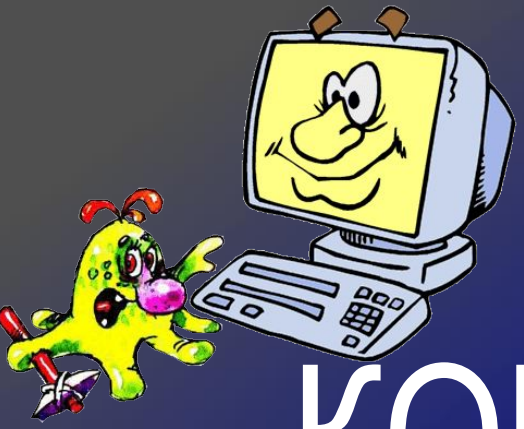
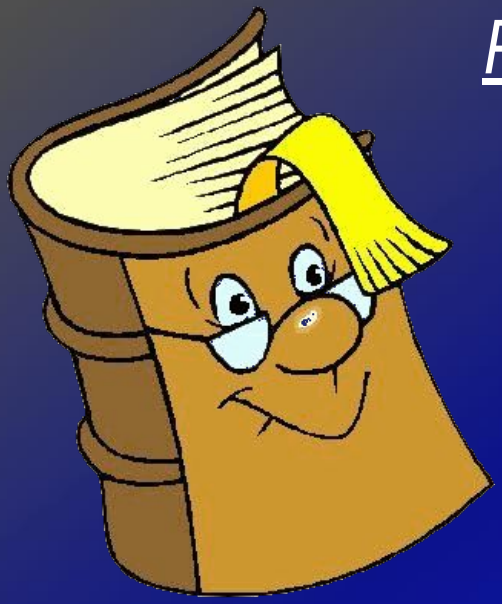


КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

ЧТО ТАКОЕ ИНФОРМАЦИЯ?

РАЗЪЯСНЕНИЕ, ИЗЛОЖЕНИЕ



ТРИ ПРИНЦИПА

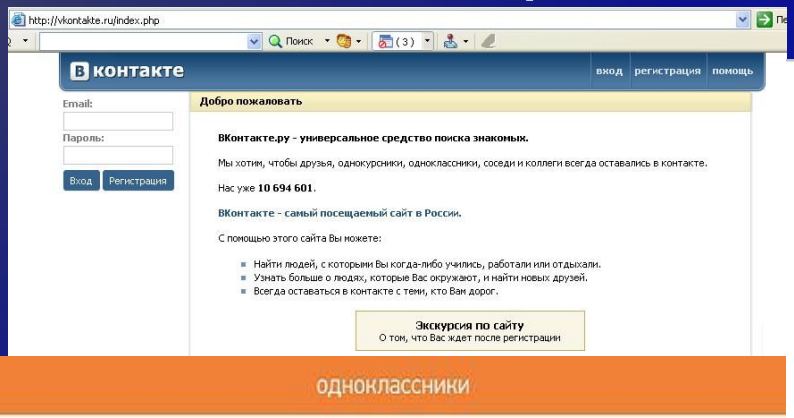
- Целостность данных
- Конфиденциальность информации
- Доступность информации для всех авторизованных пользователей

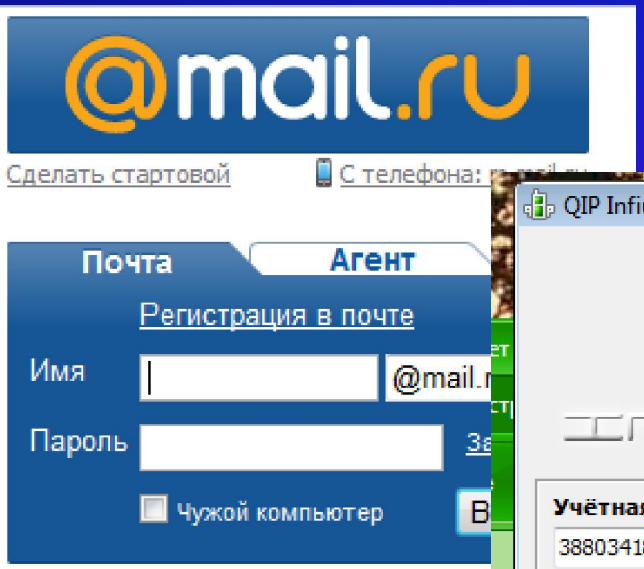
ОСНОВНЫЕ ЦЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ

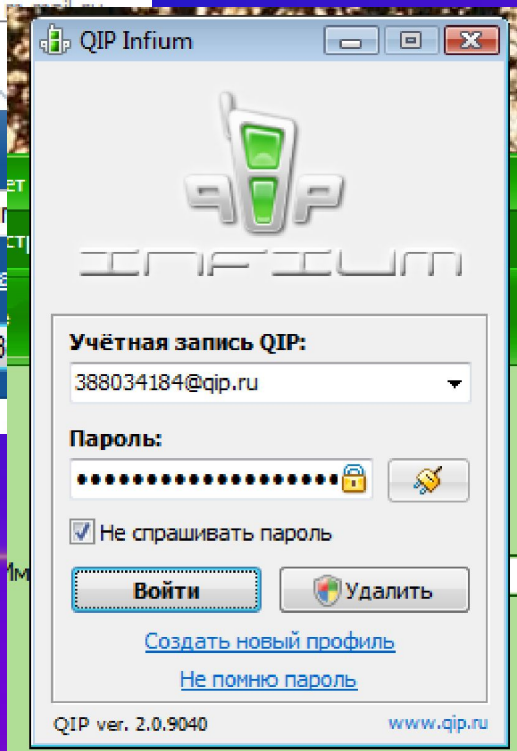
- ✔ Обеспечение физической целостности;
- ✔ Предупреждение несанкционированного получения;
- ✔ Предупреждение несанкционированной модификации;
- ✔ Предупреждение несанкционированного копирования;
- ✔ Хищение носителей информации (дисков, распечаток и т. д.);
- ✔ Чтение или фотографирование информации с экрана;
- ✔ Программный несанкционированный доступ к информации.

ПОГОВОРИМ О ВЫБОРЕ ПАРОЛЯ

Пароль – конкретно выбранное засекреченное слово или засекреченная строка символов







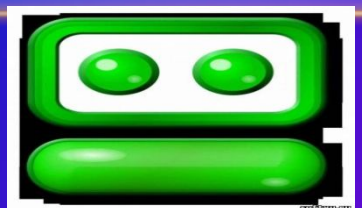
RoboForm

- • Автоматически сохраняет введенные интернет-пароли.
- • Автоматически вводит пароли в формы.
- • Нажимает кнопку Login за Вас.
- • Заполняет формы вашей персональной информацией.
- • Сохраняет различную секретную информацию и заметки.
- • Генерирует случайные пароли.

RoboForm2GO

Удивительно простой в использовании

- 1. Подключите USB-диск с RoboForm2Go к любому компьютеру в любой точке Мира.
- 2. RoboForm2Go сохранит ваши пароли и закладки, поможет быстро войти в сетевые учетные записи, а также заполнит сложные регистрационные и платежные формы.
- 3. Отключите ваш USB-диск - и никаких личных данных не останется на компьютере: RoboForm2Go не оставляет следов своей работы.



КАКИМ ОБРАЗОМ ЛУЧШЕ ВЫБИРАТЬ СОСТАВЛЯЮЩИЕ ДЛЯ ПАРОЛЯ?

- Не применять пароль, который является словарным словом.
- Если есть возможность, то можно использовать знаки препинания.
- Можно применять символы из нижнего и верхнего регистров, а так же цифры от 0 до 9.

Valentina ValenTINA84

- Оптимальным для составления пароля является количество цифр (букв) от 8 – 10.
- Использовать последние символы из списка цифр, знаков или алфавита.
- Остерегаться программ перехватчиков.

ЧТО ТАКОЕ ФИШИНГ?

Фишинг – вид интернет-мошенничества, цель которого – получить идентифицированные данные пользователей.

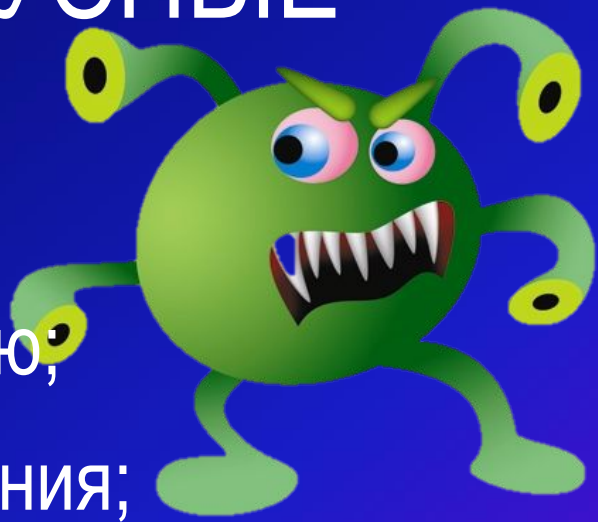
«Если не сообщите данные в течении недели, вы будете заблокированы»

«Если хотите обезопасить себя от фишинга, пройдите по этой ссылке и введите свой логин и пароль»

В США в 2006 году ущерб составил 1244 долларов.

В 2005 году сумма не превышала 257 долларов

ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ



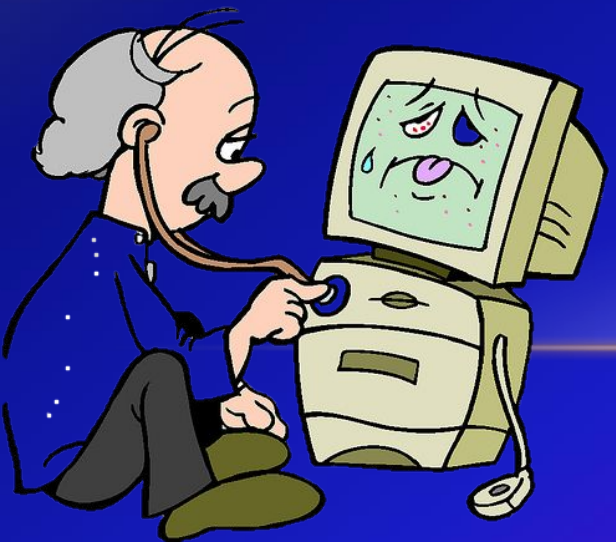
- Способность к саморазмножению;
- Высокой скорости распространения;
- Избирательности поражаемых систем;
- Трудности борьбы с вирусами и т.д.

КОМПЬЮТЕРНЫЙ ВИРУС -

Это программа, которая может создавать свои копии и внедрять их в файлы, загрузочные секторы дисков, сети.

При этом копии сохраняют возможность дальнейшего распространения.

Часто вирусы обладают разрушительным действием.



КАК НАЗЫВАЕТ СЕБЯ ЧЕЛОВЕК, КОТОРЫЙ «ПИШЕТ» ВИРУСЫ?

ВИРЬМЕЙКЕР

КАК МОЖЕТ ПОПАСТЬ НА ПК ВРЕДОНОСНАЯ ПРОГРАММА?

- Глобальная сеть Internet
- Электронная почта
- Локальная сеть
- Компьютеры «общего назначения»
- Пиратское программное обеспечение
- Съемные носители

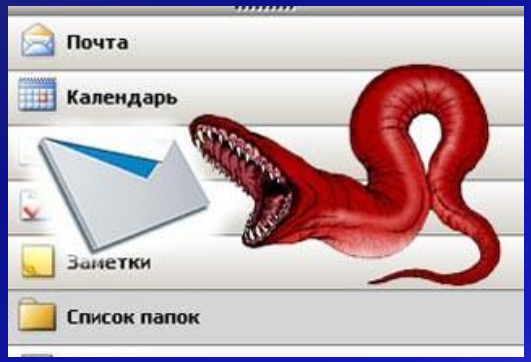
ОСНОВНЫЕ ПРИЗНАКИ ПРОЯВЛЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

- Неправильная работа нормально работающих программ;
- Медленная работа компьютера;
- Невозможность загрузки ОС;
- Исчезновение файлов и каталогов;
- Изменение размеров файлов;
- Неожиданное увеличение количества файлов на диске;
- Уменьшение размеров свободной оперативной памяти;
- Выводы на экраны неожиданных сообщений и изображений;
- Подача непредусмотренных звуковых сигналов;
- Частые зависания и сбои в работе компьютера

ПРИЗНАКИ КЛАССИФИКАЦИИ ВИРУСОВ

среда обитания

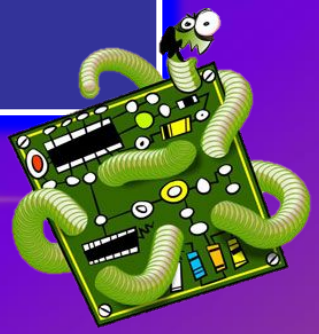
особенности алгоритма работы



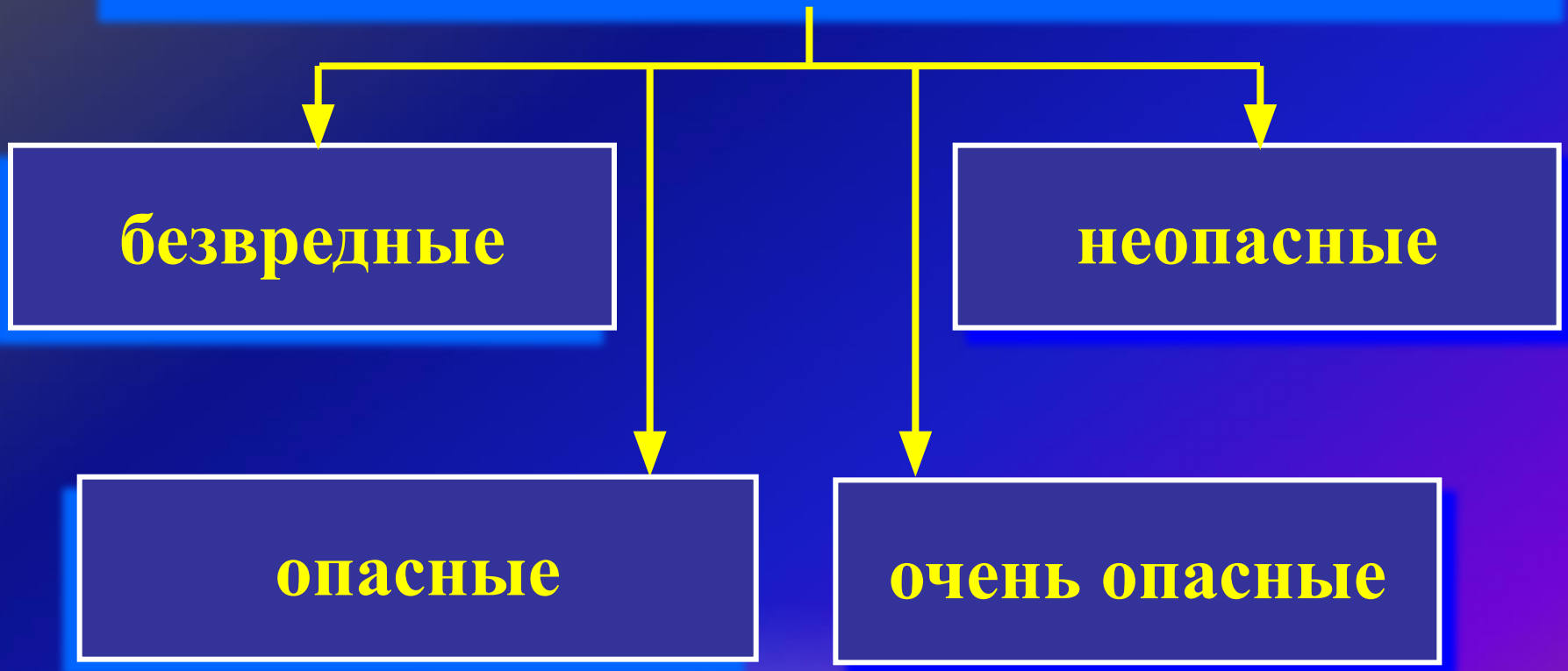
деструктивные возможности

СРЕДА ОБИТАНИЯ

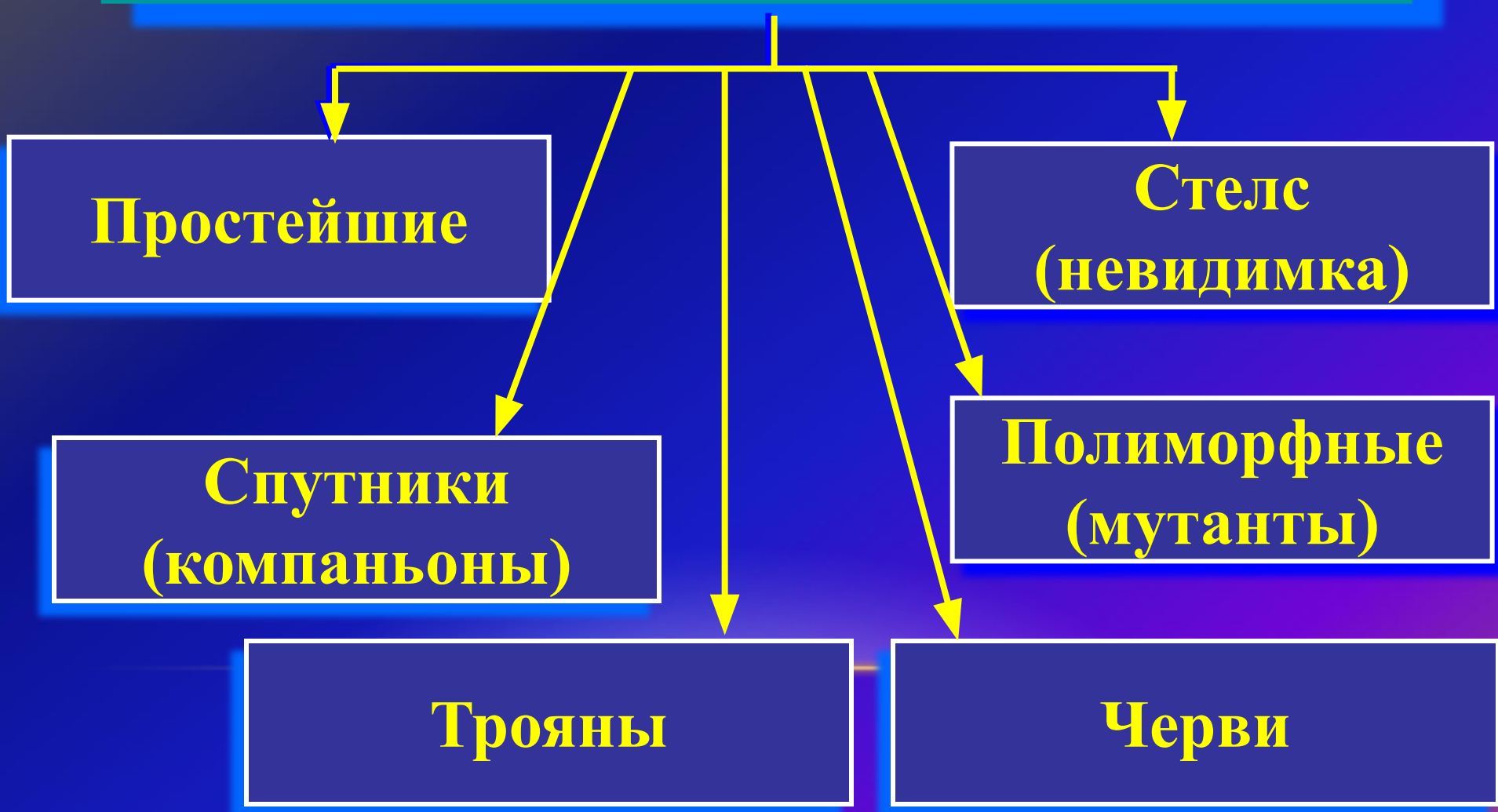
- файловые
- загрузочные
- макро
- сетевые



ДЕСТРУКТИВНЫЕ ВОЗМОЖНОСТИ



Алгоритм работы

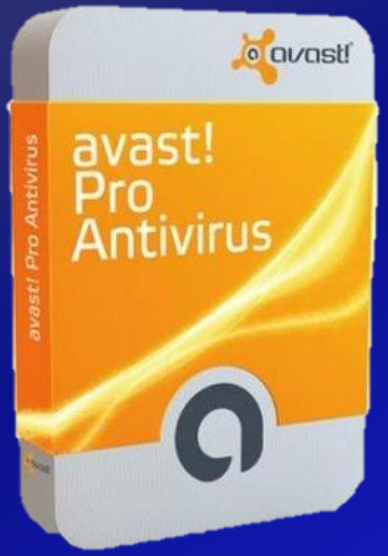


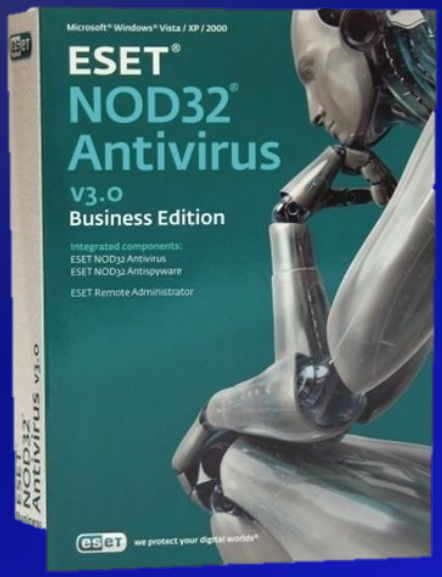
АНТИВИРУСНАЯ ПРОГРАММА

Программа, позволяющая выявлять вирусы, лечить зараженные файлы и диски, обнаруживать и предотвращать подозрительные действия.

- Сканеры, ревизоры
- Блокировщики
- Иммунизаторы

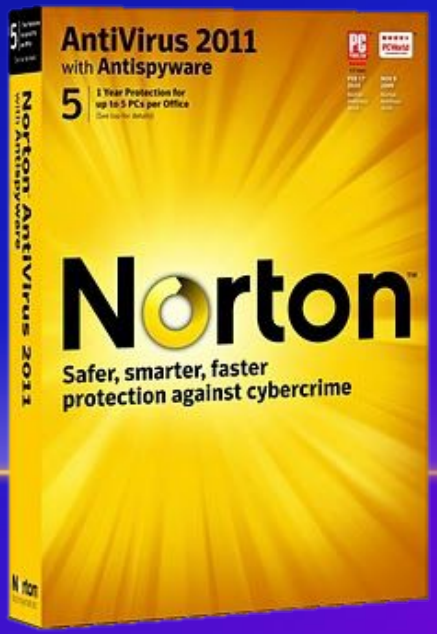

Антивирус
Касперского
2011
KASPERSKY lab
Базовая защита
компьютера
НОВИНКА
ГАДЖЕТ
РАБОЧЕГО
СТОЛА
ПРОДУКТ


avast!
avast! Pro Antivirus


Microsoft® Windows® Vista / XP / 2000
ESET®
NOD32®
Antivirus
v3.0
Business Edition
Integrated components:
ESET NOD32 Antivirus
ESET NOD32 Antispyware
ESET Remote Administrator
eset we protect your digital worlds®


Comodo
AntiVirus
Comodo
© Comodo Group, Inc. 2011. All rights reserv


AVIRA®


AntiVirus 2011
with Antispyware
5
1 Year Protection for
up to 5 PCs per Office
Norton AntiVirus 2011
Norton
Safer, smarter, faster
protection against cybercrime


Dr.WEB®
Антивирус
Dr.WEB®
Антивирус
5.0

УГОЛОВНЫЙ КОДЕКС РФ (УК РФ) ОТ 13.06.1996 N 63-ФЗ

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 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 двадцати до ста восьмидесяти часов, либо исправительными работами на срок 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 ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на срок до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

ЗАКОНОДАТЕЛЬСТВО РФ О ВРЕДОНОСНЫХ ПРОГРАММАХ

Глава 28 «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
Статья 273.

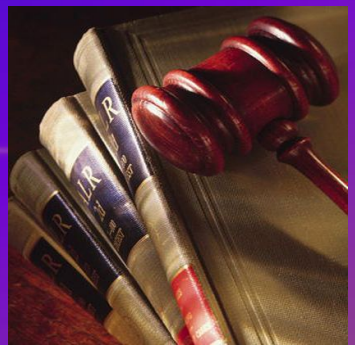
«Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ, или машинных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

То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свобода 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.




w.danature.lact.ru