# Информационная безопастность

Выполнил студент 169-20 АТТ Капитоненко.Г.Д

# План презентации :

- Защита информации
- КОМПЬЮТЕРНЫЕ ВИРУСЫ
- АНТИВИРУСНЫЕ ПРОГРАММЫ
- Список литературы

# Защита информации

- - деятельность, направленная на сохранение государственной, служебной, коммерческой или личной тайн, а также на сохранение носителей информации любого содержания.
- Защита обеспечивается соблюдением режима секретности, применением охранных систем сигнализации и наблюдения, использованием шифров и паролей.
- Информационная безопасность – это совокупность мер по защите информационной среды общества и человека.
- Безопасность

Конфиденциальность

Доступность

Целостность

# Цели информационной безопасности

- Защита национальных интересов;
- Обеспечение человека и общества достоверной и полной информацией;
- Правовая защита человека и общества при получении, распространении и использовании информации.

# Средства защиты информации

- 1. Технические средства – реализуются в виде электрических, электромеханических, электронных устройств.
- 2. Программные средства – программы, специально предназначенные для выполнения функций, связанных с защитой информации.
- 3. Организационные средства – организационно-правовые мероприятия, осуществляемые для обеспечения защиты информации.
- 4. Законодательные средства – законодательные акты страны, которыми регламентируются правила использования и обработки информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.
- 5. Морально-этические средства – всевозможные нормы, которые сложились традиционно или складываются по мере распространения вычислительных средств в данной стране или обществе.

# Способы защиты информации

- **Препятствие – физически преграждает злоумышленнику путь к защищаемой информации.**
- **Управление доступом – идентификация пользователей, персонала и ресурсов системы, проверка полномочий, разрешение и создание условий работы в пределах установленного регламента, регистрация обращений к защищаемым ресурсам, реагирование (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий.**
- **Маскировка – способ защиты информации путем ее криптографического шифрования.**
- **Регламентация – заключается в разработке и реализации комплексов мероприятий, создающих такие условия при которых возможности несанкционированного доступа к защищаемой информации сводились бы к минимуму.**
- **Принуждение – пользователи и персонал вынуждены соблюдать правила обработки и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.**

# Основные виды компьютерных преступлений

- Несанкционированный доступ к информации, хранящейся в компьютере.

Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

Разработка и распространение компьютерных вирусов. Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер. Варианты вирусов зависят от целей, преследуемых их создателем.

Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

Подделка компьютерной информации.

Хищение компьютерной информации.

# КОМПЬЮТЕРНЫЕ ВИРУСЫ

- это программы, которые могут «размножаться» и скрытно внедрять свои копии: в файлы, в загрузочные секторы дисков, в документы.

При этом копии могут сохранять способность дальнейшего распространения. Вирус может дописывать себя везде, где он имеет шанс выполниться.

# По величине вредных воздействий

- неопасные, действие которых приводит к:

уменьшению свободной памяти на диске, графическим и звуковым эффектам;

уменьшению свободной памяти на диске,

графическим и звуковым эффектам;

- опасные, действие которых приводит к:

сбоям и зависанию компьютера;

сбоям и зависанию компьютера;

- очень опасные, действие которых приводит к:

потере программ и данных (изменению или удалению файлов и каталогов) форматированию винчестера и т.д.

потере программ и данных (изменению или удалению файлов и каталогов)

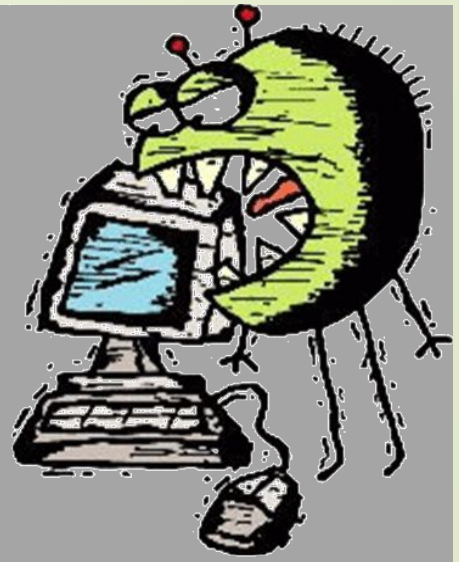
форматированию винчестера и т.д.

# По «среде обитания»

- файловые - внедряются в исполняемые файлы (программы) и активизируются при их запуске (не заражают файлы со звуком и изображением);
- загрузочные - записывают себя в загрузочный сектор диска;
- макровирусы - заражают файлы документов Word и электронных таблиц Excel;
- сетевые – распространяются и заражают компьютеры по сети. Интернет-черви ( передаются в почтовых сообщениях) и скрипт-вирусы (передаются через программы на языках JavaScript, VBScript) .

# Вредоносная программа

- Шпионское, рекламное программное обеспечение
- Вирусы, черви, троянские и хакерские программы
- Потенциально опасное программное обеспечение



# Несанкционированный доступ

- - действия, нарушающие установленный порядок доступа или правила разграничения, доступ к программам и данным, который получают абоненты, которые не прошли регистрацию и не имеют права на ознакомление или работу с этими ресурсами.Для предотвращения несанкционированного доступа осуществляется контроль доступа.
- Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются пароли .
- К биометрическим системам защиты информации относятся системы идентификации:
- по отпечаткам пальцев;
- по характеристикам речи;
- по радужной оболочке глаза;
- по изображению лица;
- по геометрии ладони руки

# АНТИВИРУСНЫЕ ПРОГРАММЫ

- Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.
- Программы-доктора , или фаги, «лечат» зараженные программы или диски, «выкусывая» из зараженных программ тело вируса, т.е. восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.
- Программы-ревизоры сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий об этом сообщается пользователю.
- Доктора-ревизоры – это гибриды ревизоров и докторов, т.е программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.
- Программы-фильтры располагаются резидентно в оперативной памяти компьютера, они перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.
- Программы вакцины , или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает эти программы и диски уже зараженными.

# Антивирусные программы

- обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер:

Интернет,

локальная сеть,

электронная почта,

съемные носители информации.

Принцип работы антивирусных программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.

# Список литература


- Гай Светоний Транквилл. Книга первая // Жизнь двенадцати цезарей = De vita XII caesarvm : [пер. с лат.] / перевод Гаспаров М.. — М. : Издательство «Наука», 1964. — 374 с. — (Литературные памятники).
- Сингх, Саймон. Книга шифров : Тайная история шифров и их расшифровки. — М. : Издательство «АСТ», 2009. — 448 с. — ISBN 5-17-038477-7.
- Измозик, В. С. «Черные кабинеты» : история российской перлюстрации. XVIII — начало XX века. — М. : Новое литературное обозрение, 2015. — ISBN 978-5-4448-0392-9.
- Жельников В. Язык сообщения // Криптография от папируса до компьютера. — М.: ABF, 1996. — 335 с. — ISBN 5-87484-054-0.
- Анин, Б. Ю.. «Марфинская шаражка» // Радиоэлектронный шпионаж. — М. : Центрполиграф, 2000. — 491, [2] с., [8] л. ил., портр. — (Секретная папка). — 10 000 экз. — ISBN 5-227-00659-8.
- Носов В. А. Краткий исторический очерк развития криптографии // Московский университет и развитие криптографии в России, МГУ, 17-18 октября, 2002 : материалы конференции. — 2002. — С. 20—32.
- Токарева Н. Н. Об истории криптографии в России // Прикладная дискретная математика. — 2012. — Декабрь (№ 4 (18)).

# Спасибо за внимание !