

*информационная
безопасность*



Мы живем в век взрывного развития информационных технологий. Виртуализация, рост количества социальных сетей привели к «вбросу» большого количества личных данных в online, «облачные вычисления» – все это придало новый импульс развитию сферы информационной безопасности.



Основные цели и задачи информационной безопасности.

- Секретность*
- Целостность*
- Идентификация*
- Аутентификация*
- Уполномочивание*
- Контроль доступа*
- Сертификация*
- Неотказуемость*
- Датирование*
- Аннулирование*
- Свидетельствование*
- Анонимность*

Информационные угрозы и как они проявляются

*Источник угрозы – это
потенциальные
антропогенные,
техногенные или стихийные
носители угрозы
безопасности.*

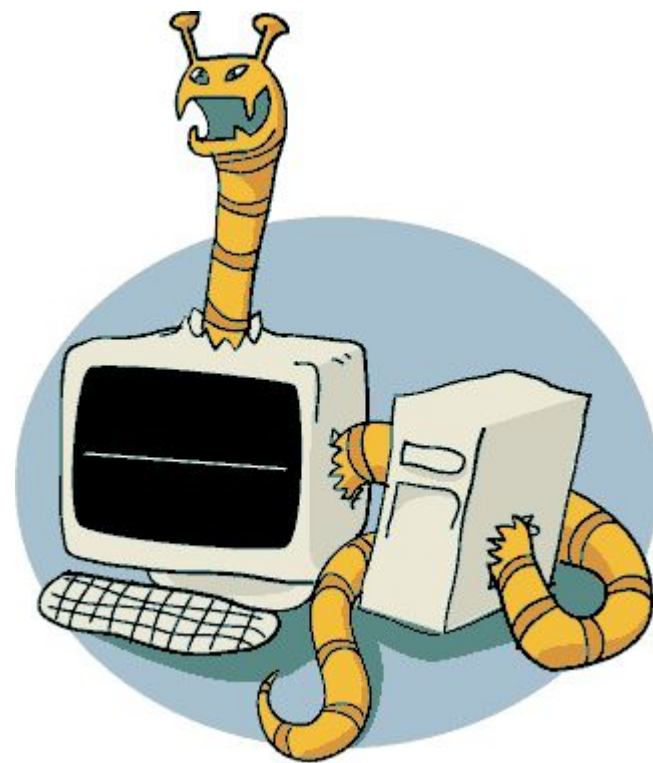


"троян" или троянский конь (troj);

- **- червь (worm);**
- шпион или spy,**
- rootkit;**
- bot или zombie.**



Известные компьютерные черви типа IM-Worm имеют общий способ самораспространения — рассылку на обнаруженные записи контактного листа интернет-пейджера сообщений, содержащих URL на файл, расположенный на каком-либо веб-сервере. Данный прием практически полностью повторяет один из используемых почтовыми червями способов саморассылки.



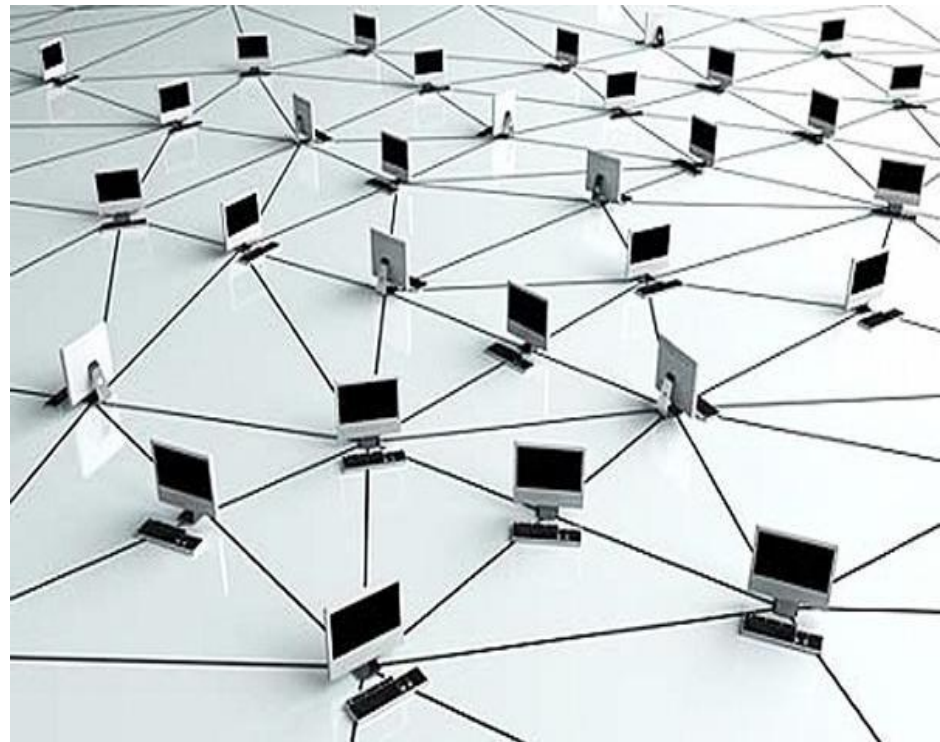
Троян или «троянский конь»

Пример заражения Трояном - вам приходит письмо от некой «знакомой» с текстом: - «Привет! Я только вернулась с моря - так клева отдохнула! Вот мои фотки - посмотри.», и вложенными файлами с расширением «.JPG». Вот эти самые файлы это и есть троянский конь в недрах которого спрятан вредоносный код. Наиболее часто встречающиеся источники заражения - электронная почта, сайты знакомств, сайты с музыкой, сайты с бесплатными ПО. Что делает «Троян»? Как правило, его задача открыть путь для остальных вирусов, выступить первым плацдармом.



bot или zombie.

Она позволяет злоумышленникам удаленно и скрытно управлять зараженными машинами. Причем управлять можно каждым зараженным ПК в отдельности, их группой и всей сетью целиком. Понятно, что пользователь зараженного компьютера («бота») и не догадывается, что его ПК используется киберпреступниками. По этой причине зараженные компьютеры еще называются «зомби», а сеть, в которую они входят, – зомби-сетью.



Шпион или spy

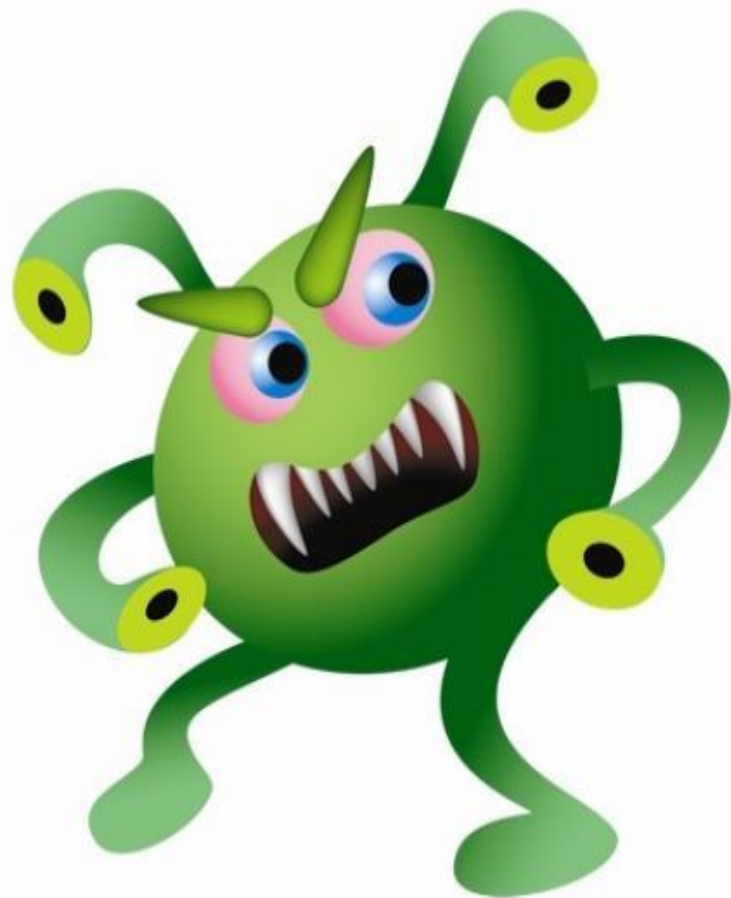
Эти программы предназначены для шпионажа за пользователем. Это в первую очередь клавиатурные шпионы, всевозможные системы слежения за активностью пользователя. Интересной особенностью многих программ данной категории является то, что они зачастую вполне легально распространяются и продаются, снабжены подробной документацией и инсталлятором. Однако решаемые ими задачи (скрытый сбор информации, скрытая отправка собранной информации в соответствии с настройками не оставляет сомнений в вредоносности данных программ).



rootkick

Итак, руткит (rootkit) – это программа (набор программ) для скрывания следов присутствия злоумышленника или вредоносного кода в операционной системе.

Установив руткит на ваш компьютер, хакер получает над ним полный контроль, может удаленно управлять компьютером и загружать на него другие вредоносные программы.



Методы защиты информации от информационных угроз.

Для защиты компьютера от заражения вирусами и другими видами зловредов, конечно, необходимо установить антивирусное программное обеспечение.



AVG

KASPERSKY

NOD 32
antivirus system



AVIRA AntiVir®

McAfee®
SECURITY



avast! antivirus

ZONE
LABS

bitdefender
secure your every bit



symante

Антивирусная программа - это компьютерная программа, целью которой является обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы. Многие антивирусные программы позволяют не только обнаруживать, но и препятствуют несанкционированному проникновению вредоносных программ в компьютер.



Топ-5 самых надёжных антивирусных программ

Во время тестов антивирусы сравнивались по 5 показателям:

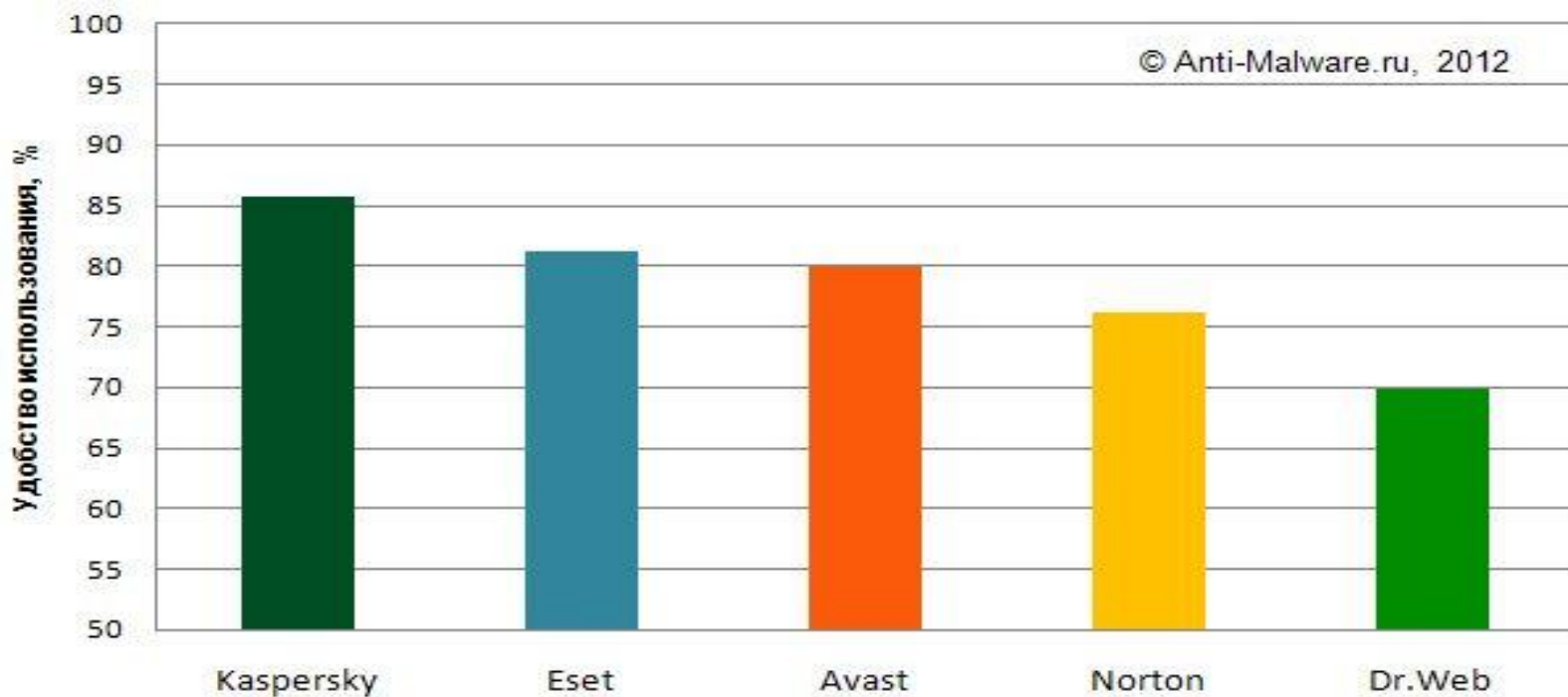
скорость выполнения отдельных операций;

скорость обучения пользователей;

количество ошибок;

визуальная привлекательность интерфейса;

субъективная удовлетворенность пользователей



Из рассмотренного становится очевидно, что обеспечение информационной безопасности является комплексной задачей. Это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал.



Для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

