СРЕДСТВА ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ. АНТИВИРУСНЫЕ ПРОГРАММЫ

Цели занятия

- Познакомится с видами угроз и элементами обеспечения компьютерной безопасности.
- Формировать понятие об антивирусных программах и способах защиты ПК.
- Развивать навыки обеспечения безопасности операционных систем.

Информационная безопасность

- — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

- **Компью́терная безопа́сность** — раздел информационной безопасности, включающий меры безопасности, применяемые для защиты вычислительных устройств (компьютеры, смартфоны и другие), а также компьютерных сетей (частных и публичных сетей, включая Интернет).

1. Угрозы


Конфиденциальность
Целостность
Данные
и
средства
обеспечения
Доступность

Безопасность информационных систем разбита на три компонента

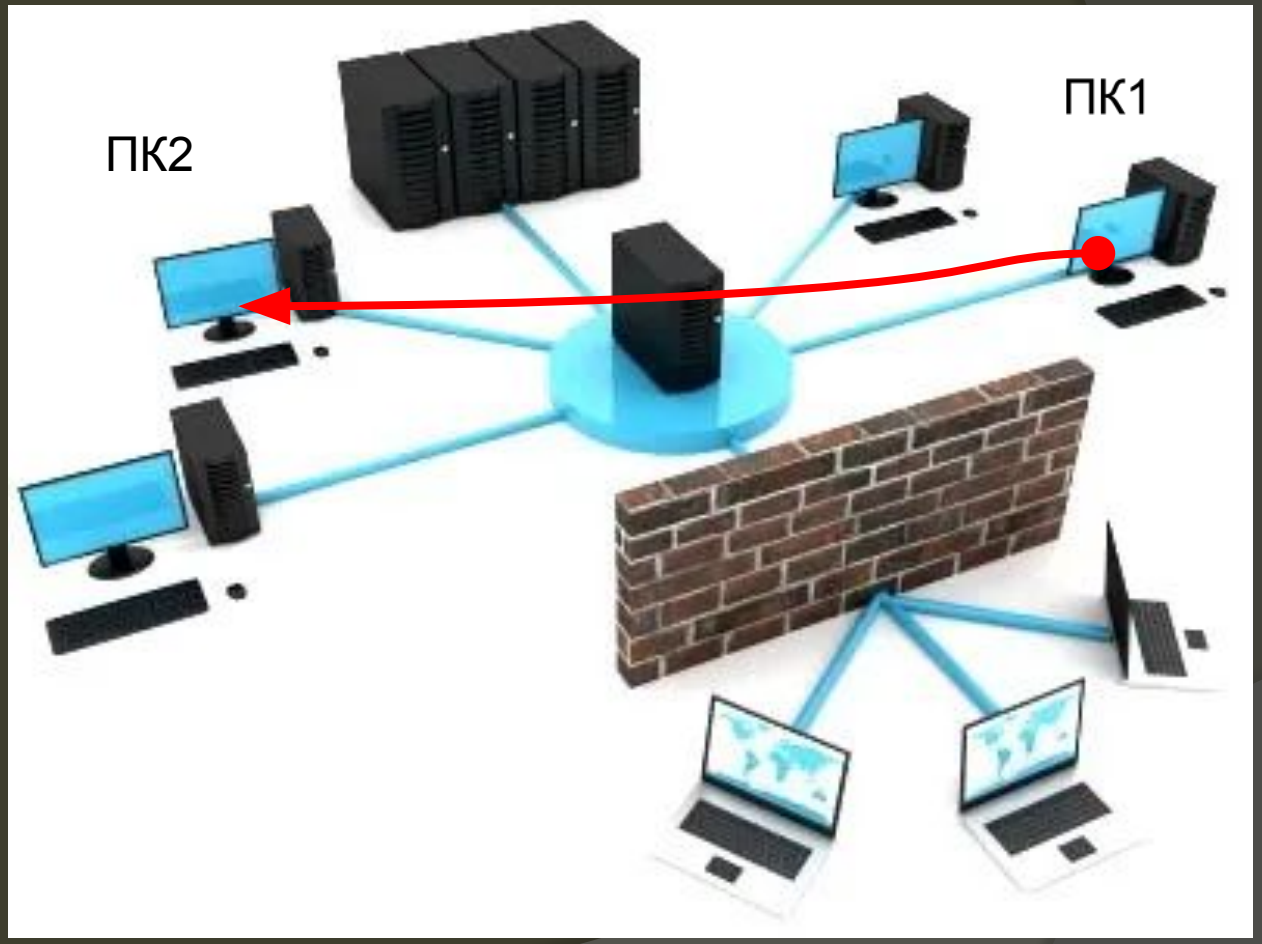
Угрозы	Задачи
Незащищенность данных	**Конфиденциальность** – направлено на сохранение секретности данных.
Подделка данных	**Целостность** – означает, что пользователи, не обладающие необходимыми правами, не должны иметь возможности изменять какие-либо данные без разрешения их владельцев
Отказ от обслуживания	**Доступность** – означает, что никто не может нарушить работу системы и вывести ее из строя.

Угроза «взлома» чужого компьютера

Причина возникновения этой проблемы — *дефекты в программном обеспечении*, установленном на компьютере ПК2.

Когда дефект влияет на безопасность, мы называем его *уязвимостью*.

Вводимые данные, позволяющие воспользоваться дефектом, обычно называются *вредоносным кодом.*



DoS и DDoS - атаки

Атаки, вызывающие отказ от обслуживания (denial of service, (**DoS**)), приобретают все более распространенный характер.

Если атака выполняется одновременно с большого числа компьютеров, говорят о **DDoS-атаке.**

Киберпреступники зачастую пользуются бот-сетями

Ботнет - компьютерная сеть, состоящая из некоторого количества хостов с запущенными **ботами** — автономным программным обеспечением.

Чаще всего *бот* в составе ботнета является *программой*, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера.

Страны с самым большим количеством зараженных компьютеров

По некоторым оценкам, около четверти из 600 млн компьютеров, подключённых к Интернету, могут находиться в ботнетах.

Вредоносные программы вида **ботнет распространяются** с помощью

- вложений электронной почты и
- через загрузку файлов и поддельных программ.

Злоумышленники также нацеливаются на такие уязвимые места, как не обновленное программное обеспечение и отсутствие защиты в сети Интернет

№	Страна	Количество заражённых компьютеров
1	Индия	2 017 847
2	Китай	1 697 954
3	Египет	1 404 250
4	Иран	749 570
5	Вьетнам	686 920
6	Бразилия	580 168
7	Турция	530 796
8	Россия	516 295
9	Таиланд	494 069
10	Мексика	470 213

Взломщики

Попадаются плохие люди, желающие причинить неприятности (возможно, для извлечения собственной коммерческой выгоды), называемые **взломщиками**, **злоумышленниками**, **чёрными хакерами**.

Их мотивацией является: воровство, хактивизм, вандализм, терроризм, кибервойна, шпионаж, рассылка спама, вымогательство, жульничество, а иногда взломщики просто хотят показать плачевное состояние системы безопасности организации.

Взлом программного обеспечения

Один из основных способов взлома пользовательского компьютера основан на использовании уязвимостей в программном обеспечении, запущенных в систему чтобы сделать что-либо отличное от предназначения, заложенного программистом.

- Атака, нацеленная на инфицирование пользовательского браузера путем попутной, скрытой загрузки, с последующим заражением посещённых веб-серверов.
- Атаки, использующие переполнение буфера.
- Указатели на несуществующие объекты
- Атаки, использующие разыменование нулевого указателя
- Атаки, использующие внедрение команд
- Инсайдерские атаки
- Логические бомбы
- Лазейки

Можно ли создать защищенные системы?

1. А нельзя ли создать защищенную компьютерную систему?

- Теоритически можно.

2. Если да, то почему она до сих пор не создана?

- Сегодняшние системы не являются защищенными, но пользователи не собираются от них отказываться.
- Единственный известный способ создать защищенную систему заключается в поддержании ее простоты. Функциональные возможности являются врагом безопасности.

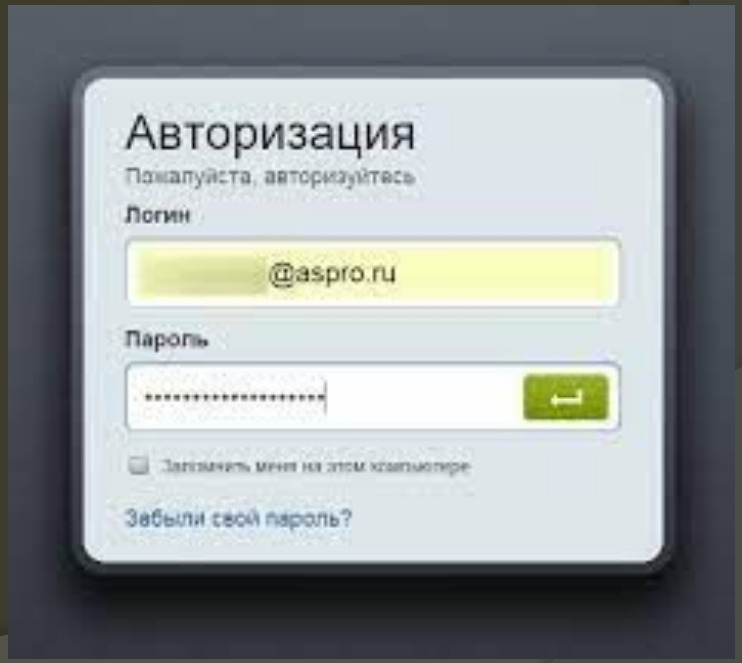
Безопасность информационных систем

Средства защиты ИС

- Средства защиты от несанкционированного доступа
  - Средства авторизации;
  - Управление доступом (мандатное, избирательное, на основе ролей);
  - Журналирование.
- Системы аутентификации:
  - Пароль;
  - Ключ доступа (физический или электронный);
  - Сертификат;
  - Биометрия.
- Антивирусные средства.
- Межсетевые экраны.
- Криптографические средства:
  - Шифрование;
  - Цифровая подпись.
- Системы резервного копирования.
- Средства контроля доступа в помещения.

Авторизáция

— предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.



Аутентификация

— процедура проверки легальности пользователя или данных, например,

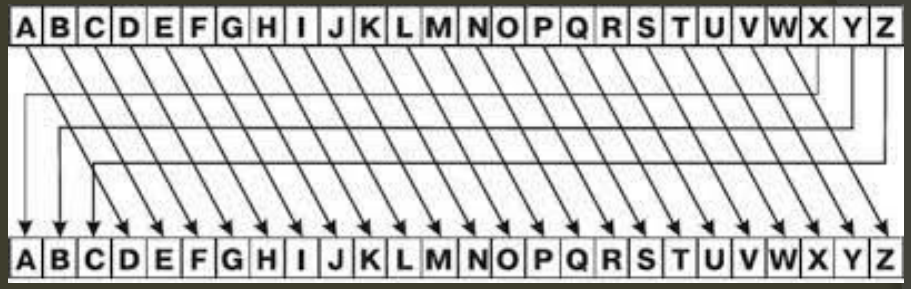
- проверки соответствия введённого пользователем пароля к учётной записи паролю в базе данных,
- проверка цифровой подписи письма по ключу шифрования,
- проверка контрольной суммы файла на соответствие заявленной автором этого файла.

- «Неслабые» пароли
- Одноразовые пароли
- Схема аутентификации «оклик — отзыв»
- Аутентификация с использованием физического объекта (н-р, пластиковая карта)
- Аутентификация с использованием биометрических данных (отпечатки пальцев, тембр голоса, радужная оболочка глаз, личная подпись)

Криптографические средства

- Криптография используется в операционных системах во многих местах.
  - Например, некоторые файловые системы могут зашифровать все данные на диске,
  - такие протоколы, как IPSec, позволяют зашифровать и/или подписать все сетевые пакеты,
  - большинство операционных систем шифруют пароли, чтобы не дать взломщикам возможности их восстановления.
- Замысел криптографии заключается в том, чтобы закодировать *открытый текст* — сообщение или файл, превратив его в *зашифрованный текст*, чтобы о том, как его снова превратить в открытый текст, знали только те, кто имеет на это право.

Шифр Цезаря



- Ключ 3
- Открытый текст

HELLO CEASER CIHER

- Зашифрованной текст

KHOOR FDHVDU FLSKHU

Принцип: *без знания ключа враг не сможет прочитать сообщение*

- Шифрование с секретным ключом
- Шифрование с открытым ключом
- Криптографическая хеш-функция
- Цифровые подписи
- Криптографические процессоры (микросхема)

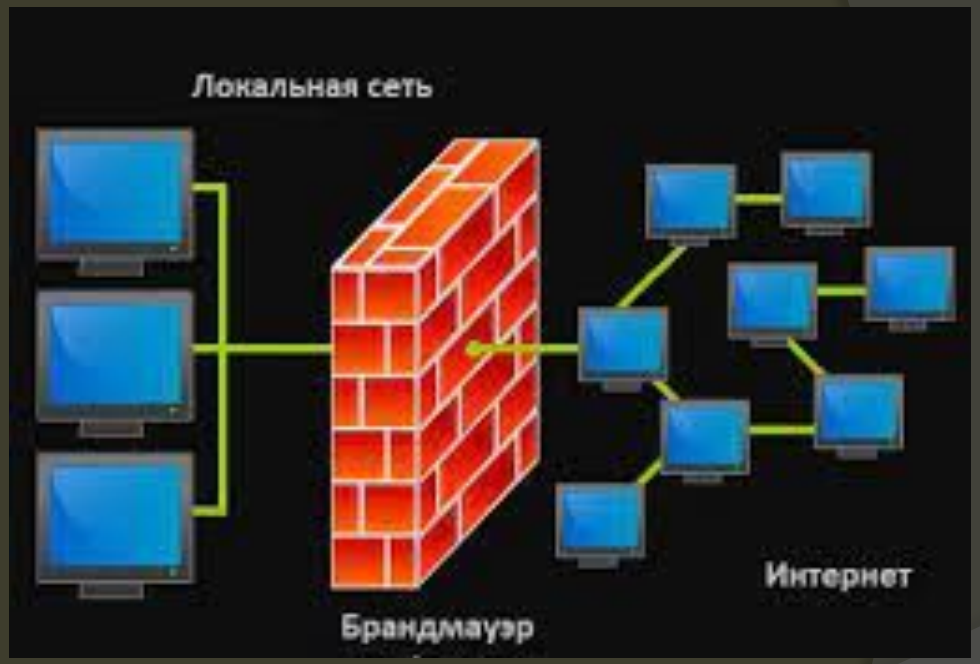
Брандмауэры (межсетевые экраны)

Являются современной адаптацией средневекового вспомогательного защитного средства: выкапывания глубокого рва вокруг своего замка.

Эта конструкция заставляет всех входить или выходить из замка, проходя по единственному подъемному мосту, где они могут быть проверены полицией, следящей за режимом входа-выхода.

Брандмауэры (межсетевые экраны)

- У компании может быть множество локальных сетей, соединенных в произвольном порядке, но весь информационный поток, направленный в компанию или из нее, принудительно направлен через электронный подъемный мост
- Брандмауэр Windows является частью Центра обеспечения безопасности Windows.
- **Межсетевой экран**, **сетевой экран** — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами



Антивирусные средства

Компьютерный вирус -

- это вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и *распространять* свои копии по разнообразным каналам связи.

Принято разделять вирусы:

- по поражаемым объектам *(файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);*
- по механизму заражения: *паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом*.
- по поражаемым операционным системам и платформам (DOS, Windows, Unix, Linux, Android);
- по используемым технологиям (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

Некоторые особенности вредоносных программ

- Вирус – это саморазмножающаяся программа: она распространяется с файла на файл и с компьютера на компьютер. Кроме того, вирус может быть запрограммирован на уничтожение или повреждение данных.
- Черви считаются подклассом вирусов, но обладают характерными особенностями. Червь размножается (воспроизводит себя), не заражая другие файлы. Он внедряется один раз на конкретный компьютер и ищет способы распространиться далее на другие компьютеры.
- Троянец – это программа, которая внешне выглядит как легальный программный продукт, но при запуске совершает вредоносные действия.
- Фишинг – это особый вид кибермошенничества, направленный на то, чтобы обманным путем заставить вас раскрыть персональные данные, как правило финансового характера. Мошенники создают поддельный веб-сайт, чтобы вы ввели на нем конфиденциальные данные, такие как логин, пароль или PIN-код.
- Клавиатурный шпион (кейлоггер) – это программа, отслеживающая нажатия кнопок на клавиатуре.
- Руткит – это набор программ, используемый хакерами для сокрытия своего присутствия в системе при попытках неавторизованного доступа к компьютеру.

Антивирусная программа -

это специализированная программа для

- *обнаружения* компьютерных вирусов, а также нежелательных программ,
- *восстановления* заражённых такими программами файлов
- и *профилактики* — предотвращения заражения файлов или операционной системы.

Три основных уровня антивирусной защиты:

- Поиск и уничтожение известных вирусов
- Поиск и уничтожение неизвестных вирусов
- Блокировка появления вирусов

Уровни и средства антивирусной защиты

1 уровень
Защита от известных вирусов

Используемый метод – сканирование.

Сканеры (или детекторы) - выявляют вирусы по их уникальному фрагменту программного кода (сигнатуре), сравнивая с фрагментами *известных* вирусов, находящихся в базе данных.

Сканеры бывают транзитными (периодически запускаемыми) и резидентными (постоянно находящимися в ОЗУ)

Полифагами называют программы, которые к тому же включают функции восстановления заражённых файлов.

Недостатки сканеров:

- Позволяют обнаружить только уже известные вирусы, для которых определена сигнатура
- Необходимо оперативно пополнять БД вирусов
- Некоторые вирусы видоизменяют свой программный код

2 уровень
Защита от неизвестных вирусов

Метод – контроль целостности системы (обнаружение изменений)

Ревизоры - фиксируют эталонные характеристики вычислительной системы и периодически сравнивают их с текущими характеристиками.

Делятся на транзитные и резидентные.

Вакцинация – это метод программного самоконтроля, состоящий в присоединении к защищаемой программе модуля (вакцины), контролирующего характеристики программы (н-р контрольную сумму).

Эвристические анализаторы используют методы, позволяющие выявить по известным признакам некоторые маскирующиеся или новые модифицированные вирусы известных типов.

Недостатки ревизоров:

- Многие изменения системы вызваны не вирусами, а работой системных программ или действиями пользователя-программиста
- Не всегда обеспечивает корректное лечение заражённых файлов

3 уровень
Защита от проявлений вирусов

Метод основан на перехвате характерных для вируса функций.

Программы-фильтры (резидентные сторожа, мониторы) постоянно находятся в ОП и перехватывают заданные прерывания с целью контроля подозрительных действий (модификация главной загрузочной записи, загрузочных записей дисков, запись по абсолютному адресу, низкоуровневое форматирование диска, оставление в ОП резистентного модуля и др.).

Встроенные аппаратные средства ПК обеспечивают контроль модификации системного загрузчика и таблицы разделов жёсткого диска. Осуществляется при помощи программы, расположенной в ПЗУ.

Наиболее полная защита от вирусов может быть обеспечена с помощью специальных контроллеров аппаратной защиты. Такой контроллер подключается к ISA-шине ПК и на аппаратном уровне контролирует все обращения к дисковой подсистеме компьютера.

Профилактика угроз

В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

- Не работать под привилегированными учётными записями без крайней необходимости (учётная запись администратора в Windows).
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.
- Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

При работе в глобальных сетях общего пользования

- кроме традиционных способов антивирусной защиты данных компьютеров, становится актуальным антивирусный контроль всего проходящего трафика.

- Это может быть осуществлено путем реализации ***антивирусного прокси-сервера***, либо интеграции ***антивирусной компоненты с межсетевым экраном***.

Спасибо за внимание