

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Основные понятия и положения. Виды угроз в информационной сфере, внутренние и внешние источники угроз. Международные стандарты информационной безопасности, стандарты РФ.
- Виды вирусов. Антивирусные программы.
- Методы защиты персонального компьютера.

-
- «Информационные войны никто не объявлял, но они идут постоянно»
 - Второй этап эры информатизации (информационное или постиндустриальное общество)

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

- **Информационная безопасность — это состояние защищённости информационной среды общества посредством различных средств и методов.**
- Информационная безопасность организации- состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие.

СТАНДАРТИЗИРОВАННЫЕ ОПРЕДЕЛЕНИЯ

- Безопасность информации (данных) — состояние защищенности информации (данных), при котором обеспечены её (их) **конфиденциальность, точность, полнота, доступность и целостность.**
- Информационная безопасность — защита конфиденциальности, целостности и доступности информации.
- Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям.
- Целостность: обеспечение достоверности и полноты информации и методов её обработки.
- Доступность: обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

- В качестве стандартной модели безопасности часто приводят модель из трёх категорий:
 - конфиденциальность — состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;
 - целостность — избежание несанкционированной модификации информации;
 - доступность — избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ

- Системный подход к описанию информационной безопасности предлагает выделить следующие составляющие информационной безопасности:
 - законодательная, нормативно-правовая и научная база.
 - структура и задачи органов (подразделений), обеспечивающих безопасность ИТ.
 - организационно-технические и режимные меры и методы (Политика информационной безопасности).
 - программно-технические способы и средства обеспечения информационной безопасности.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

```
graph TD; A[ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ] --- B[Организационное обеспечение (менеджмент)]; A --- C[Аппаратное обеспечение]; A --- D[Программное обеспечение]; A --- E[Криптография и математика];
```

**Организационное
обеспечение
(менеджмент)**

Аппаратное
обеспечение

Программное
обеспечение

Криптография и
математика

ОРГАНЫ (ПОДРАЗДЕЛЕНИЯ), ОБЕСПЕЧИВАЮЩИЕ

ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

- В зависимости от приложения деятельности в области защиты информации (в рамках государственных органов власти или коммерческих организаций), сама деятельность организуется специальными государственными органами (подразделениями), либо отделами (службами) предприятия.
- Государственные органы РФ, контролирующие деятельность в области защиты информации:
 - Комитет Государственной думы по безопасности;
 - Совет безопасности России;
 - Федеральная служба по техническому и экспортному контролю (ФСТЭК России), ранее - Гостехкомиссия;
 - Федеральная служба безопасности Российской Федерации (ФСБ России);
 - Министерство внутренних дел Российской Федерации (МВД России);
 - **Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).**

ВИДЫ УГРОЗ В ИНФОРМАЦИОННОЙ СФЕРЕ (ИЗ ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ)

- Угрозы конституционным правам и свободам человека;
- Угрозы развитию отечественной индустрии информации;
- Угрозы информационному обеспечению государственной политики;
- Угрозы безопасности информационных и телекоммуникационных средств.

УГРОЗЫ ДАННЫХ В ЭИС

- Под **угрозой** ИС будем понимать потенциально возможное событие, действие или процесс, которое посредством воздействия на компоненты информационной системы (ИС) может привести к нанесению ущерба как техническим средствам так и информационно-программному обеспечению ИС.
- Обычно различают угрозы **случайного** и **преднамеренного** характера.
- К **случайным** относятся угрозы потерь данных и нарушений работоспособности ИС, возникающие вследствие:
 - ошибок и сбоев в работе программных и технических средств ИС;
 - стихийных бедствий;
 - ошибок в работе пользователей и т.п

УГРОЗЫ ЭИС

- Угрозы **преднамеренного характера** исходят со стороны нарушителей (злоумышленников), т. е. лиц, которые сознательно стремятся получить несанкционированный доступ к ресурсам ИС или нарушить ее работоспособность.
- К такого рода **угрозам** можно отнести:
 - внесение изменений в финансовые документы;
 - незаконное копирование компонентов информационного, программного обеспечения;
 - нарушение работоспособности ИС с целью нанесения ущерба компании.

БЕЗОПАСНОСТЬ ЭИС

- Под **уязвимостью** ИС будем понимать любую характеристику или свойство системы, использование которой нарушителем может привести к реализации угрозы.
- Под **атакой** будем понимать любое действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей ИС.

□ Министерство обороны США приводит следующую классификацию угроз информационным системам по степени нарастания ущерба:

1. Некомпетентные служащие
2. Хакеры и кракеры
3. Служащие не удовлетворённые своим статусом
4. Нечестные служащие.
5. Инициативный шпионаж.
6. Организованная преступность.
7. Политические диссиденты.
8. Террористические группы.
9. Экономические, политический, военный шпионаж.
10. Tактические удары и стратегические операции противника по разрушению информационного пространства государства в ходе ведения информационной войны.

СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- ISO/IEC 17799:2005 — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.
- ISO/IEC 27000 — Словарь и определения.
- ISO/IEC 27001:2005 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.
- ISO/IEC 27002 — Сейчас: ISO/IEC 17799:2005. Дата выхода — 2007 год.

СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- ГОСТ Р 50922-96 — Защита информации. Основные термины и определения.
- Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.
- ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
- ГОСТ Р 51275-99 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
- ГОСТ Р ИСО/МЭК 15408-1-2002 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
- ГОСТ Р ИСО/МЭК 15408-2-2002 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

- Конкретные требования к защите информации обусловлены спецификой каждой ИС.
- Информация должна защищаться во всех структурных элементах ИС.

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

- Препятствие;
- Управление;
- Маскировка;
- Принуждение;
- Нападение;
- Побуждение.

-
- ▣ **Препятствие** заключается в создании на пути возникновения или распространения угрозы барьера. (пример- блокировки)
 - ▣ **Управление** заключается в определении алгоритмов функционирования систем обработки информации, а также процедур и правил, препятствующих возникновению угроз. (пример- административное разграничение прав доступа)

-
- ▣ **Маскировка**- преобразование информации, вследствие которого снижается степень распознавания скрываемой информации. (пример- шифрование информации)
 - ▣ **Принуждение**- метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой ответственности (материальной, уголовной, административной).

-
- ▣ **Побуждение**- способ защиты информации, при котором пользователи и персонал внутренне побуждаются к соблюдению всех правил.
 - ▣ **Нападение**- способ защиты, применяемый в активной фазе информационной войны. Цель- заставить противника сосредоточить усилия на защите, ослабив усилия создания угроз.

БЕЗОПАСНОСТЬ КОМПЬЮТЕРОВ (РАБОЧИХ СТАНЦИЙ)

▣ **Компьютерные угрозы:**

- ▣ Вредоносные программы,
- ▣ Спам,
- ▣ Сетевые атаки (хакеры, кракеры),
- ▣ Внутренние угрозы (инсайдеры).

▣ **Каналы распространения угроз:**

- ▣ Электронная почта
- ▣ Интернет-сайты
- ▣ Социальные сети
- ▣ Сети передачи данных
- ▣ Физический перенос данных

ВИРУСЫ

- **Компьютерный вирус** – это программа, способная создавать свои копии, внедрять их в различные объекты или ресурсы компьютерных систем, сетей и производить определенные действия без ведома пользователя.
- Свое название компьютерный вирус получил за некоторое сходство с биологическим вирусом (например, в зараженной программе самовоспроизводится другая программа – вирус, а инфицированная программа может длительное время работать без ошибок, как в стадии инкубации).
- Программа, внутри которой находится вирус, называется **зараженной программой**.

ОСНОВНЫЕ СИМПТОМЫ

ЗАРАЖЕНИЯ ПК

- Замедление работы некоторых программ.
- Увеличение размеров файлов (особенно выполняемых).
- Появление не существовавших ранее “странных” файлов.
- Уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы).

ОСНОВНЫЕ СИМПТОМЫ ЗАРАЖЕНИЯ ПК

- Внезапно возникающие разнообразные видео и звуковые эффекты.
- Появление сбоев в работе операционной системы (в том числе зависание).
- Запись информации на диски в моменты времени, когда этого не должно происходить.
- Прекращение работы или неправильная работа ранее нормально функционирующих программ.

РАСПРЕДЕЛЕНИЕ НОВЫХ ВИРУСОВ ПО ПЛАТФОРМАМ (2010)

Windows	439922	99,912%
*nix	230	0,052
Mac	20	0,005
Mobile	88	0,020
Прочие	51	0,012

- *nix: FreeBSD, Linux, Perl, PHP, Ruby, Unix
- Mobile: Python, Symbian
- Прочие: BeOS, Boot, Boot-DOS, MS-DOS, Multi, SAP, SQL, SunOS

КЛАССИФИКАЦИЯ ВИРУСОВ:



Рис. 1. Классификация вредоносных программ (источник: «Лаборатория Касперского»)

-
- Компьютерные вирусы – программы, которые создают кракеры специально для нанесения ущерба пользователям ПК.
 - ***Их создание и распространение является преступлением.***

РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО (УК РФ)

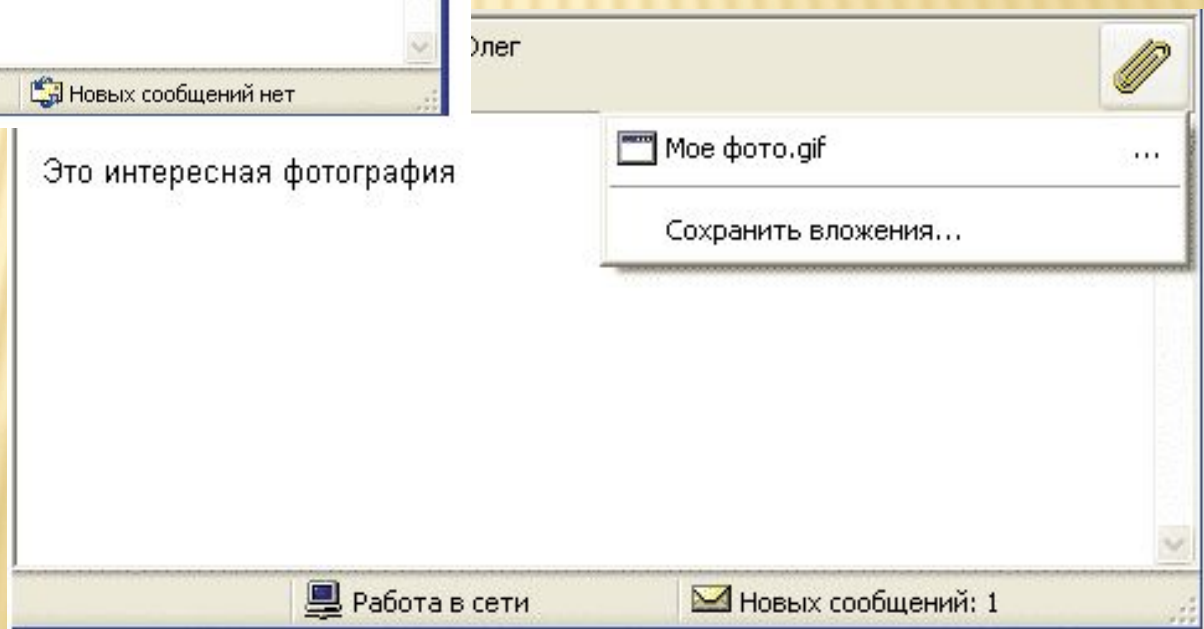
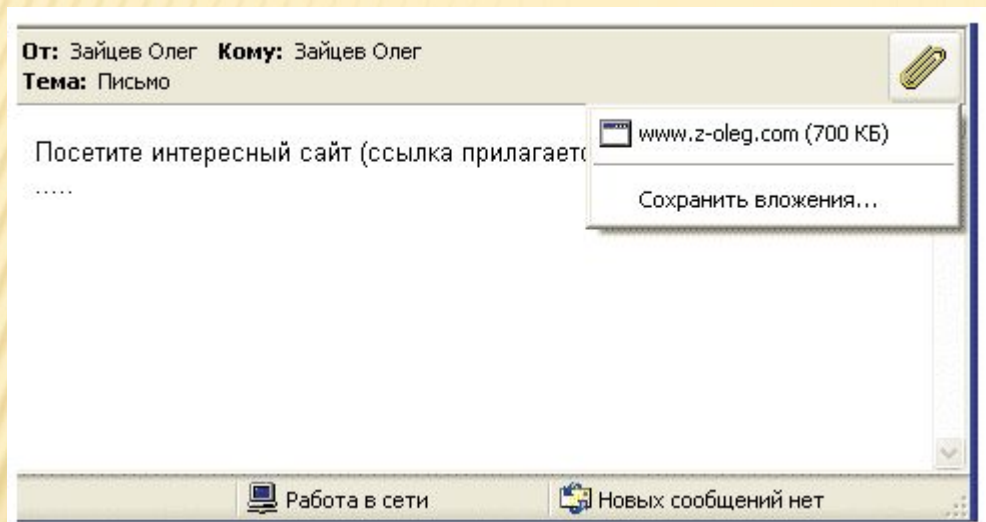
- Статья 272. Неправомерный доступ к компьютерной информации.
- Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.
- Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

-
- Первая локальная эпидемия произошла в 1986г (вирус «Brain»).
 - Всемирная эпидемия заражения этим почтовым вирусом началась 5 мая 2000г, когда компьютеры по сети Интернет получили сообщения «Я тебя люблю» с вложенным файлом, который и содержал вирус.

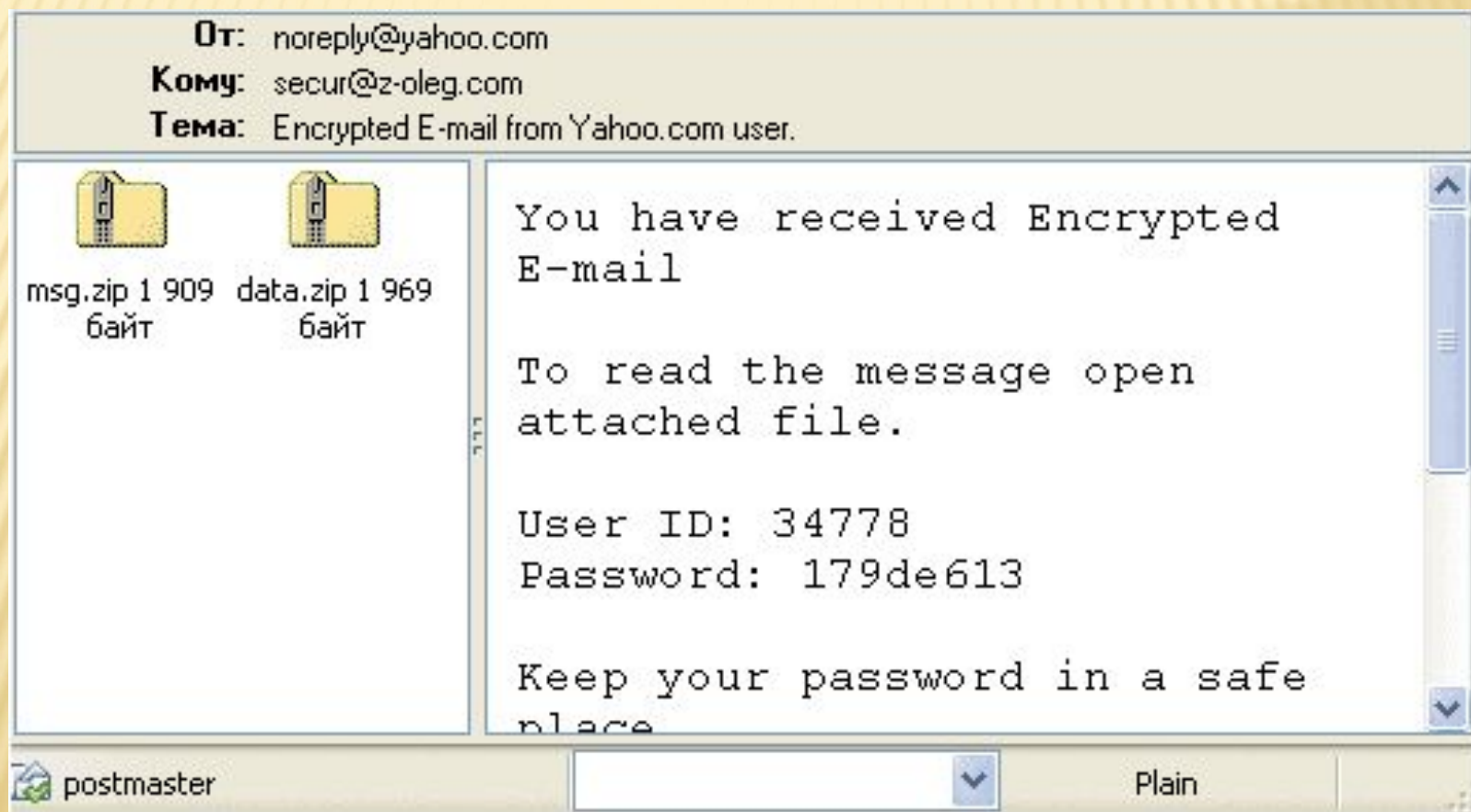
-
- Отличительными особенностями компьютерных вирусов являются:
 - 1) маленький объем файла;
 - 2) самостоятельный запуск;
 - 3) многократное копирование кода;
 - 4) создание помех для корректной работы компьютера.

- По масштабу вредных воздействий компьютерные вирусы делятся на:
 - * **Безвредные** – не влияют на работу ПК, лишь уменьшают объем свободной памяти на диске, в результате своего размножения
 - * **Неопасные** – влияние, которых ограничивается уменьшением памяти на диске, графическими, звуковыми и другими внешними эффектами;
 - * **Опасные** – приводят к сбоям и зависаниям при работе на ПК;
 - * **Очень опасные** – приводят к потере программ и данных (изменение, удаление), форматированию винчестера и т.д.

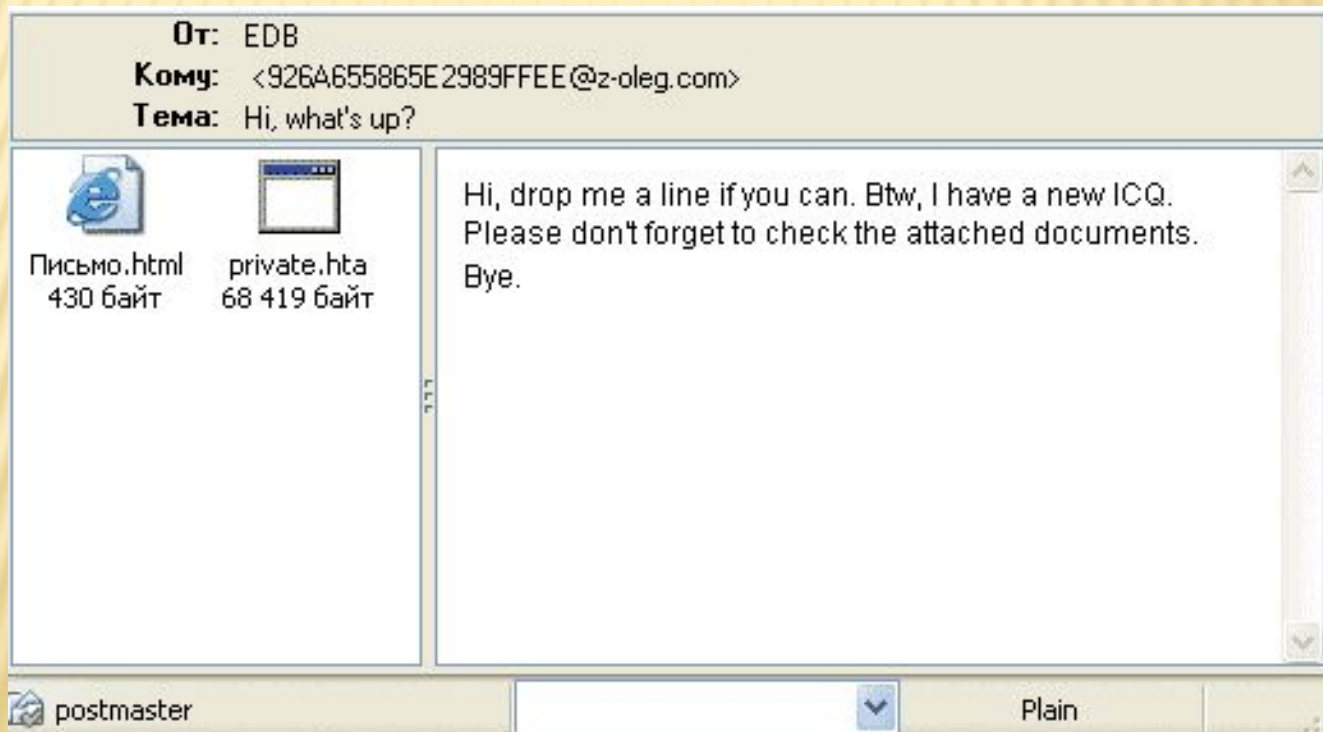
ПУТИ ЗАРАЖЕНИЯ ПК ПО ЭЛЕКТРОННОЙ ПОЧТЕ (МАСКИРОВКА ИСТИННОГО РАСШИРЕНИЯ ФАЙЛОВ)



ПУТИ ЗАРАЖЕНИЯ ПК ПО ЭЛЕКТРОННОЙ ПОЧТЕ (РАССЫЛКА АРХИВОМ С ПАРОЛЕМ)



РАССЫЛКА ВРЕДОНОСНЫХ СКРИПТОВ ИЛИ ФАЙЛОВ СПРАВКИ С ВРЕДОНОСНЫМИ ПРОГРАММАМИ



АНТИВИРУСНАЯ ПРОГРАММА

- **Антивирусная программа** — это приложение для поиска, блокировки и удаления вредоносных программ, а также профилактики заражения компьютера этими программами. С ее помощью можно защитить компьютер от вирусов.
- Для защиты от новых вирусов необходимо регулярно обновлять антивирусную программу.
- Большинство антивирусных программ можно настроить на автоматическое обновление.

Продукты "Лаборатории Касперского":

- Для дома
- Kaspersky Anti-Virus 2011 Build 11.0.2.556 CF2
- Kaspersky Internet Security 2011 Build 11.0.2.556 CF2
- Kaspersky PURE R2 9.1.0.124
- Для бизнеса
- Kaspersky Anti-Virus for Windows Workstations 6.0.4.1424 MP4 CF1
- Kaspersky Anti-Virus for Windows Servers 6.0.4.1424 MP4 CF1
- Kaspersky Anti-Virus for Windows Servers Enterprise Edition 8.0.0.559
- Kaspersky Small Office Security 2 Build 9.1.0.59
- Kaspersky Administration Kit 8.0.2134 CF2

Продукты Игоря Данилова:

Для дома

Dr.Web Antivirus Pro 6.00.1

Dr.Web Security Space Pro 6.00.1

Для бизнеса

Dr.Web for File Servers 6.00.1

Dr.Web Enterprise Suite 6.00 Build
201009100

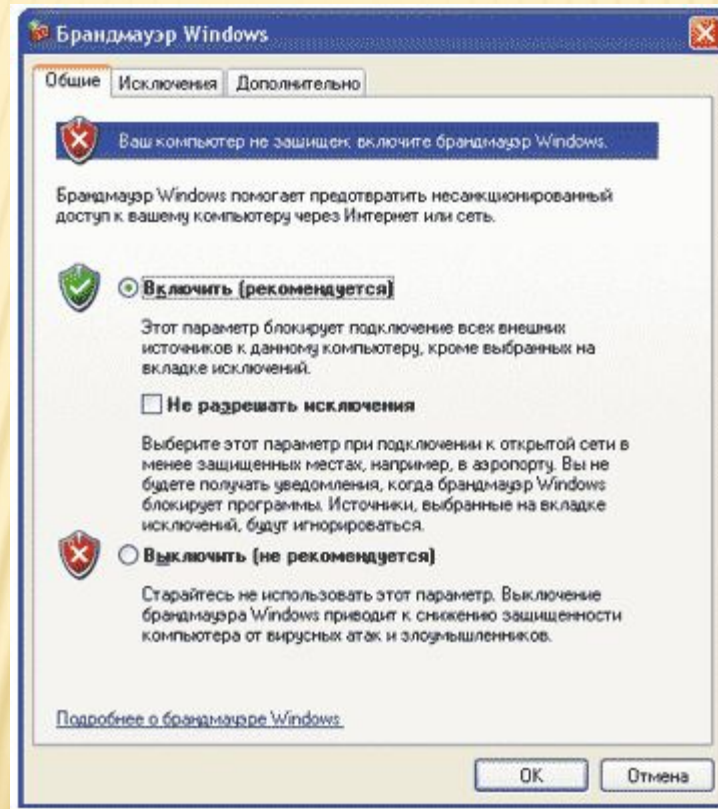
БРАНДМАУЭР (FIREWALL)

- Если компьютер используется дома, включение **брандмауэра** — самый эффективный и важный этап его защиты.
- Если сеть развернута дома или в малом офисе, необходимо защитить **каждый входящий в нее компьютер**.
- Для защиты сети служит аппаратный брандмауэр, например маршрутизатор. Кроме того, на каждом компьютере следует установить программный брандмауэр для блокировки распространения вируса в случае, если один из компьютеров все же будет заражен.

БРАНДМАУЭР (FIREWALL)

- ZoneAlarm,
- Norton Personal Firewall,
- OutPost Firewall,
- McAfee Internet Security,
- Kaspersky Anti-Hacker

НАСТРОЙКА БРАНДМАУЭРА В WINDOWS XP



ОТКЛЮЧАЕМ АВТОЗАПУСК ДЛЯ ЗАЩИТЫ ОТ ВРЕДНОСНОГО ПО (WINDOWS XP)

- 1. Пуск - Выполнить - пишем команду gpedit.msc
- 2. В разделе Конфигурация компьютера разверните по очереди узлы "Административные шаблоны" - "Система"
- 3. В окне справа находим пункт "Отключить автозапуск"
- 4. Дважды щелкните элемент "Отключить автозапуск"
- 5. Изменяем на "Включен" и видим ниже свойство "Отключить автозапуск на...: ставим «на Всех дисководах»"
- 6. Перезагружаем ПК

ОТКЛЮЧАЕМ АВТОЗАПУСК ДЛЯ ЗАЩИТЫ ОТ ВРЕДНОСНОГО ПО (WINDOWS XP)

The screenshot shows the Group Policy Editor window titled "Групповая политика". The left pane shows the tree structure with "Система" selected under "Административные шаблоны". The right pane displays a list of policies, with "Отключить автозапуск" (Disable automatic startup) highlighted and its state set to "Включена" (Enabled). A red arrow points to this policy.

Состояние	Состояние
Профили пользователей	
Сценарии	
Вход в систему	
Дисковые квоты	
Сетевой вход в систему	
Групповая политика	
Удаленный помощник	
Восстановление системы	
Отчет об ошибках	
Защита файлов Windows	
Удаленный вызов процедур (RPC)	
Служба времени Windows	
Управление связью через Интернет	
DCOM	
Предотвращение доступа к потенциально небезопасным фу...	Не задана
Не отображать страницу "Управление данным сервером" при...	Не задана
Отображать диалог слежения за завершением работы	Не задана
Включить свойство данных состояния системы слежения за ...	Не задана
Включить постоянную временную метку	Не задана
Указать расположение установочных файлов Windows	Не задана
Указать размещение установочных файлов пакета обновлен...	Не задана
Отключить сообщения о состоянии загрузки, завершения ра...	Не задана
Подробные сообщения о состоянии	Не задана
Запретить запуск из Справки перечисленных программ	Не задана
Отключить автозапуск	Включена
Не выполнять автоматическое шифрование файлов, переме...	Не задана
Загружать отсутствующие COM-компоненты	Не задана
Разрешить клиентам отслеживания изменившихся связей исп...	Не задана
Не выключайте питание компьютера после завершения раб...	Не задана
Отключить запрос на использование Windows Update при по...	Не задана

ОТКЛЮЧАЕМ АВТОЗАПУСК ДЛЯ ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПО (WINDOWS 7)

The screenshot shows the Windows 7 Group Policy Editor. The left pane shows the navigation tree with 'Политики автозапуска' (Autorun Policies) selected. The right pane displays the 'Отключить автозапуск' (Turn off autorun) policy. The policy is currently set to 'Отключена' (Disabled). A table below the policy details shows the status of various related settings.

Состояние	Состояние	Комментарий
Отключить автозапуск	Отключена	Нет
Не устанавливать флажок «Всегда выполнять выбранное...	Не задана	Нет
Отключить автозапуск устройств, не являющихся томами	Не задана	Нет
Вариант работы автозапуска по умолчанию	Не задана	Нет

AUTORUN.INF

- **Autorun.inf** — файл, используемый для автоматического запуска или установки приложений и программ на носителях информации в среде операционной системы Microsoft Windows (начиная с версии Windows 95).

-
- В настоящее время файл **autorun.inf** широко используется для распространения компьютерных **вирусов** через **flash-накопители** и сетевые диски. Для этого авторы вирусов прописывают имя исполняемого файла с вредоносным кодом в параметр open. При подключении заражённого flash-накопителя **Windows** запускает записанный в параметре «open» файл на исполнение, в результате чего происходит заражение компьютера.

МЕТОДЫ ЗАЩИТЫ ПК ОТ ВИРУСОВ

AUTORUN.INF

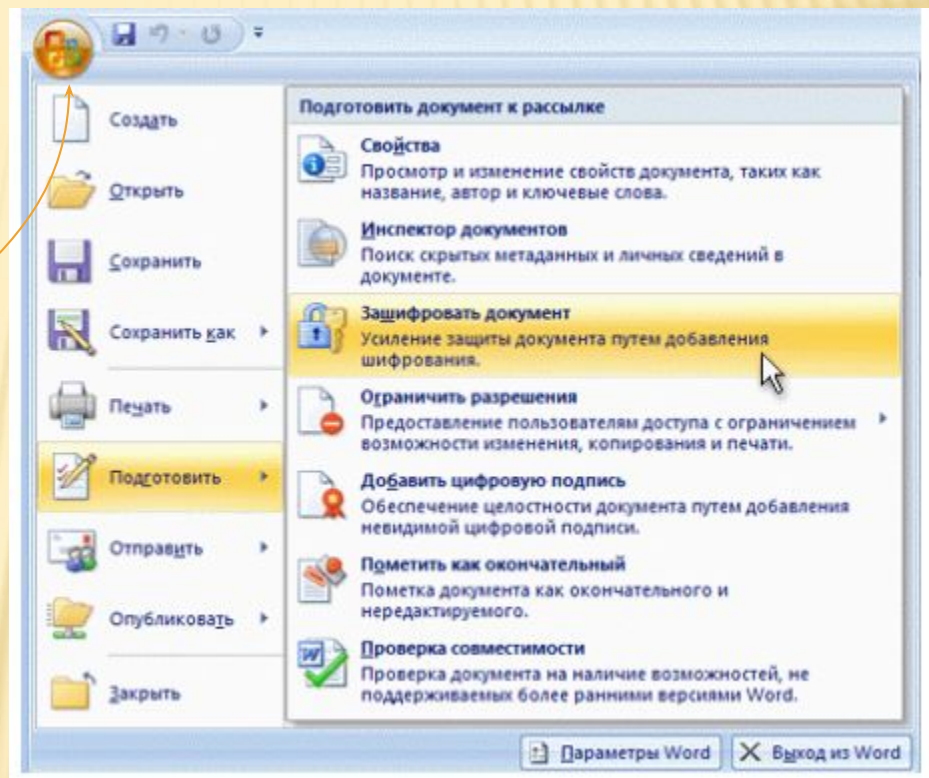
- 1) Отключение Автозапуска (см. слайды выше);
- 2) Удаление файла **Autorun.inf** с носителей и создание Папки с именем **Autorun.inf** !!!

ЗАЩИТА ВАШЕЙ ЛИЧНОЙ ИНФОРМАЦИИ НА ПК (ПАРОЛЬНАЯ ЗАЩИТА)

- Используйте надежные пароли, представляющие собой **сочетание прописных и строчных букв, цифр и символов**. Пароли, не содержащие набор таких элементов, являются ненадежными.
- Надежный пароль: **Y6dh!et5.**
- Ненадежный пароль: **House27.**
- Пароли должны состоять не менее чем из 8 знаков. Рекомендуется использовать фразу-пароль, состоящую из 14 или более знаков.

ШИФРОВАНИЕ ДОКУМЕНТА И ЗАДАНИЕ ПАРОЛЯ ДЛЯ ЕГО ОТКРЫТИЯ

- Чтобы зашифровать файл и задать пароль для его открытия, выполните действия, описанные ниже.
- Нажмите кнопку Microsoft Office, наведите указатель мыши на пункт Подготовить и выберите пункт Зашифровать документ.



ВАША ЛИЧНАЯ БЕЗОПАСНОСТЬ ЗА ПК:

- Согласно исследованиям американских ученых (2010 год) за компьютером можно проводить не более 3 часов в день.
- Не проводите много времени за экраном монитора, это вредно для здоровья: новые мониторы не очень полезны для зрения. Фильмы лучше смотреть по телевизору.
- Не забывайте о настройке монитора компьютера (в Windows это называется настройка темы). Устанавливайте приятные вам цвета шрифта и экрана, не портящие глаза.

-
- Удачной всем зачетной недели и сессии.
 - Искренне Ваша.
 - И.В. Усикова)))