Защита компъюторной информации

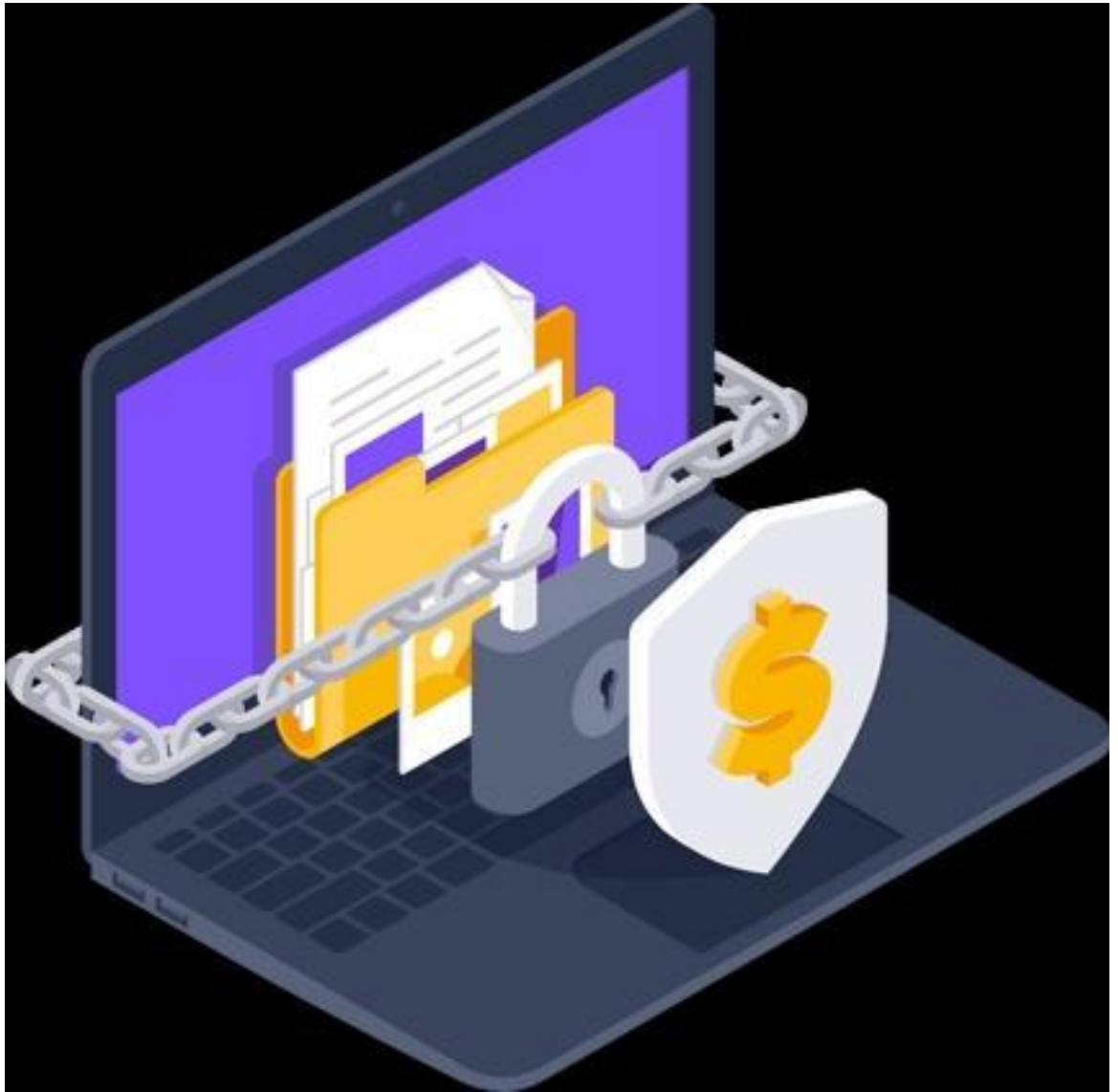
Презентация по информатике

Ученики первого курса 27 группы

Саксман Альбины

- **Защита информации - это комплекс мер по ограничению доступа к информации и программам пользователей, по обеспечению ее подлинности, целостности в процессе передачи (обмена) и хранения.**

Защита информации от несанкционированного доступа



Несанкционированный доступ к информации

- – доступ, нарушающий установленные правила разграничения доступа. Субъект, осуществляющий несанкционированный доступ, является нарушителем доступа.

Защита с использованием паролей

- Средствами программы BIOS Setup
- При загрузке операционной системы
- Защита любого диска, папки или файла на компьютере.

Биометрические системы защиты

- Идентификация по отпечаткам пальцев.
- Идентификация по характеристикам речи
- Идентификация по радужной оболочке г
- Идентификация по изображению лица.
- Идентификация ладони руки.

Физическая защита данных на дисках

- RAID-массивы - несколько жестких дисков подключаемых к RAID-контроллеру, который рассматривает их как единый логический носитель информации. Используются для обеспечения большей скорости чтения/записи и надежнос на жестких дисках
- Два способа реализации RAID-масс
- Аппаратный
- программный

Два способа реализации RAID-массива:

- Аппаратный (состоит из нескольких жестких дисков, управляемых при помощи специальной платы контроллера RAID-массива) Программный (реализуется при помощи специальн массивов:
- RAID 0.
- RAID 1.

Защита информации от вредоносных программ

Вредоносные программы

- Вредоносные программы – это программы, наносящие вред данным и программам, хранящимся на компьютере, к ним относятся: Вирусы, черви, троянские и хакерские программы. Шпионское, рекламное программное обеспечение. Потенциально опасное программное обеспечение.

Компьютерные вирусы

- Компьютерные вирусы – это вредоносные программы, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

Классификация вирусов

- По «среде обитания» вирусы можно разделить на:
- Загрузочные (заражают загрузочный сектор гибкого или жесткого диска)
- Файловые (внедряются в исполнимые файлы и обычно активизируются при их запуске)
- Макровирусы (существуют для интегрированного офисного приложения Microsoft Office)

Защита от вредоносных программ

- Антивирусные программы – это программы, использующиеся для защиты от вредоносных программ.
- Большинство антивирусных программ сочетает в себе функции:
- постоянной защиты (антивирусный монитор) защиты по требованию пользователя (антивирусный сканер)

Сетевые черви

- Сетевые черви – это вредоносные программы, распространяющие свои копии по локальным и/или глобальным сетям.

- Сетевые черви кроме вредоносных действий могут выполнять шпионскую функцию троянских программ, т. е. похищать персональных данных пользователя, а также вызывать уничтожение программ и данных

Классификация сетевых червей

- Web-черви (используют для своего распространения Web-серверы).
- Разновидностью Web-червей являются скрипты Скрипты (заражение происходит при их передаче по Всемирной паутине с серверов Интернета в браузер локального компьютера).
- Почтовые черви (для своего распространения используют электронную почту).

Троянские программы

- Троянская программа (троянец) — вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удаленному пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

Классификация троянских программ

- Троянские утилиты удаленного администрирования (утилиты для скрытого удаленного управления системой компьютера).
- Троянские программы — шпионы (осуществляют электронный шпионаж за пользователем зараженного компьютера)
- Рекламные программы (могут скрыто собирать различную информацию о пользователе компьютера и затем отправлять ее злоумышленнику)

Хакерские утилиты

- Утилиты для сетевых атак (на удаленные серверы посылаются многочисленные запросы, приводящие к отказу в обслуживании/зависанию сервера)
- Утилиты взлома удаленных компьютеров (предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими или для внедрения во взломанную систему других вредоносных программ).
- Руткиты (набор программ для скрытого взятия под контроль взломанной системы)

Защита от вредоносных программ

- Профилактическая защита от загрузочных вирусов состоит в отказе от загрузки ОС с гибких дисков и установке в BIOS вашего компьютера защиты загрузочного сектора от изменений.
- Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы, полученные из сомнительных источников и предварительно не проверенные антивирусными программами.
- Профилактическая защита от макровирусов состоит в том, что при запуске документа сообщается о присутствии в нем макросов (потенциальных вирусов) и предлагается запретить их загрузку.

Защита от сетевых червей

- Профилактическая защита от Web-червей и скриптов состоит в том, что в браузере можно запретить получение скриптов на локальный компьютер, либо использовать антивирусные программы, которые включают межсетевой экран и модуль проверки скриптов.
- Профилактическая защита от почтовых червей состоит в том, что не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников, а также переходить по сомнительным ссылкам (+ использовать антивирусные программы)

Защита от троянских программ и хакерских утилит

- **Профилактическая защита от троянских программ и хакерских утилит состоит** в
- использовании антивирусных программ
- в своевременной загрузке из сети Интернет обновленных баз
- обновлении системы безопасности операционной системы и приложений.
- в борьбе с руткитами эффективен межсетевой экран.

СПОСИБОООО ЗА ВНИМАНИЕ