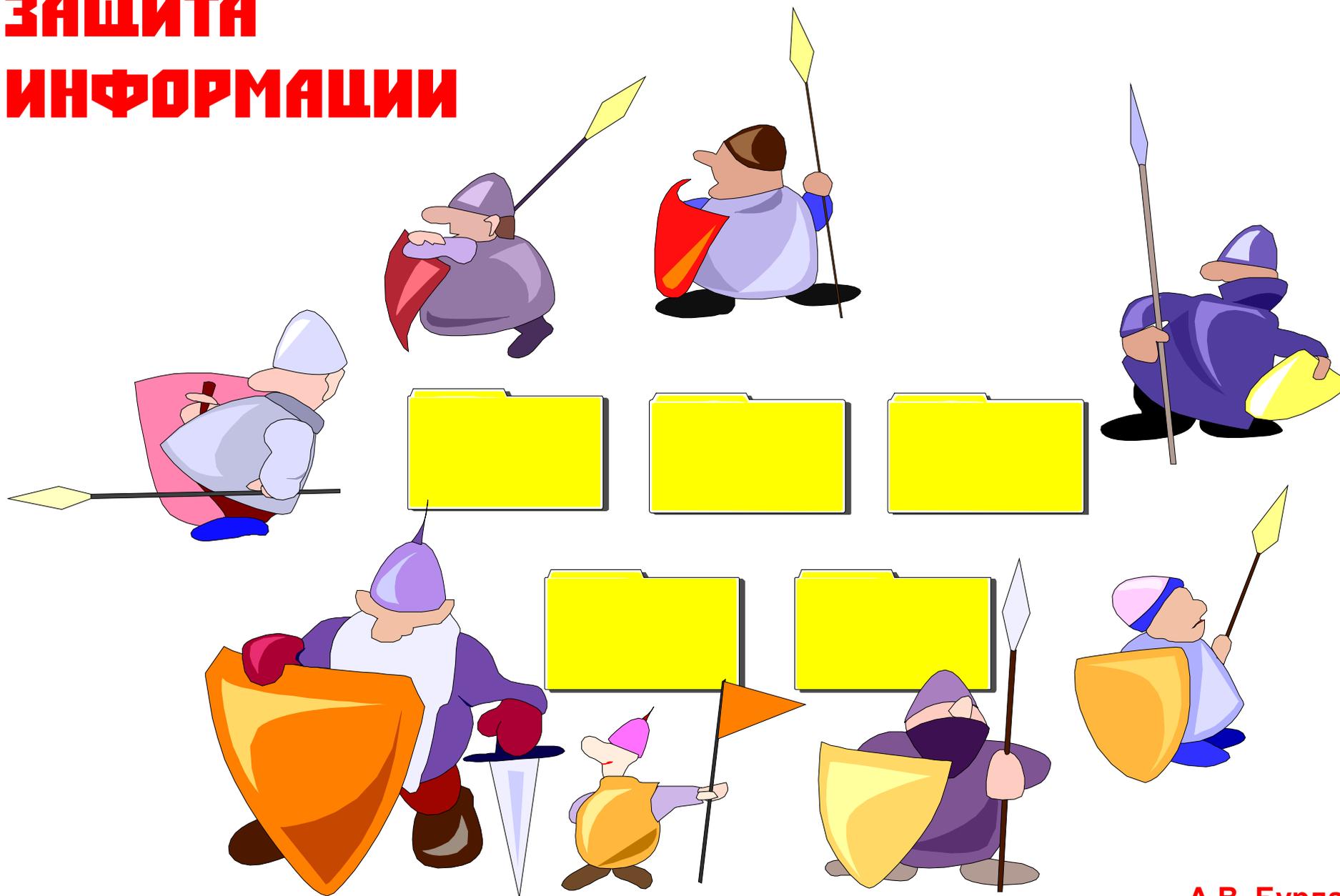


# ЗАЩИТА ИНФОРМАЦИИ



**А.В. Бурдаев**  
заместитель директора по ИТ  
МОУ Просветской СОШ м.р. Волжский Самарской области

# ЗНАЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Компьютеры, да еще и объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных.

Теперь нетехнический специалист среднего уровня может выполнять работу, которую раньше делал только высококвалифицированный программист. Служащий имеет в своем распоряжении столько точной и оперативной информации, сколько никогда не имел.

Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным.

Все увеличивается число компьютерных преступлений, что может привести в конечном счете к подрыву экономики. И поэтому становится ясно, что **информация - это ресурс, который надо защищать.**

# ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Целостность** - защита от сбоев, ведущих к потере информации

**Конфиденциальность** – недоступность информации третьим лицам

**Доступность** данных для авторизованных пользователей.

**Точки приложения процесса защиты информации к системе:**

аппаратное обеспечение,

программное обеспечение и

обеспечение связи (коммуникации).



**СРЕДСТВА И КАНАЛЫ СВЯЗИ**

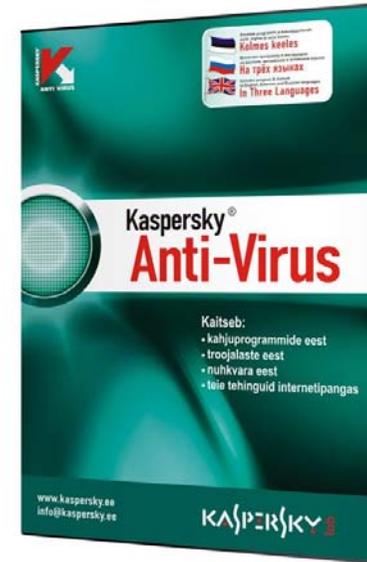
# ПРИЧИНЫ ПОТЕРИ ИНФОРМАЦИИ

- 1. Несанкционированный доступ** извне, копирование или изменение информации случайные или умышленные действия, приводящие:
  - к искажению либо уничтожению данных;
  - к ознакомлению посторонних лиц с конфиденциальной информацией.
- 2. Некорректная работа программного обеспечения**, приводящая к потере или порче данных из-за:
  - ошибок в прикладном или сетевом ПО;
  - заражения систем компьютерными вирусами.
- 3. Технические сбои оборудования**, вызванные:
  - отключением электропитания;
  - отказом носителей
- 4. Ошибки обслуживающего персонала.**
  - при работе с аппаратными средствами
  - при работе с ПО
  - при обработке информации



# КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

- средства физической защиты (ИБП, механические и электронные ключи)
- программные средства (антивирусные программы, системы разграничения полномочий, программные средства контроля доступа);
- административные меры защиты (ограничение доступа в помещения и к компьютерам).



# АДМИНИСТРАТИВНЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ



**Разделение персонала с выделением помещений** или расположением подразделений компактными группами на некотором удалении друг от друга.

**Ограничение доступа в помещения посторонних лиц** или сотрудников других подразделений. Совершенно необходимо запирать и опечатывать помещения при сдаче их под охрану после окончания работы.

**Ограничение круга лиц, имеющих доступ к каждому компьютеру.**

Требование **в перерывах выключать компьютер** или **использовать специальные программы – хранители экранов**, которые позволяют стереть информацию с экрана монитора и закрыть паролем возможность снятия режима хранителя экрана.

# ЗАЩИТА ИНФОРМАЦИИ ПРИ ТЕХНИЧЕСКИХ СБОЯХ

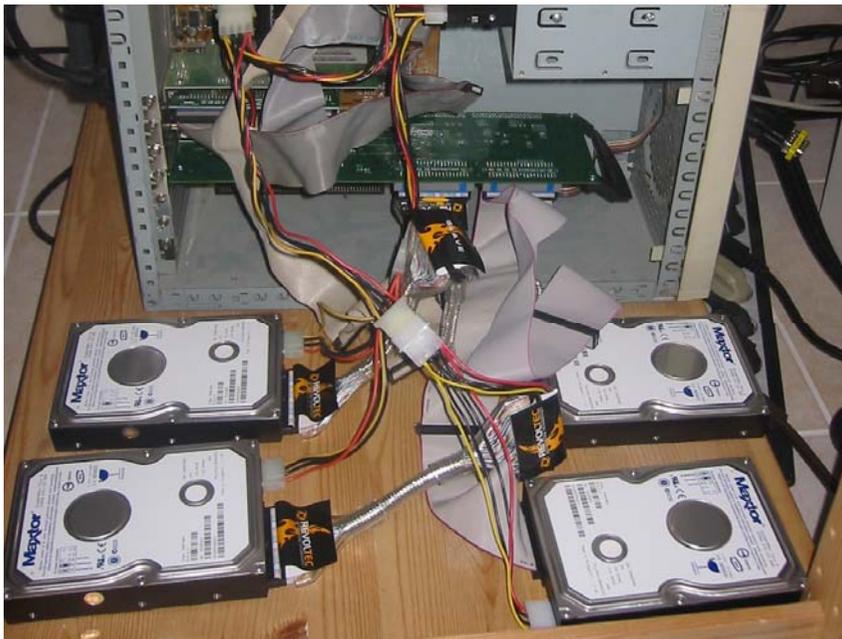
Защита при отключении электропитания:

- **установка источников бесперебойного питания (ИБП).**

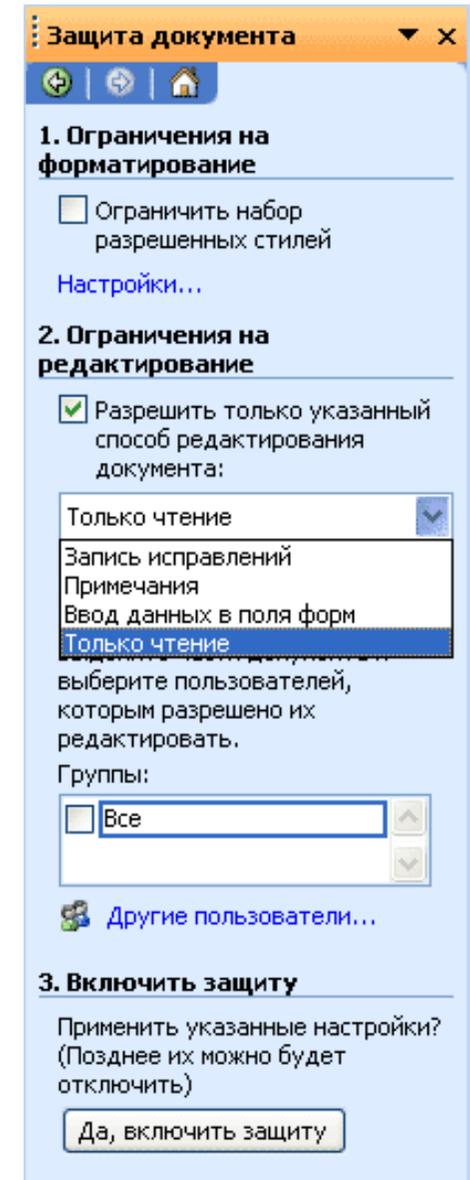
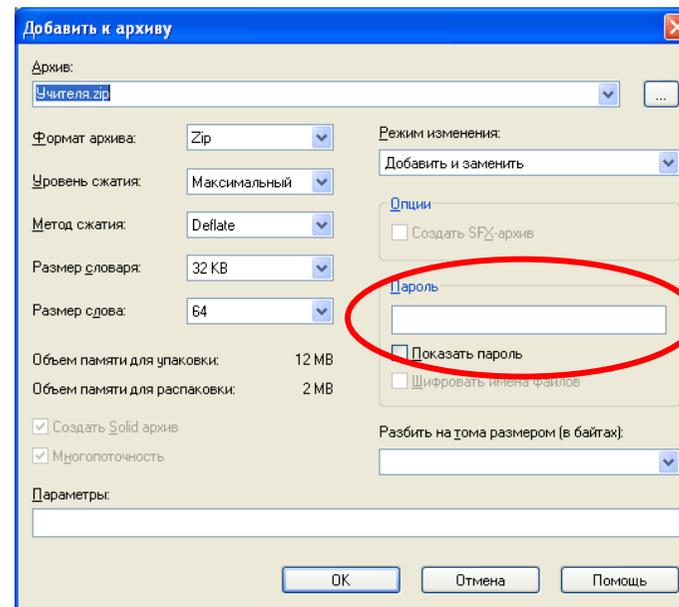
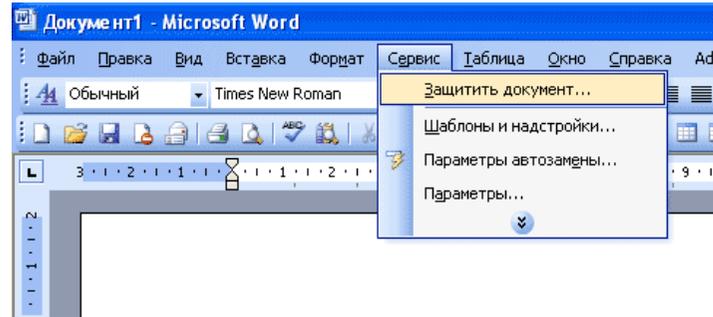
Предотвращение сбоя дисков:

- дублирующие друг друга **зеркальные диски**, либо **дисковые массивы** – избыточные системы независимых дисков (Redundant Arrays of Independent Disks, RAID).
- архивация данных – **создание резервных копий** информации на различных носителях или в пределах одного носителя.

Для ценной архивной информации предусматривают отдельное помещение. Дубликаты наиболее ценных данных хранят в другом здании или даже в другом городе. Последняя мера делает данные неуязвимыми в случае пожара или другого стихийного бедствия.



# ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ЧЕРЕЗ СИСТЕМУ ПАРОЛЕЙ



**Уровни установки паролей:**

**Базовый** - пароль на BIOS

**Системный** – создание учетных записей и групповых политик

**Программный** – установка паролей на запуск приложений, доступ к каталогам и выполнение операций через специальные программы

**Уровень приложений** – защита паролем создаваемых документов и архивов.

# ВРЕДОНОСНОЕ ПО (MALWARE)

**Вредоносная программа** — это любое программное обеспечение, предназначенное для обеспечения получения несанкционированного доступа к информации, хранимой на ЭВМ с целью причинения вреда (ущерба) владельцу информации и/или владельцу ЭВМ (сети ЭВМ).



*Программа, наносящая ущерба третьим лицам: крэк (ущерб правообладателю), hack tool - не является вредоносной.*

## **ОСНОВНЫЕ ВИДЫ (классификация по способам распространения)**

**Компьютерный вирус** — распространяется в пределах одного компьютера. Заражение других компьютеров происходит только при непреднамеренном распространении пользователями, например, через внешние носители. Различают файловые, загрузочные, стелс-, макро-, полиморфные и т.д. вирусы

**Сетевой червь** — распространяется по сети самостоятельно.

**Троян** не имеет собственных механизмов распространения, сознательно или неосознанно устанавливается пользователем, часто под видом полезного ПО — кодеков, скринсейверов и т.п..

**Бэкдор** — загружается трояном или злоумышленником собственноручно, после получения им доступа к системе.

А также: *шпионы, руткит, кейлоггеры, ботнеты, эксплойты* и т.д...

# ПРИЗНАКИ АКТИВНОСТИ ВРЕДНОСНОГО ПО

Условно делятся на две группы:

## Сбои в работе аппаратного и программного обеспечения

- прекращение или сильное замедление доступа в интернет;
- изменение домашней страницы в браузере, автоматическое открытие новых окон (вкладок);
- отключение антивируса, блокировка доступа к антивирусным сайтам;
- невозможность запустить исполняемый файл (выдается сообщение об ошибке);
- невозможность открытия дисков или папок
- случайное и/или беспорядочное завершение работы компьютера или программ

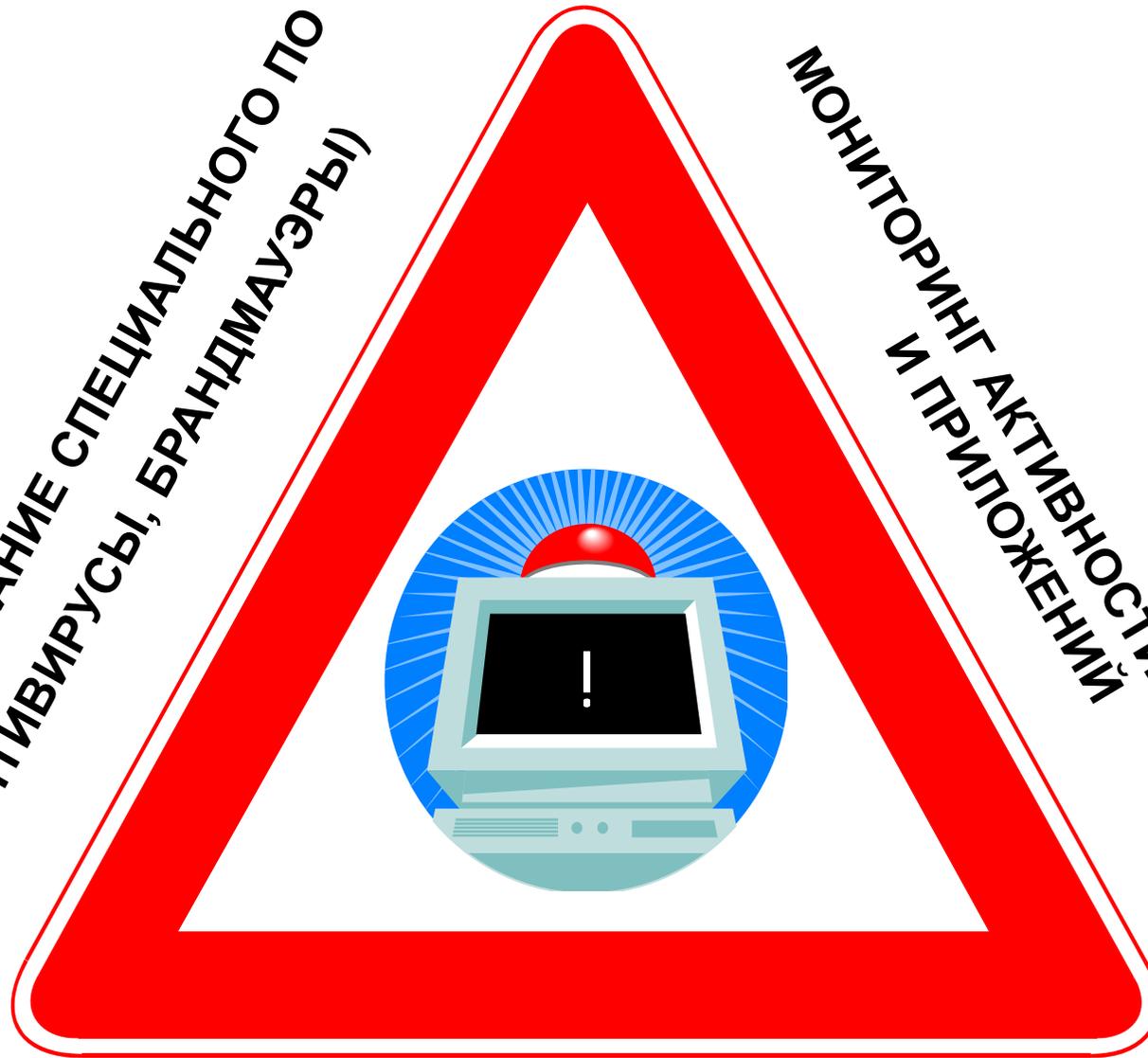
## Несанкционированная активность системы и приложений

- запрос неизвестных программ на доступ в интернет
- изменение обоев на рабочем столе, появление новых значков;
- появление новых неизвестных процессов в диспетчере задач;
- появление в автозапуске новых приложений;
- запрет на изменение настроек компьютера администратором;
- всплывание окон системных сообщений с непривычным текстом;
- мониторы интернета показывают фальшивые загрузки;
- перезапуск компьютера во время старта какой-либо программы;



# СПОСОБЫ ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПО

**ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНОГО ПО  
(АНТИВИРУСЫ, БРАНДМАУЭРЫ)**



**МОНИТОРИНГ АКТИВНОСТИ СИСТЕМЫ  
И ПРИЛОЖЕНИЙ**

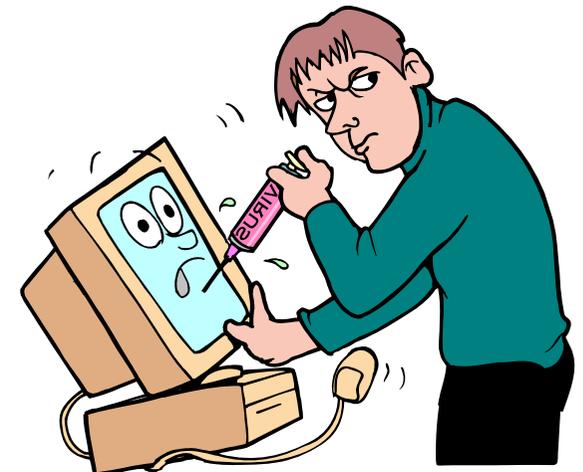
**КОНТРОЛЬ ЗА СМЕННЫМИ НОСИТЕЛЯМИ  
(ЗАЩИТА ОТ ЗАПИСИ, ОТКЛЮЧЕНИЕ АВТОЗАПУСКА)**

# КЛАССИФИКАЦИЯ ЗАЩИТНОГО ПО



# ПРЕСТУПЛЕНИЯ В СФЕРЕ IT

- **взлом интернет-сайтов ("хакинг")**, обычно с последующим изменением содержания сайта.
- **"кардинг"** - похищение реквизитов, идентифицирующих пользователей в сети Интернет как владельцев банковских кредитных карт с их возможным последующим использованием.
- **"крекинг"** - снятие защиты с программного обеспечения для последующего бесплатного использования. Сюда же можно отнести пиратское распространение законно купленных копий программного обеспечения.
- **незаконное получение и использование чужих учетных данных** для пользования сетью Интернет.
- **"нюкинг"**, или "d.o.s."-атаки - **действия, вызывающие "отказ в обслуживании"** (Denial of Service) - "зависание" удаленного компьютера.
- **"спамминг"** - **массовая несанкционированная рассылка электронных сообщений** рекламного или иного характера.
- **чтение чужих электронных сообщений.**



# ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ IT



## Специализированные статьи:

### Глава 28. Преступления в сфере компьютерной информации

#### Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.
2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

#### Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.
2. Те же деяния, повлекшие тяжкие последствия - наказываются лишением свободы на срок от трех до семи лет.

#### Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.
2. То же деяние, повлекшее по неосторожности тяжкие последствия - наказывается лишением свободы на срок до четырех лет.

# ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ IT



## Прочие статьи:

**Статья 117.** Истязание (причинение физических или психических страданий насильственными действиями).

**Статья 129.** Клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию в публично демонстрирующемся произведении или средствах массовой информации.

**Статья 130.** Оскорбление, то есть унижение чести и достоинства другого лица, выраженное в неприличной форме публично демонстрирующемся произведении или средствах массовой информации.

**Статья 137.** Нарушение неприкосновенности частной жизни, то есть незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан.

**Статья 138.** Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений,

**Статья 159.** Мошенничество - хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

**Статья 165.** Причинение имущественного ущерба путем обмана или злоупотребления доверием.

**Статья 174.** Легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления.

**Статья 183.** Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, а равно иным незаконным способом.

**Статья 187.** Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов

**Статья 213.** Хулиганство, то есть грубое нарушение общественного порядка, выражающее явное неуважение к обществу, сопровождающееся угрозой применения насилия, а равно уничтожением или повреждением чужого имущества.

# ЗАЩИТА АВТОРСКИХ ПРАВ НА ПРОГРАММНЫЕ ПРОДУКТЫ

## Законами РФ:

от 09.07.1993 №5351-1 (ред. от 20.07.2004)

«Об авторском праве и смежных правах» (п.1 ст.7)

от 23.09.1992. №3523-1 (ред. от 02.02.2006)

«О правовой охране программ для ЭВМ и баз данных». (п.2 ст. 2)

**ПРОГРАММЫ ДЛЯ ЭВМ ОТНЕСЕНЫ К ОБЪЕКТАМ  
АВТОРСКОГО ПРАВА.**



Согласно закону «О правовой охране программ...»:

Ст. 14 ч. 1. **Использование программы для ЭВМ** пользователями **осуществляется на основании договора с правообладателем**

Ст. 14 ч. 2. **Договор** на использование программы для ЭВМ или базы данных **заключается в письменной форме.**

Ст. 14 ч. 3. **При продаже и предоставлении массовым пользователям доступа к программам для ЭВМ и базам данных допускается применение особого порядка заключения договоров, например путем изложения условий договора на передаваемых экземплярах программ для ЭВМ и баз данных.**

# ПРАВА ПОЛЬЗОВАТЕЛЯ



Согласно закону «О правовой охране программ для ЭВМ...»:

**Использование программы для ЭВМ** или базы данных - это выпуск в свет, **воспроизведение** (изготовление одного или более экземпляров программы для ЭВМ или базы данных в любой материальной форме, а также их **запись в память ЭВМ**), **распространение** (предоставление доступа к воспроизведенной программе) и иные действия по их введению в хозяйственный оборот.

**Ст. 15 ч. 1.** Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без получения дополнительного разрешения правообладателя **осуществлять любые действия, связанные с функционированием программы** для ЭВМ или базы данных в соответствии с ее назначением. ...Запись и хранение в памяти ЭВМ допускаются в отношении одной ЭВМ или одного пользователя в сети, если иное не предусмотрено договором с правообладателем.

**Ст. 15 ч. 2.** ...лицо, правомерно владеющее экземпляром программы для ЭВМ, **вправе** без согласия правообладателя и без выплаты ему дополнительного вознаграждения:

- **осуществлять адаптацию программы** для ЭВМ или базы данных;
- **изготавливать или поручать изготовление копии** программы для ЭВМ или базы данных при условии, что эта копия предназначена **только для архивных целей**.

# ТИПЫ ЛИЦЕНЗИЙ Software



## Проприетарное (коммерческое)

## Бесплатное

### ОЕМ-лицензия

(привязана к оборудованию)



### Открытая лицензия

(привязана к приобретателю)

### Коробочная лицензия

(«самодостаточна»)

### Некоммерческое

Freeware, Public domain, Open source,  
Donateware, Abandonware, Adware

### Условно-бесплатное

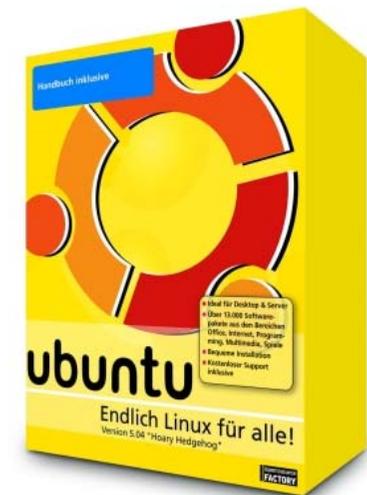
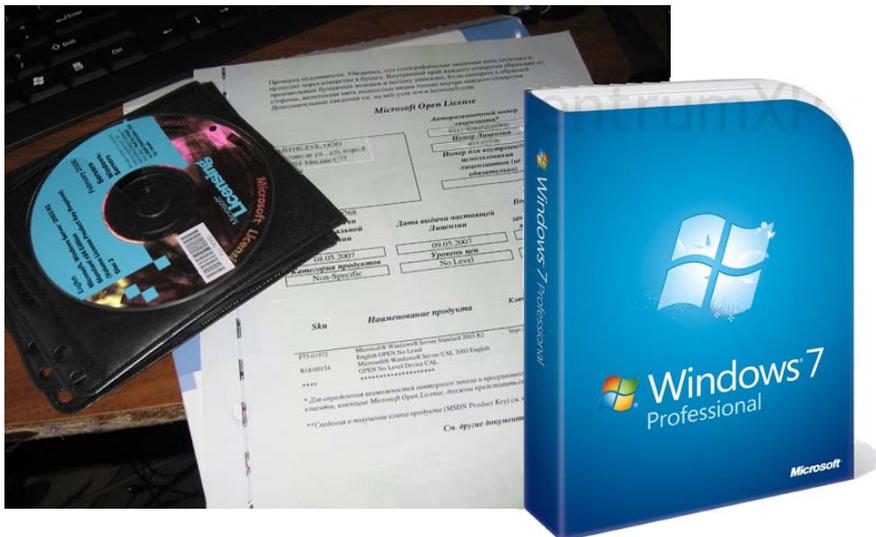
Shareware, Nagware, Crippleware,  
Leware

### Пробное

Trialware, Betaware

### Демонстрационное

Demoware, CD-ware



# КОНТРАФАКТНЫЕ ЭКЗЕМПЛЯРЫ ПО



Согласно закону «О правовой охране программ для ЭВМ...»:

**Ст. 17 ч.1. Физическое или юридическое лицо, которое не выполняет требований настоящего Закона** в отношении исключительных прав правообладателей, в том числе ввозит в Российскую Федерацию экземпляры программы для ЭВМ или базы данных, изготовленные без разрешения их правообладателей, **является нарушителем авторских прав.**

**Ст. 17 ч. 2. Контрафактными признаются экземпляры программы для ЭВМ или базы данных, изготовление или использование которых влечет за собой нарушение авторских прав.**

**Ст. 18 ч. 1. Автор программы для ЭВМ и иные правообладатели вправе требовать:**

признания прав; восстановления положения, существовавшего до нарушения права, и **прекращения действий, нарушающих право** или создающих угрозу его нарушения; **возмещения** лицом, нарушившим исключительное право, **причиненных убытков** в соответствии с гражданским законодательством;

**принятия иных предусмотренных законодательными актами мер**, связанных с защитой их прав.

**Ст. 18 ч.2. За защитой своего права правообладатели могут обратиться в суд, арбитражный или третейский суд.**

# ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ НЕЛИЦЕНЗИОННОГО ПО

## Кодекс РФ об административных правонарушениях:



**Статья 7.12.** Нарушение авторских и смежных прав, изобретательских и патентных прав

Ввоз, продажа, сдача в прокат или иное **незаконное использование экземпляров произведений или фонограмм в целях извлечения дохода** в случаях, если экземпляры произведений или фонограмм являются контрафактными в соответствии с законодательством РФ об авторском праве и смежных правах..., а равно иное нарушение авторских и смежных прав в целях извлечения дохода - влечет наложение административного штрафа на граждан в размере от пятнадцати до двадцати минимальных размеров оплаты труда с конфискацией контрафактных экземпляров..., и иных орудий совершения административного правонарушения; на должностных лиц - от тридцати до сорока минимальных размеров оплаты труда с конфискацией...; на юридических лиц - от трехсот до четырехсот минимальных размеров оплаты труда с конфискацией...

## Уголовный кодекс РФ



**Статья 146.** Нарушение авторских и смежных прав

**Часть 2.** **Незаконное использование объектов авторского права** или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в **крупном размере** (**стоимость** экземпляров произведений или фонограмм либо стоимость прав на использование объектов авторского права и смежных прав **превышают пятьдесят тысяч рублей**), - наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет.

**Часть 3.** Деяния, предусмотренные частью второй настоящей статьи, если они совершены **группой лиц** по предварительному сговору или организованной группой; в **особо крупном размере** (**стоимость** экземпляров произведений или фонограмм либо стоимость прав на использование объектов авторского права и смежных прав **превышают двести пятьдесят тысяч рублей**); **лицом с использованием своего служебного положения**, - наказываются лишением свободы на срок до пяти лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового.