Основы защиты информации

РЕПОЗИТОРИЙ ГГУ ИМЕНИ ФРАНЦИСКА СКОРИНЫ

Информация

- Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

Законы, регулирующие работу с информацией

- Конституция РБ
- Гражданский кодекс РБ
- Уголовный кодекс РБ
  - Статья 349. Несанкционированный доступ к компьютерной информации
  - Статья 354. Разработка, использование либо распространение вредоносных
  - Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

Законы, регулирующие работу с информацией

- «О средствах массовой информации»
- «О связи»
- «Об авторском праве и смежных правах»
- «О правовой охране программ для электронных вычислительных машин и баз данных»

Угрозы компьютеру и информации, хранящейся на нем

- Несанкционированный доступ
- Вирусные атаки
- Неисправность оборудования
- Чрезвычайные ситуации

Ваш компьютер, что он может рассказать о вас

- Набор программ, которые вы используете во время работы, и интенсивность обращения к этим приложениям.
- Предыстория открытия документов за последнее время.
- Нелегально приобретенное программное обеспечение.
- Электронная корреспонденция

Ваш компьютер, что он может рассказать о вас

- Вся история путешествий по Интернету.
- Файлы документов, с которыми вы работаете в настоящий момент.
- Точные сведения о дате и времени подготовки конкретных документов.
- Целые документы и их фрагменты, которые вы удалили.
- Пароли доступа к ресурсам Интернета.
- Номера кредитных карточек, используемых для онлайновых покупок.

Защита «личного» компьютера вне сети

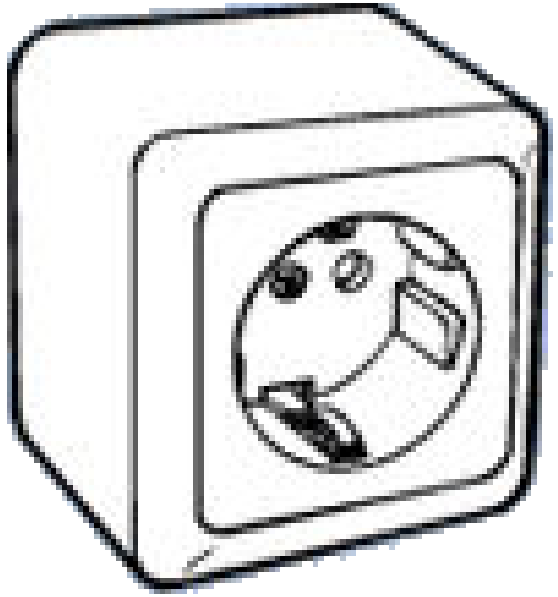
- Надежное электропитание компьютера
  - Нестабильность напряжения
  - Поломки оборудования
  - Высокочастотные помехи
  - Стихийные бедствия
- Создать личный архив с важными данными на независимом носителе информации
- Антивирусная защита

Защита «общего» компьютера вне сети

- Ограничить физический доступ к компьютеру – не устанавливать компьютер в местах, посещаемых случайными людьми
- Парольная защита входа в компьютер

Надежное электропитание

- Защита:
  - Сетевые фильтры
  - Блоки бесперебойного питания (UPS – Uninterruptible Power System)
  - Надежное заземление

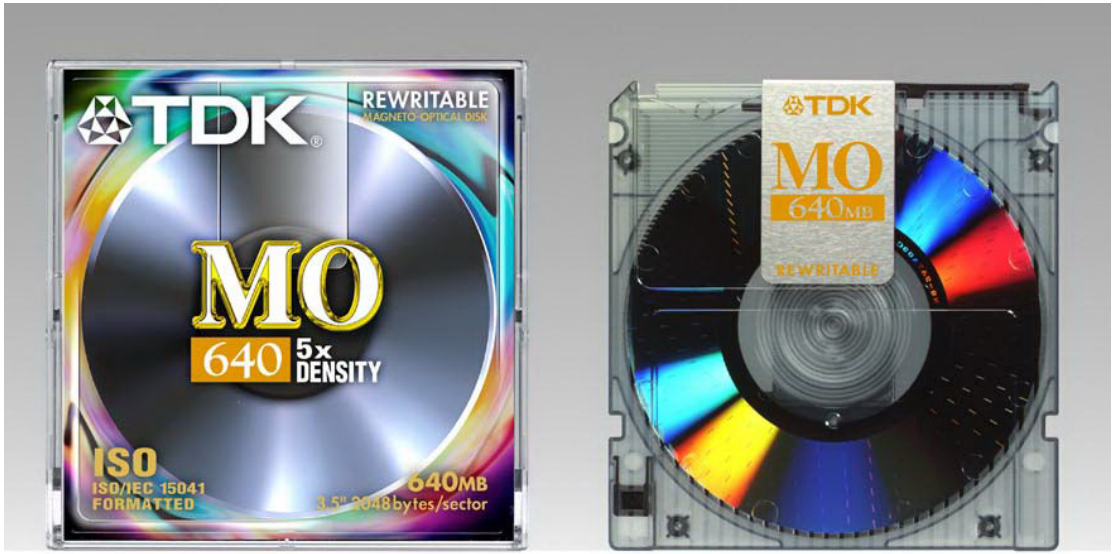


Резервное копирование информации

- Резервное копирование и архивация данных позволяет восстанавливать потерянную информацию и работоспособность системы.
- Все важные документы СРАЗУ сохраняются на несколько носителей (жесткий диск, дискета, CD-RW или Flash-память)
- При переносе важной информации должно быть НЕСКОЛЬКО КОПИЙ.

Надежность носителей при хранении данных

- Магнитооптический диск
- Жесткий диск
- Flash-память
- CD-R, CD-RW
- Гибкий диск



Защита документов Word

- При работе с одним документом в группе используется разноуровневая защита:
  Сервис → Установить защиту
- При работе на компьютере, к которому имеют доступ разные люди, используется защита документа паролем:
  Сервис → Параметры → Безопасность

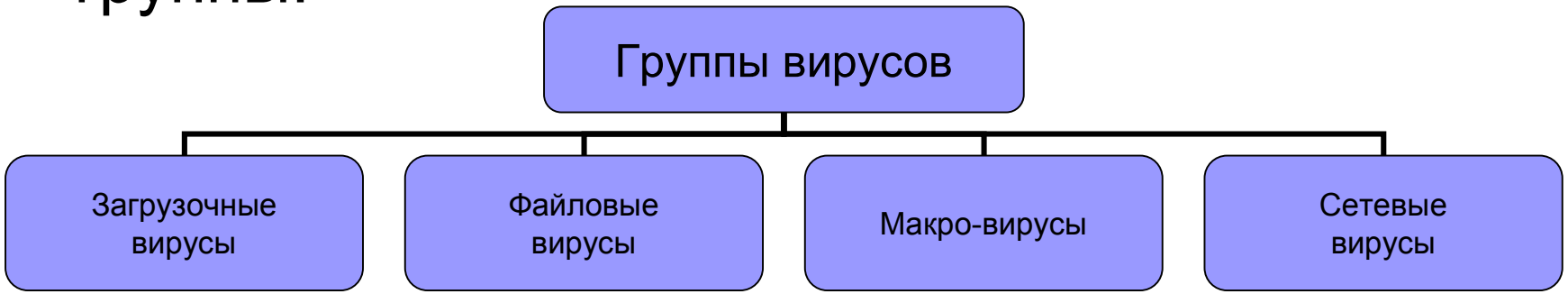
Компьютерные вирусы

- Компьютерный вирус – программа, способная к созданию собственных копий с записью их в оперативную память компьютера, на магнитные носители и / или рассылке по сети.

  Для вируса главное попасть в среду обитания, то есть в операционную систему, не защищенную от функционирования вирусной программы.

Типы компьютерных вирусов

- По объектам атаки и распространения вирусы можно разделить на следующие группы:



Загрузочный вирус

Поражает загрузочный сектор жесткого диска и передается с компьютера на компьютер через зараженную дискету, если ее забыли вынуть из дисковода незараженного компьютера и перезагрузили этот компьютер.

Файловый вирус

Поражает исполняемые файлы, к которым относятся файлы с расширениями .exe и .com, размножается и чаще всего выполняет разрушительные действия.

Макро-вирусы

Заражают файлы документов Word и электронных таблиц Excel.

После загрузки зараженного документа в приложение макро-вирусы присутствуют в памяти компьютера и могут заражать другие документы. Угроза заражения прекращается после закрытия приложения.

Сетевые вирусы

Распространяются по компьютерной сети и заражают при получении файлов с серверов файловых архивов.

Существуют специфичные сетевые вирусы, которые используют для своего распространения электронную почту и Всемирную паутину. «Почтовый» вирус содержится во вложенных в почтовое сообщение файлах.

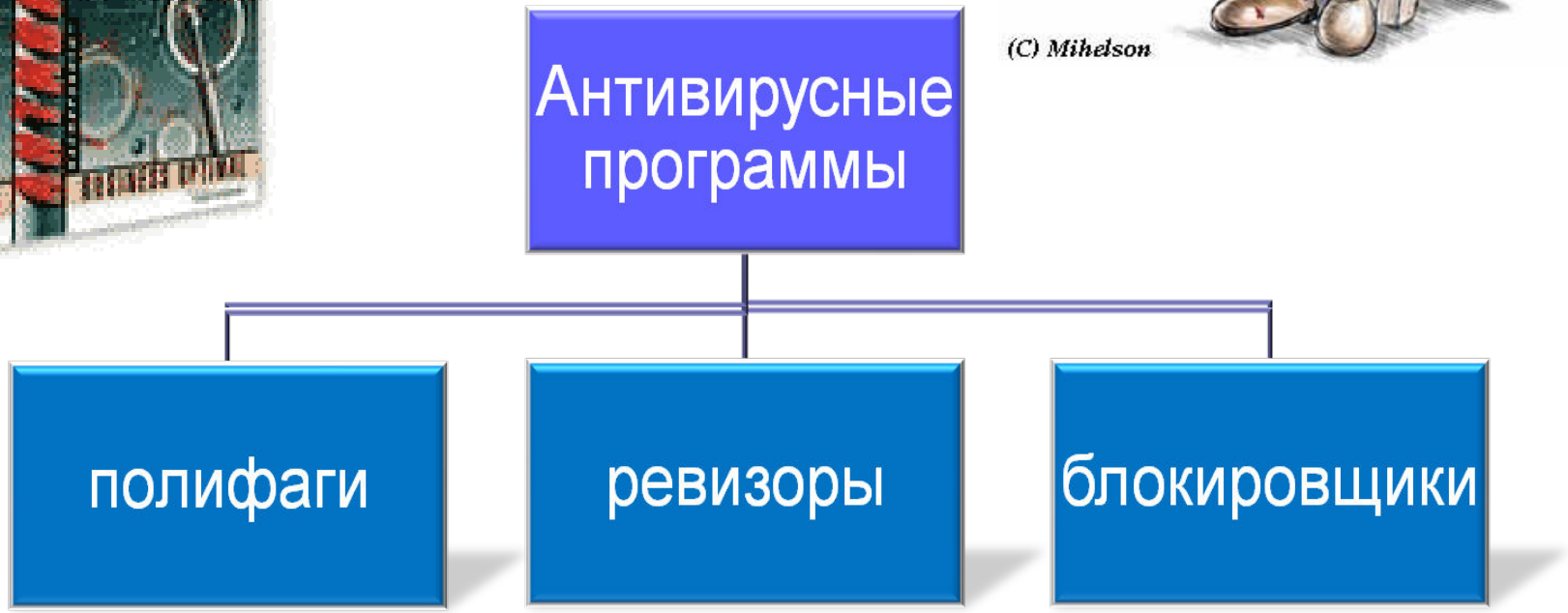
Заражение компьютера происходит после открытия вложенного файла.

Виды вирусов

- Троянский конь (Троян) – программа, маскирующаяся под полезную программу, используется для получения конфиденциальной информации и отсылки ее хозяину (создателю) или для деструктивных действий
- Червь (Worm) – вирус, путешествующий по сети и производящий деструктивное действие на компьютер
- Логическая бомба – вирус, имеющий таймер, срабатывающий в заданную дату и время.
- Полиморфный вирус – вирус, меняющий свой внешний вид при каждом новом инфицировании.

Признаки инфицирования

- Появление необычных системных сообщений
- Исчезновение файлов или увеличение их размеров
- Замедление работы системы
- Внезапный недостаток дискового пространства
- Недоступность диска
- Прекращение работы системы



Полифаги

Принцип работы основан на проверке файлов, секторов дисков, оперативной памяти и поиске в них известных и новых вирусов.

Полифаги могут обеспечить проверку файлов в процессе их загрузки в оперативную память.

Достоинства полифагов : универсальность.

Недостатки: небольшая скорость поиска вирусов.

Ревизоры

Принцип работы основан на подсчете контрольных сумм для всех файлов на диске, которые сохраняются в базе данных антивируса.

При последующем запуске ревизоры сверяют информацию записанную в базе данных с реальным значением, и если оно не совпадает то ревизоры сигнализируют о том, что файл был изменен иди заражен.

Недостаток: ревизор не может обнаружить вирус в новых файлах.

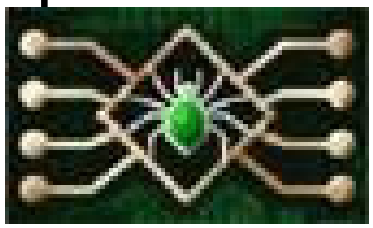
Блокировщики

Это программы перехватывающие «вирусоопасные» ситуации.

Достоинства: способность обнаруживать и останавливать вирус на самой ранней стадии его размножения.

Антивирусные программы

- AVP (лаборатория Касперского) - http://www.kaspersky.ru/ http://www.viruslist.com/
- Dr. Web (Dr. Web Spider) (Санкт-Петербургская антивирусная лаборатория И.Данилова) http://drweb.ru/



- Norton Antivirus (компания Symantec) http://www.norton.com/

Антивирусная защита – советы

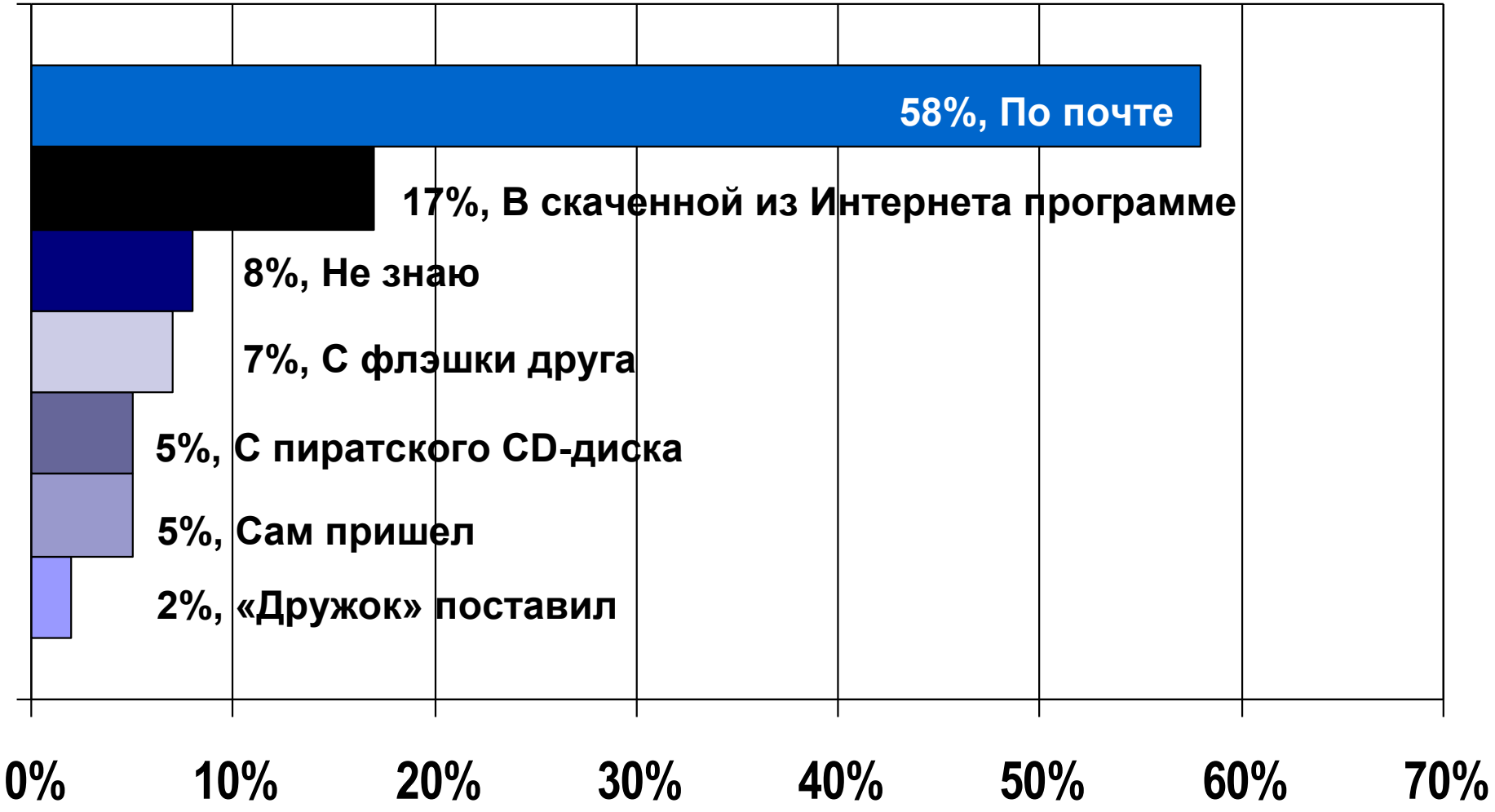
- Приобретенные диски перед использованием проверяйте на наличие вирусов
- Сразу после установки ОС установите антивирусную программу
- Установите расписание полных проверок (не реже одного раза в неделю)
- Настройте программу антивирусного сканирования на режим непрерывной проверки компьютера

Антивирусная защита – советы

- Делайте резервное копирование данных только после антивирусной проверки
- Не забывайте периодически обновлять антивирусные программы и вирусные базы данных
- Следите за поведением системы

Результаты опроса:

Как последний раз к Вам попал вирус?



Угрозы исходящие от Сети

- Угроза взлома конфиденциальной информации:
  - Кража паролей
  - Кража секретной информации
  - Кража банковских счетов
- Нарушение работы системы
- Вирусные атаки

Угрозы электронной почте

- Вирусные атаки
- Рассылка спама
- Взлом почтового ящика для доступа к письмам
- Перехват паролей, что позволяет пользоваться чужим почтовым ящиком

Защита электронной почты - советы

- Не открывайте письма, пришедшие от неизвестных абонентов и имеющие вложения
- Используйте почтовые ящики на бесплатных почтовых серверах, там автоматически идет проверка на вирусы
- Настройте антивирусную программу на проверку входящей почты
- Регулярно меняйте пароли захода в почтовый ящик

Угрозы от World Wide Web

- Фальсификация Web-сайтов
- Переназначение модемного соединения с местного провайдера на спутниковую телефонную сеть
- Запуск программ на локальном компьютере
- Открытие доступа к ресурсам файловой системы локального компьютера
- Раскрытие конфиденциальности Web-путешествий
- Нарушение работы системы

Защита при работе с WWW - советы

- Используйте повышенные уровни безопасности
- Отключите выполнение встроенных в страницы сайтов программ

Кто такие хакеры?

- to hack (англ.) – применительно к компьютерам может иметь два противоположных значения: взломать систему и починить ее.
- Слово «хакер» совмещает в себе по крайней мере два значения: одно окрашенное негативно («взломщик»), другое – нейтрально или даже хвалебное («ас», «мастер»)

Кто такие крэкеры?

- to crack (англ.) – вор-взломщик
- Крэкеры – взломщики систем компьютерной безопасности.