



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)

- ▶ 1-2-3 Key.Ink
- ▶ Acrobat Key.Ink
- ▶ Act Key.Ink
- ▶ Asterisk Key.Ink
- ▶ Backup Key.Ink
- ▶ BestCrypt Key.Ink
- ▶ EFS Key.Ink
- ▶ FileMaker Key.Ink
- ▶ Internet Explorer Key.Ink
- ▶ Lotus Notes Key.Ink
- ▶ Lotus Word Pro Key.Ink
- ▶ Mail Key.Ink
- ▶ Messenger Key.Ink
- ▶ Money Key.Ink
- ▶ MYOB Key.Ink
- ▶ Network Connections Key.Ink
- ▶ Office Key.Ink
- ▶ OneNote Key.Ink
- ▶ Organizer Key.Ink
- ▶ Outlook Express Key.Ink
- ▶ Paradox Key.Ink
- ▶ Passware Kit Enterprise Help.Ink
- ▶ Peachtree Key.Ink
- ▶ Project Key.Ink
- ▶ Quattro Pro Key.Ink
- ▶ QuickBooks Key.Ink
- ▶ Quicken Key.Ink
- ▶ RAR Key.Ink
- ▶ Schedule Key.Ink
- ▶ SQL Key.Ink
- ▶ Windows Key.Ink
- ▶ WordPerfect Key.Ink
- ▶ Zip Key.Ink

The screenshot shows a window titled "Office Key - Password Recovery for MS Office". The window has a menu bar with "File", "Edit", and "Help". Below the menu bar is a toolbar with five buttons: "Recover" (with a folder icon), "Online" (with a CD icon), "Support" (with a document icon), "Settings" (with a key icon), and "Stop" (with a red X icon). The main content area contains the following text:

Office Key recovers passwords for Excel, Word, Access, Outlook, PowerPoint, VBA files and Outlook e-mail accounts.

Browse (Ctrl+O) for the file, select from recent files list or drag the file to this window to start recovery.

Password recovery engine settings. Press (Ctrl+T) to change. Hide settings.

Priority: normal
Dictionary: off
Xieve: off
Brute-force: on, length: [1 - 7]
Symbol set: 0123456789abcdefghijklmnopqrstuvwxyz

Click Online toolbar button to instantly preview encrypted files content. [Learn more...](#)

Ready



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

Phoenix - AwardBIOS v6.00PG
Copyright (C) 1984-2006, Phoenix Technologies, LTD

ASUS ABN5X ACPI BIOS Revision 1003

Main Processor: AMD Athlon(tm) 64 Processor 3200+
Memory Testing : 2097152K OK(Installed Memory: 2097152K)

Primary IDE Master : ST3160812A 3.AAE
Primary IDE Slave : None
Secondary IDE Master : PIONEER DVD-RW DVR-111D 1.23
Secondary IDE Slave : None
First SATA Master : W
Second SATA Master : N
Third SATA Master : N
Fourth SATA Master : None



Enter Password:

Press DEL to enter SETUP, F8 to Enter Boot Menu
06/01/2006-NF-CK804-ABN5X-00



Защита учетной записи пользователя (доступ к ОС)

Microsoft
Windows XP

Чтобы начать работу, щелкните имя пользователя

 expert
Введите пароль
 EN 

 user

 Выключить компьютер

После входа в систему можно добавлять или изменять учетные записи.
Для этого в панели управления нужно выбрать "Учетные записи пользователей".



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
_
```

 Disk 2 - 307 MB

D:
85,1 MB FAT32

69,4 MB

Unallocated
111,2 MB

41,3 MB

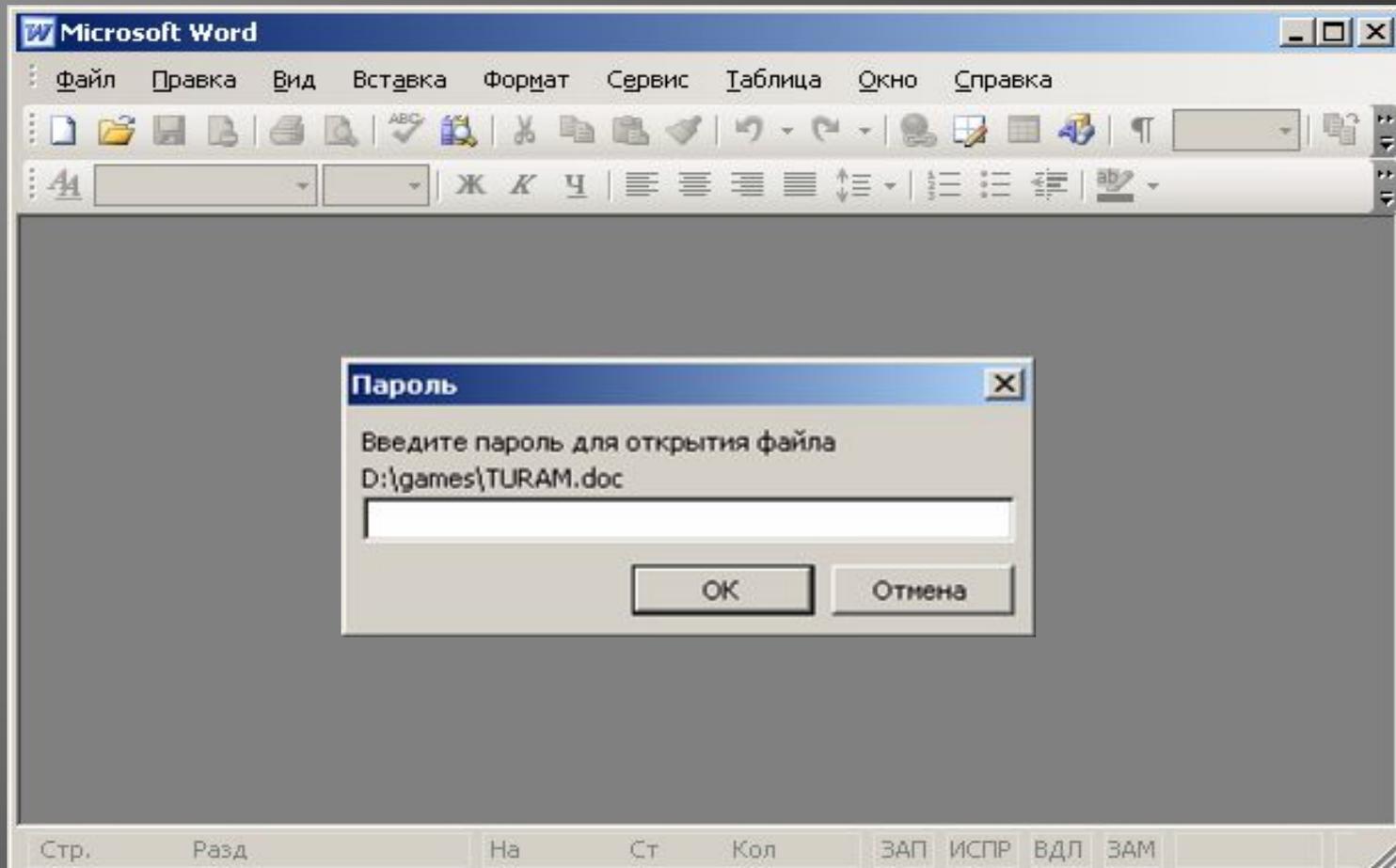


Защита на уровне доступа к данным

- ▣ защита файлов пользовательским паролем
- ▣ шифрование данных
- ▣ сокрытие информации



Защита файлов пользовательским паролем





Нижегородская академия МВД России
Кафедра математики, информатики и информационных технологий

КРИПТОГРАФИЯ



Шифрование информации

Криптография - преобразование составных частей информации с помощью специальных алгоритмов

Методы криптографии:

Перестановка Замена

Гаммирование Комбинированные методы

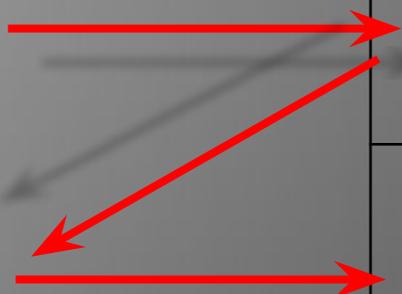
Алгоритмы шифрования:

С закрытым ключом С открытым ключом



Пример перестановки

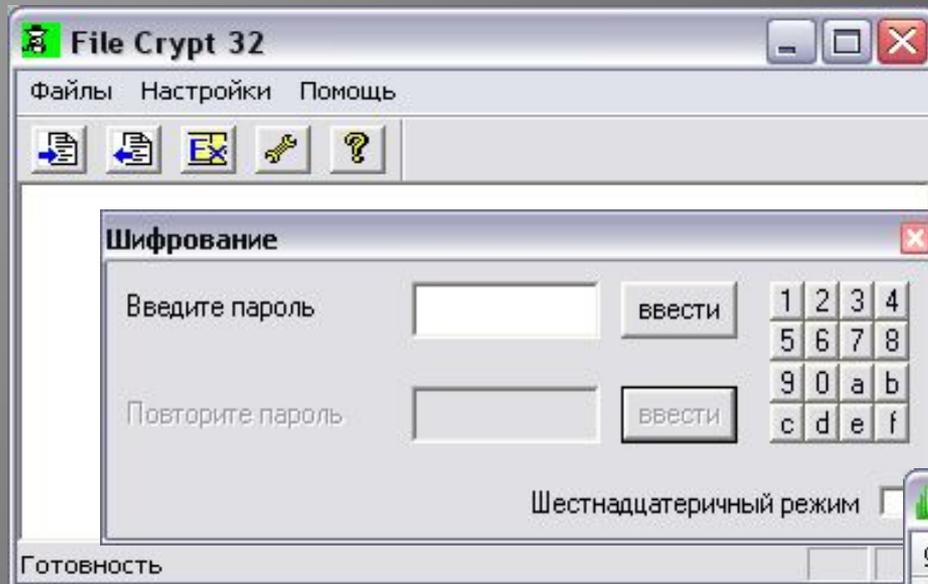
	1	2	3	4	5
П	П	Р	И	М	Е
Р	Р	_	П	Е	Р
Е	Е	С	Т	А	Н
О	О	В	К	И	_



ПРЕОР_СВИПТКМЕАИЕРН



Шифрование с закрытым ключом



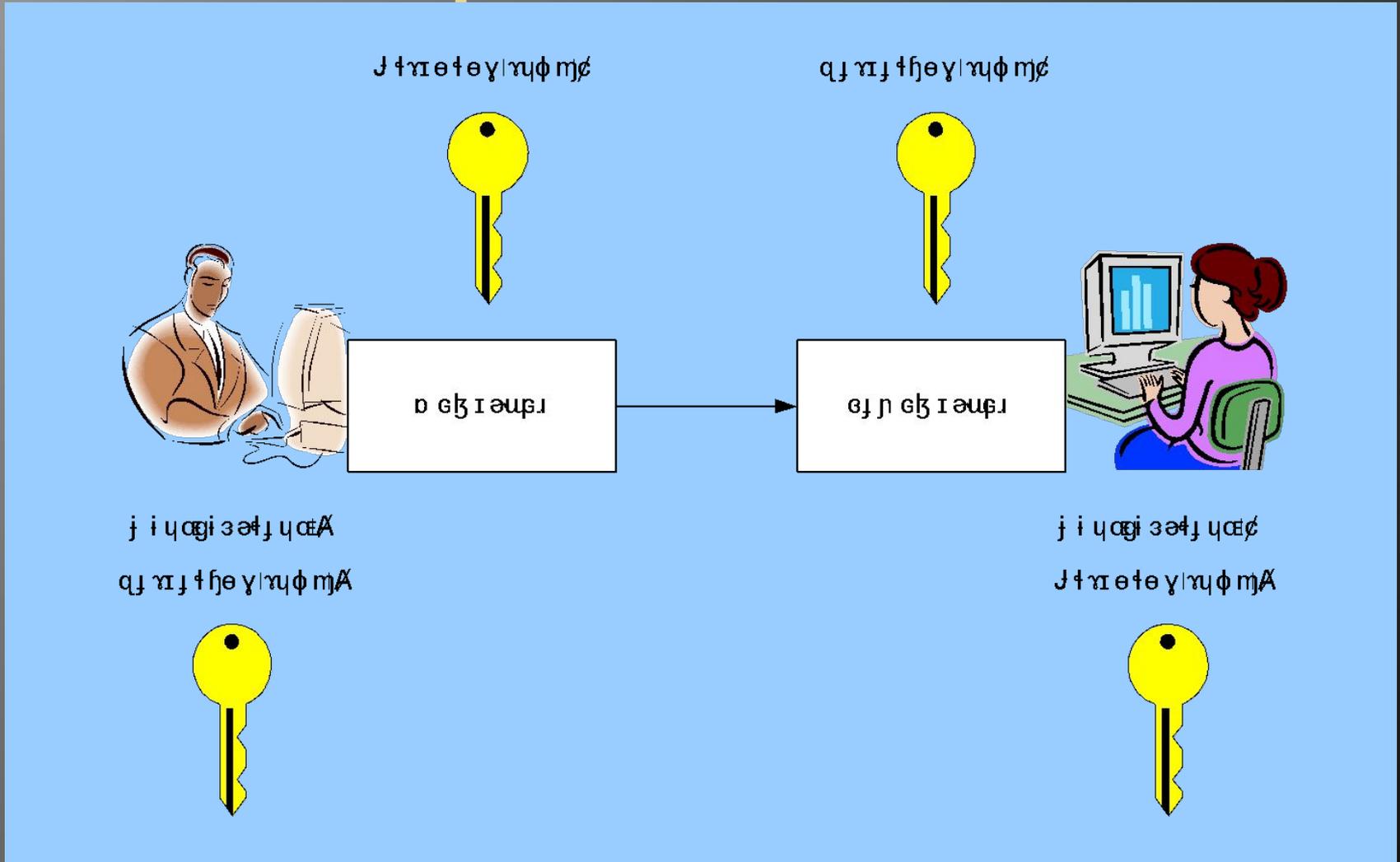
защита отдельных
файлов (*FileCrypt32*)

криптодиски
(*BestCrypt*)





Шифрование методом с ОТКРЫТЫМ КЛЮЧОМ



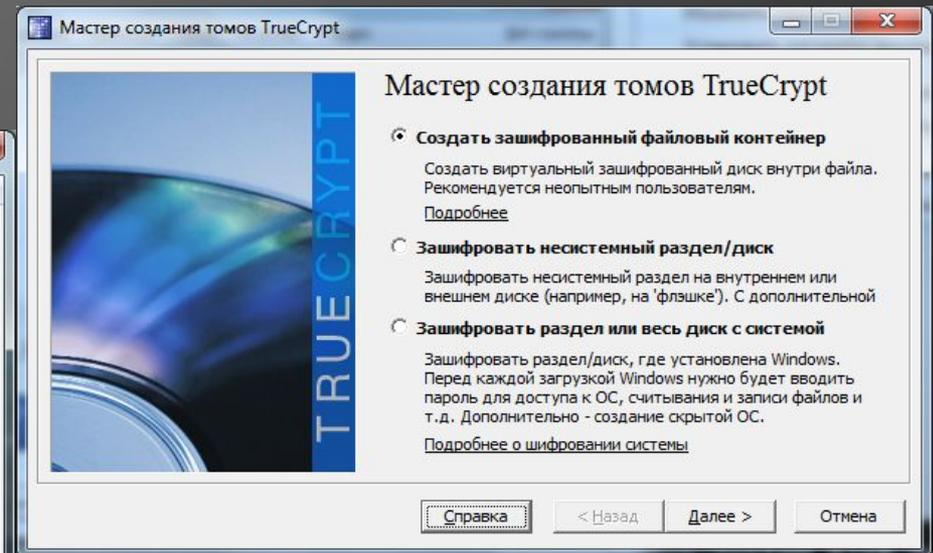
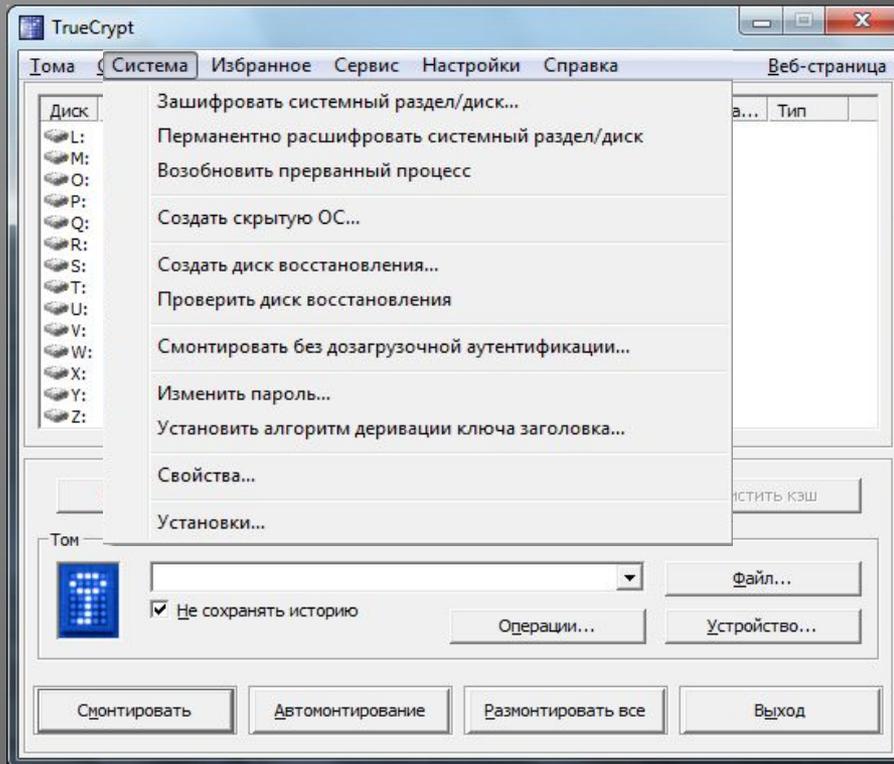


Технологии шифрования

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



Шифрование данных



```
Non-System disk or disk error
Replace and strike any key when ready
```



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)



Нижегородская академия МВД России

Кафедра математики, информатики и информационных технологий

BIOS.TXT - Блокнот

Файл Правка Формат Вид Справка

Что такое BIOS?

BIOS (basic input/output system) - базовая система ввода-вывода - это встроенное в микросхему ПЗУ (ROM), размещенной на материнской плате компьютера. В настоящее время, почти все материнские платы комплектуются Flash BIOS, BIOSом, который поддерживает технологию Plug-and-Play, называется PnP BIOS. При установке BIOS, который поддерживает технологию Plug-and-Play, называется PnP BIOS. При установке BIOS, который поддерживает технологию Plug-and-Play, называется PnP BIOS.

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

Определить тип микросхемы ПЗУ, установленной на материнской плате, несложно. Для определения типа микросхемы ПЗУ, установленной на материнской плате, несложно. Для определения типа микросхемы ПЗУ, установленной на материнской плате, несложно.

- 28Fxxx - 12V Flash память
- 29Cxxx - 5V Flash память
- 29LVxxx - 3V Flash memory

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 - 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 применения вышеуказанного, в новых версиях BIOS исправляются мелкие ошибки и недоработки.

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



Navigation icons: back, forward, home, search, print, etc.



Методы стеганографии

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



Нижегородская академия МВД России
Кафедра математики, информатики и информационных технологий

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. Установка 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**



Нижегородская академия МВД России

Кафедра математики, информатики и информационных технологий

Фальшивые антивирусы

Complete Protection Home **DOWNLOAD** Members Support

Antivirus & Security

Complete Antivirus Protection Solution
Get instant access to the world's most trusted antivirus software solutions. Protect your emails, instant messages and other files by automatically removing viruses. New built-in features also detect threats such as spyware and adware.

• A software you can truly depend on!

FREE OFFER! Receive the full protection Security Bundle for your system against all viruses, worms, spy and malware.

Download & Protect
Protect Your PC like no other software can!

Anti Virus
Anti Spyware
Anti Spam
Firewall
Safe Downloads
Instant Messaging
Safe Searches

Sign Your PC is Infected
• Opening files before viewing
• Pop-up internet web surfing
• Software warnings are frequent
• Constant program errors
• Computer is just plain slow

Full Internet Security
Antivirus, AntiSpam, AntiSpam, Firewall and the all new web protection. Identify and stop Internet threats before they become a problem.

Download Latest Version
Avast! Antivirus & Security is a trust solution for your system. Latest version, viruses, updates and updates all available any time online!

Home Download Members Support Affiliate

Copyright © Avast Software s.r.o. All rights reserved. | [Terms and Privacy](#)

YourSecurePC Is Your PC Infected? **YES NOW!**

Remove viruses instantly with **Antivirus 2010**

Download Antivirus 2010 Now and receive a FREE complimentary Firewall software package to help malware and protect your PC from malware attacks.

Download Now!

Key Technologies

- Proven Email & Instant Message
- Protect Against Adware & Spyware
- Blocking Behavior
- Defend Against Emerging Threats
- Automatic File Protection

Why We Are the Best

- 24/7 Technical Support
- One-Click Updates
- Ultra Fast Downloads
- Guaranteed Lifetime Versions
- Easy and Simple Interface

System Requirements

Microsoft Windows (Vista, XP, Windows 7)
Microsoft Windows (Vista, XP, Windows 7)
Microsoft Windows (Vista, XP, Windows 7)

Why Choose Us?

Antivirus 2010	Avast	Norton	Kaspersky	AVP	BitDefender
Removes Viruses	<input checked="" type="checkbox"/>				
Anti-Spyware	<input checked="" type="checkbox"/>				
Protect Malware	<input checked="" type="checkbox"/>				
Safe Downloading	<input checked="" type="checkbox"/>				
Safe Browsing	<input checked="" type="checkbox"/>				
Clean Warnings	<input checked="" type="checkbox"/>				
Removes Cookies	<input checked="" type="checkbox"/>				
24/7 Support	<input checked="" type="checkbox"/>				

Sign Your PC is Infected

- Opening files before viewing
- Pop-up internet web surfing
- Software warnings are frequent
- Constant program errors
- Computer is just plain slow

Scan Your PC Now!

Home Download Members Support Affiliate

Copyright © YourSecurePC.com. All rights reserved.

SECURITY 20 Years of Total Protection

Home Download Members Support

Learn how to protect your PC with our **AVAST! SECURITY SOFTWARE**

The Number One Anti-Virus Online!

The Most Popular Anti-Virus Software!

Download Now!

Complete Security

Personal Use	Small Business	Corporate Clients
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Top Features

- Faster Search Time
- Search for Internet content
- Supports all Windows platforms
- New and improved interface
- Search single & multiple PC's
- Improved security features

Also Included in Bundle

- Registry Repair™
- Anti-Virus Advance™
- Spyware Remover™

Testimonials

Download Now!

Home Download Members Support Affiliate

Copyright © Avast Software s.r.o. All rights reserved. | [Terms and Privacy](#)



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.**