Государственное бюджетное профессиональное
образовательное учреждение
«Краевой политехнический колледж»

Информационная безопасность

Преподаватель: М.С. Николаева

Чернушка

Структура занятия

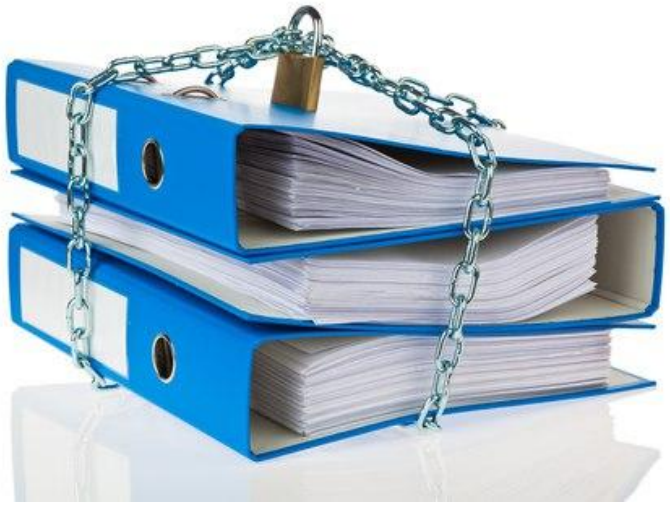
- Основные термины и определения:
  безопасность информации, несанкционированный доступ, средства защиты информации, идентификация, аутентификация, авторизация, компьютерный вирус, антивирусное программное обеспечение
- Классификация угроз информационной безопасности
- Причины несанкционированного доступа к информации
- Средства защиты информации и их краткая характеристика
- Компьютерный вирус: классификация, краткая харатекристика
- Антивирусное ПО: способы защиты, виды, принцип работы

Несанкционированный доступ

Безопасность информации –….

Предмет защиты – ……

Объект защиты – …..



Несанкционированный доступ

Безопасность информации –
защита информации от случайных или преднамеренных угроз, от модификации (изменения) и разрушения,
от невозможности обработки
этой информации

Предмет защиты – информация

Объект защиты – ПК, ПО, пользователь

Конфиденциальная информация – это информация, которая является важной для владельца и доступ к которой ограничен

Классификация угроз

- **Случайные**
  - Отказы и сбои в аппаратной части
  - Помехи в линиях связи от воздействия внешней среды
  - Ошибки человека, как звена системы
- **Преднамеренные**
  - Несанкционированный доступ к ПК
  - Несанкционированный доступ к линиям связи
  - Вредительские программы

Несанкционированный доступ

Несанкционированный доступ - доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения

Последствия

- утечка персональных данных (сотрудников компании и организаций-партнеров)
- утечка коммерческой тайны
- утечка служебной переписки
- утечка государственной тайны
- искажение информации
- полное либо частичное лишение работоспособности системы безопасности компании

Причины доступа

- ошибки конфигурации (прав доступа)
- слабая защищённость средств авторизации (хищение паролей, физический доступ к плохо охраняемому оборудованию, доступ к незаблокированным рабочим местам сотрудников в отсутствие сотрудников)
- ошибки в программном обеспечении
- злоупотребление служебными полномочиями (воровство резервных копий, копирование информации на внешние носители при праве доступа к информации)
- прослушивание каналов связи при использовании незащищённых соединений внутри ЛВС
- использование клавиатурных шпионов, вирусов и троянов на компьютерах сотрудников для персонализации

Средства защиты информации

В зависимости от угрозы и ценности функционирования сети используются разные компоненты системы защиты, а также организуется совместное использование отдельных видов и средств защиты

Средства защиты информации – это совокупность технического, инженерного, электронного, оптического и другого оборудования, которое используются для обеспечения безопасности информации и её защиты от несанкционированного доступа

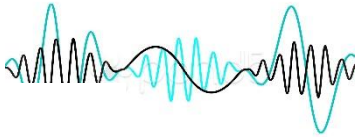
Физические средства защиты информации

Физические – автономно функционирующие устройства для создания различного рода препятствий злоумышленику

- изоляция зданий, оборудование дверей
- электронные замки
- видеонаблюдение
- механические преграды, турнике специальное остекление, сейфы, шкафы
- механические и электромеханические замки, замки с кодовым набором
- датчики различного типа; теле и фотосистемы наблюдения

Аппаратные и программные средства защиты

Аппаратные – устройства, встраиваемые в аппаратуру системы защиты информации (генераторы шума)



Программные – пакеты программ и ПО

- идентификация и аутентификация
- разграничение доступа к документам (совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа, пароли)
- защита электронных документов (ЭЦП – электронная цифровая подпись – реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП)

Программные средства защиты

Прежде чем получить доступ к ресурсам компьютерной системы, user должен пройти процесс первичного взаимодействия с компьютерной системой, который включает 3 основных этапа

Идентификация	Аутентификация	Авторизация
• процедура распознавания пользователя по его идентификатору (id, имени, логину)	• процедура проверки подлинности заявленного пользователя (логин = пароль)	• предоставление определённому лицу или группе лиц прав на выполнение определённых действий

Иные средства защиты информации

Криптографические – преобразование информации в вид, недоступный для чтения или скрытие факта присутствия информации

Организационные средства – организация работы с компьютерной системой и конфиденциальной информацией (разграничение доступа, смена паролей)

Правовые средства – определение прав, обязанностей и ответственности лицам, имеющим право доступа к конфиденциальной информации (Федеральный закон РФ от 27 июля 2006 г. N 149-ФЗ)

Государственное бюджетное профессиональное
образовательное учреждение
«Краевой политехнический колледж»

Компьютерный вирус
Антивирусное ПО

Преподаватель: М.С. Николаева

Чернушка

Компьютерный вирус

Компьютерный вирус – специально написанная, размножающаяся программа, выполняющая нежелательные действия на компьютере

Компьютерный вирус – вид вредоносного ПО, способного внедряться в код других программ, системные области памяти, загрузочные секторы жёсткого диска и распространять свои копии по разнообразным каналам связи

Основная цель - его распространение

Специально написанная программа

Выполняет на ПК нежелательные действия

Обладает способностью к размножению

Классификация по среде обитания

Вид	Заражаемые объекты	Способ заражения
загрузочные	boot-сектор логического диска или MBR винчестера (Master Boot Record - основная загрузочная запись, содержит таблицу разделов для диска и небольшой исполняемый код, называемый основным загрузочным)ё	встраивание своего кода в загрузчик, получают управление при загрузке с зараженного диска
файловые	файловая система ПК, её структуры и объекты (*.EXE, *.COM, *.BAT файлы)	добавление своего кода к программе, получают управление при запуске зараженного объекта
макровирусы	файлы MS Office, а также любого другого приложения, использующего макросы	встраивание своего кода в макросы документа, получают управление при выполнении зараженного макроса
сетевые	оперативная память (RAM, ОЗУ)	проникновение из сети с использованием сетевых протоколов

Классификация по способу заражения

Вид	Краткое описание
резидентные	вирусы, которые при инфицировании компьютера оставляют свою резидентную часть в памяти они могут перехватывать прерывания операционной системы, а также обращения к инфицированным файлам со стороны программ и операционной системы эти вирусы могут оставаться активными вплоть до выключения или перезагрузки компьютера
нерезидентные	вирусы, не оставляющие своих резидентных частей в оперативной памяти компьютера

По деструктивному воздействию

Вид	Краткое описание
безвредные	вирусы никак не влияющие на работу компьютера (исключение: уменьшение свободного места на диске и объёма оперативной памяти)
неопасные	вирусы, которые проявляют себя в выводе различных графических, звуковых эффектов и прочих безвредных действий (появление нежелательной рекламы)
опасные	вирусы, которые могут привести к различным сбоям в работе компьютеров, а также их систем и сетей
очень опасные	вирусы, приводящие к потере, уничтожению информации, потере работоспособности программ и системы в целом

По особенностям алгоритма работы вируса

Вид	Краткое описание
простейшие	не изменяют содержимое файлов, могут быть легко обнаружены и уничтожены
черви	вирусы, которые распространяются в компьютерных сетях, они проникают в память компьютера из компьютерной сети, вычисляют адреса других компьютеров и пересылают на эти адреса свои копии
стелс-вирусы (вирусы-невидимки)	трудно обнаружить и обезвредить, представляют вместо своего тела незаражённые участки диска
мутанты	содержат алгоритмы шифровки/расшифровки, их наиболее трудно обнаружить
логическая бомба	программа которая запускается при определённых временных или информационных условиях для осуществления вредоносных действий
троянская программа	вредоносная программа, распространяемая людьми, в отличие от вирусов и червей, которые распространяются самопроизвольно, троян маскируется под полезное ПО,

Компьютерный вирус

Профилактика компьютерного вируса

Общие средства защиты информации

Контроль поступающих извне данных

Регулярная проверка ПК при помощи антивирусных программ

Антивирусное программное обеспечение

Антивирусное программное обеспечение создано для профилактики, выявления и уничтожения компьютерных вирусов

Действия антивирусного программного обеспечения

- Попытаться «вылечить» зараженный файл, убрав из него вредоносный код
- Отправить инфицированный файл в карантин (актуально для ценных пользователю файлов, находясь в карантине, зараженный файл не сможет навредить ПК; позже его можно вылечить самостоятельно или с помощью специалистов)
- Удалить зараженный файл
- Не выполнять никаких действий (если предполагается, что файл был помечен как «вредоносный» по ошибке, можно добавить этот файл в список исключений антивируса)

Разновидности защит

- **Проактивная защита (эвристика)**

Защита от неизвестных вирусов, методика основана на изучении кода и поведения программ, характерных для вредоносного ПО. Такой тип защиты показывает лучший результат при борьбе с модифицированными вирусами. За основу принимаются данные об уже существующих угрозах. Эвристика в антивирусном контексте - набор правил, которые используются для обнаружения действий вредоносных программ без необходимости определения конкретной угрозы

- **Реактивная защита (вирусная сигнатура)**

Защита от уже известных вирусов, основанная на информации о коде и остальных особенностях вредоносного ПО.
Для максимально эффективной работы такие антивирусы должны постоянно обновлять свои базы данных вирусных сигнатур.
Защита, основанная на вирусных сигнатурах подразумевает обращение к словарю с уже известными вирусами, которые составили разработчики антивирусного ПО

Типы антивирусного программного обеспечения

Вид	Метод работы	Достоинства	Недостатки
сканеры (детекторы, фаги)	после запуска сканируют файловую систему и ОЗУ ПК и нейтрализуют найденные вирусы (эвристический анализ)	✔ универсальность ✔ сбалансированность	✔ время проверки ✔ большие размеры вирусных баз ✔ необходимость постоянного обновления баз
ревизоры	проверяют изменение длины файла	✔ эффективность и скорость проверки	✔ невозможность обнаружения вирусов в момент их появления
блокировщики (фильтры)	перехват потенциально опасных действий программ и выдача сообщения пользователю	✔ обнаружение и остановка вируса на ранней стадии его размножения	✔ возможность обхода защиты ✔ ложные срабатывания
полифаги	проверяют файлы, загрузочные сектора дисков и ОП на поиск новых и вирусов	✔ самые универсальные и эффективные	✔ занимают много места ✔ скорость работы
иммунизаторы	модификация программ таким образом, что конкретный вирус считает их уже	✔ эффективны против конкретного вируса	✔ невозможность вакцинации от неизвестных вирусов ✔ практически