCrypt*)

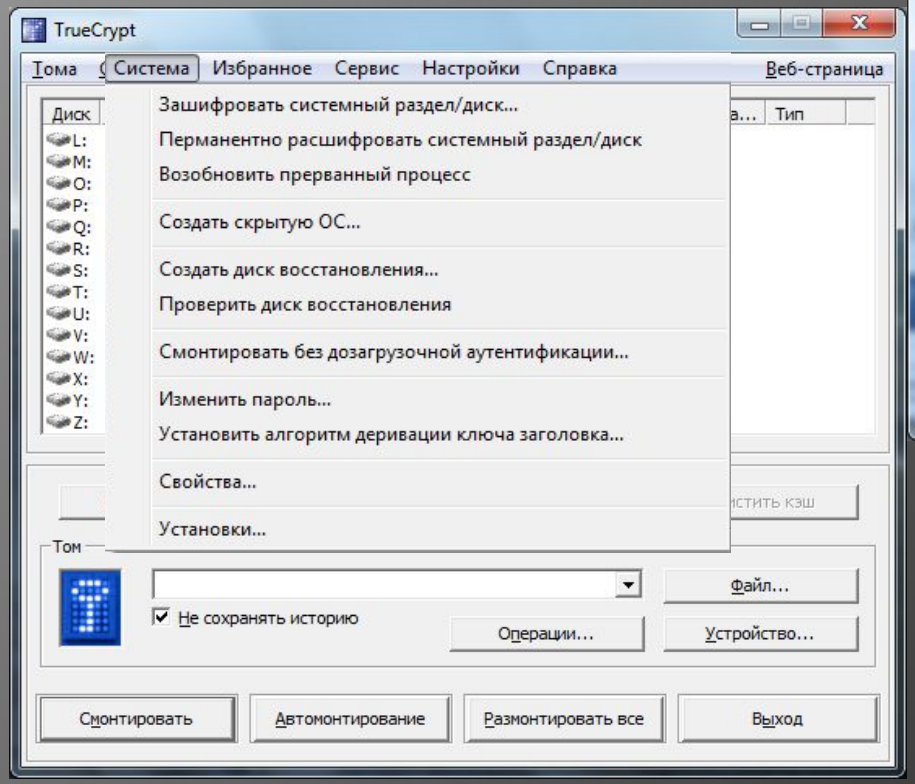
Шифрование методом с открытым ключом

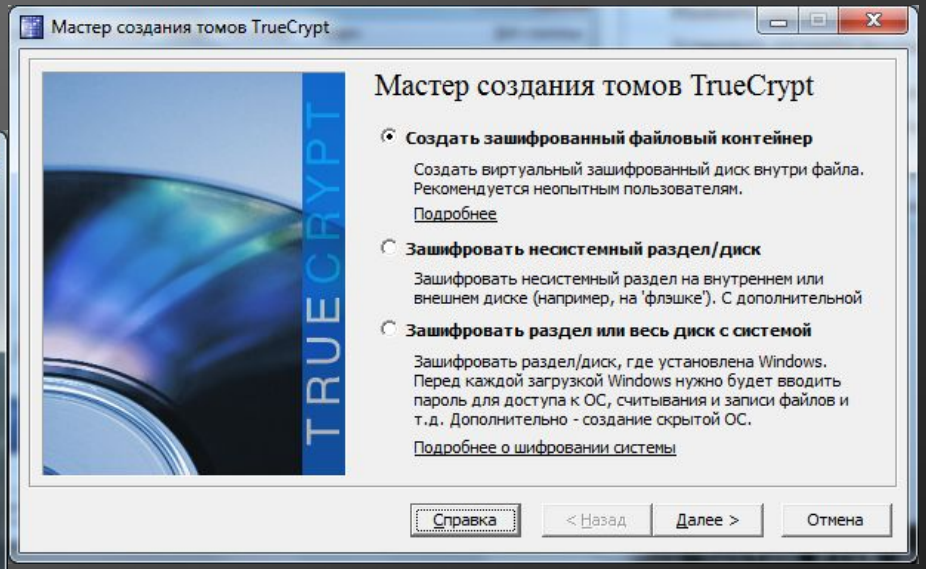


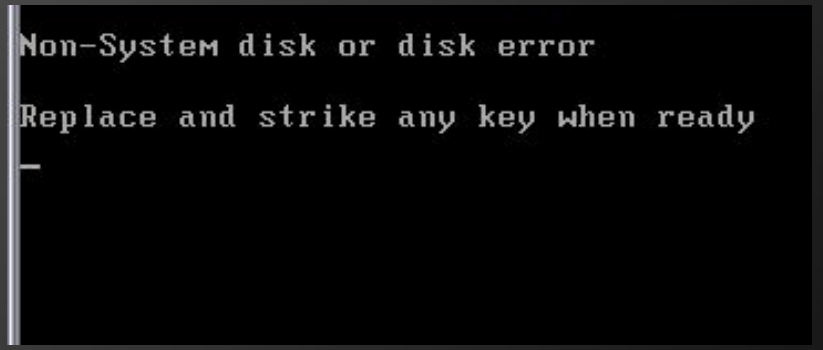
Технологии шифрования

1. Пофайловое шифрование
2. Шифрование каталогов
3. Шифрование виртуальных дисков
4. Шифрование всего диска

Шифрование данных







Стеганография

метод скрытой коммуникации между двумя сторонами, существование которой неизвестно третьей стороне (тайнопись)

Примеры:

надпись на голове посланника

(сбрили волосы, написали, отрастили волосы)

надпись «симпатическими» чернилами

(Ленин писал молоком между строк в книге)

программы стеганографии

(скрывают документ в графическом файле)

BIOS.TXT - Блокнот

Файл Правка Формат Вид Справка

Что такое BIOS?

BIOS (basic input/output system) - базовая система ввода-вывода - это встроенное в
Обычно BIOS размещается в микросхеме ПЗУ (ROM), размещенной на материнской плате к
В настоящее время, почти все материнские платы комплектуются Flash BIOS, BIOSом, к
BIOS PC стандартизирован, поэтому, в принципе менять его, также как, например, опе
BIOS, который поддерживает технологию Plug-and-Play, называется PnP BIOS. При испо

Как определить, что установленный на материнской плате BIOS, прошит во Flash ROM?

Определить тип микросхемы ПЗУ, установленнолй на материнской плате, несложно. Для
•28Fxxx - 12V Flash память •29Cxxx - 5V Flash память •29LVxxx - 3V Flash memory (р

Любые другие микросхемы, не имеющие окошка с маркировкой, не начинающейся с цифр 2

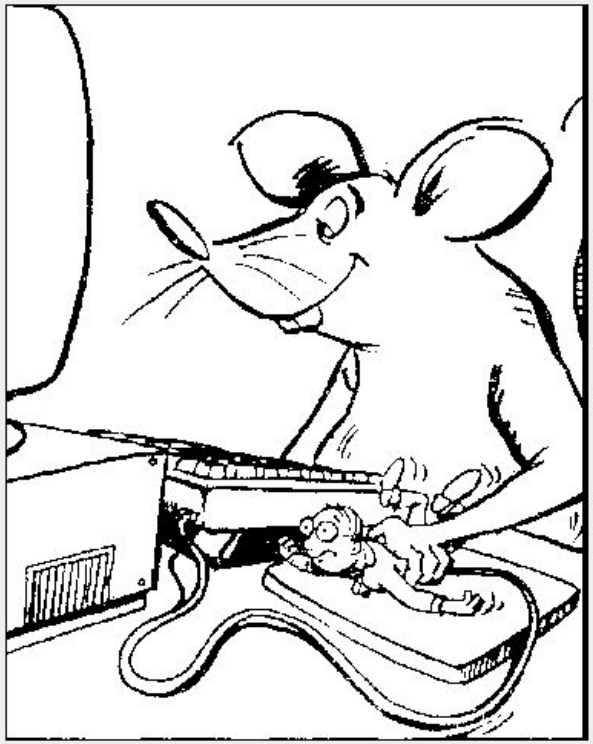
Зачем необходима перепрошивка новых версий BIOS?

Существует несколько причин, по которым это приходится делать. Основная из них - W
В настоящее время используются жесткие диски объемом более 528Мбайт. Для работы та
Полная поддержка Plug-and-Play со стороны Windows 95 возможна только в случае прим
Кроме вышеуказанного, в новых версиях BIOS исправляются мелкие ошибки и недоработк

Где можно скачать новые версии BIOS?

Во-первых новые версии BIOS доступны на сайтах их производителей. Во-вторых обычно

RAT.BMP - Программа просмотра изображений и факсов



Методы стеганографии

- Модификация изображения в пространственной области
- Модификация изображения с преобразованием
- Фрактальное кодирование
- Специальные алгоритмы

3.ВРЕДОНОСНЫЕ ПРОГРАММЫ

Изменения в УК РФ (глава 28)

внесены законом №420-ФЗ от 07.12.2011 года

Компьютерная информация - сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ:

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации

Классификация вредоносных программ по вредоносной нагрузке

1. Помехи в работе заражённого компьютера
2. Инсталляция другого вредоносного ПО
3. Кража, мошенничество, вымогательство и шпионаж
4. Иная незаконная деятельность
5. Потенциально нежелательные программы

Классификация вредоносных программ по методу распространения

1. Компьютерный вирус
2. Сетевой червь
3. Троянские программы
4. Эксплойт
5. Логическая бомба

Компьютерный вирус

Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по локальным ресурсам компьютера

Сетевой червь

Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению в компьютерных сетях через сетевые ресурсы.

Троянские программы

Вредоносные программы, созданные для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей.

Троянские программы

1. Trojan-PSW
2. Backdoor
3. Rootkit
4. Trojan-Downloader
5. Trojan-SMS

Эксплойт

компьютерная программа (или фрагмент программного кода или последовательность команд), использующая уязвимости в программном обеспечении и применяемая для проведения атаки на вычислительную систему.

Цель атаки - захват контроля над системой, нарушение её функционирования (DoS-атака).

Потенциально нежелательные программы (PUP's)

1. Adware
2. Pornware
3. Riskware
4. Spyware
5. Программы удалённого администрирования

Фальшивые антивирусы

Борьба с вредоносными программами

Признаки заражения

1. Увеличение интернет-трафика.
2. Появление в списке автозагрузки неизвестных процессов и программ.
3. Самопроизвольный запуск неизвестных приложений.
4. Появление на экране дополнительных окон, сообщений и т.д.

Признаки заражения

1. Блокирование работы операционной системы, прикладных программ, их нестабильная работа.
2. Самопроизвольное завершение работы программ, перезагрузка компьютера.
3. Уничтожение, блокирование, повреждение данных.

Действия при заражении

1. Проверка актуальности антивирусной базы, при необходимости - обновление.
2. Сканирование машинного носителя на наличие вредоносных программ.

Действия при заражении

Если сканирование невозможно или не дало результатов:

1. **Загрузка компьютера с внешнего носителя.**
2. **Сканирование встроенного машинного носителя.**
3. **Создание резервной копии пользовательских данных.**

Профилактика и защита

1. Регулярное обновление антивирусных баз.
2. Регулярное обновление программного обеспечения.
3. Регулярное сканирование машинного носителя на наличие вредоносных программ.
4. Обязательное сканирование съемных накопителей.
5. Регулярное резервирование пользовательских данных.
6. Обслуживание и оптимизация системы.