1.Тема: Безопасная работа на компьютере

Цели занятия:

-Узнать о типах угроз безопасности

-Узнать о разновидности вредоносных программ

-научится соблюдать правила безопасной работы за ПК

-Познакомится с технологиями защиты от угроз

-Научится работать с антивирусным пакетом

План занятия:

-Рассказ о разновидности угроз и вирусов, меры по защите системы и данных

-Работа в антивирусном пакете

Методические материалы:

Компьютерный вирус — вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, и распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов и даже удаление операционной системы, приведение в негодность структур размещения данных, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

Угроза нулевого дня — термин, обозначающий не устранённые уязвимости, а также вредоносные программы, против которых ещё не разработаны защитные механизмы.

Сам термин означает, что у разработчиков было 0 дней на исправление дефекта: уязвимость или атака становится публично известна до момента выпуска производителем ПО исправлений ошибки (то есть потенциально уязвимость может эксплуатироваться на работающих копиях приложения без возможности защититься от неё).

В компьютерной безопасности термин «**уязвимость**» используется для обозначения недостатка в системе, используя который, можно намеренно нарушить её целостность и вызвать неправильную работу. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, вирусов и других вредоносных

программ, скриптовых и SQL-инъекций. Некоторые уязвимости известны только теоретически, другие же активно используются и имеют известные эксплойты.

Обычно уязвимость позволяет атакующему «обмануть» приложение — выполнить непредусмотренные создателем действия или заставить приложение совершить действие, на которое у того не должно быть прав. Это делается путём внедрения каким-либо образом в программу данных или кода в такие места, что программа воспримет их как «свои». Некоторые уязвимости появляются из-за недостаточной проверки данных, вводимых пользователем, и позволяют вставить в интерпретируемый код произвольные команды (SQL-инъекция, XSS, SiXSS). Другие уязвимости появляются из-за более сложных проблем, таких как запись данных в буфер без проверки его границ (переполнение буфера). Поиск уязвимостей иногда называют *зондированием*, например, когда говорят о зондировании удалённого компьютера — подразумевают, поиск открытых сетевых портов и наличии уязвимостей, связанных с приложениями, использующими эти порты.

Черви — Worm

Червь - программа, которая делает копии самой себя. Ее вред заключается в захламлении компьютера, из-за чего он начинает работать медленнее. Отличительной особенностью червя является то, что он не может стать частью другой безвредной программы.

Вирусы-маскировщики — Rootkit

Эти вирусы используются для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Rootkit'ы также могут модифицировать операционную систему на компьютере и заменять основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Вирусы – шпионы — Spyware

Шпионы собирают информацию о действиях и поведении пользователя. В основном их интересует информация — адреса, пароли, данные кредитных карт).

Зомби — Zombie

Зомби позволяют злоумышленнику управлять компьютером пользователя. Компьютеры – зомби могут быть объединены в сеть —бот-нет) и использоваться для массовой атаки на сайты или рассылки спама. Пользователь может даже не догадываться, что его компьютер зомбирован и используется злоумышленником.

Рекламные вирусы — Adware

Программы-рекламы, без ведома пользователей встраиваются в различное программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе.

Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе.

Вирусы – блокировщики — Winlock

Такие программы блокирует пользователю доступ к операционной системе. При загрузке компьютера появляется окно, в котором пользователя обвиняют в скачивании нелицензионного контента или нарушении авторских прав. И под угрозой полного удаления всех данных с компьютера требуют отослать смс на номер телефона или пополнить его счет. Естественно, после перевода денег на счет злоумышленника, баннер никуда не пропадает.

Троянские вирусы — Trojan

Троянская программа является самым опасным типом вирусов, так как она маскируется в других безвредных программах. И до того момента как пользователь не запустит эту самую безвредную программу, троян не несет никакой опасности и обнаружить его нелегко. Троянская программа может нанести различный ущерб для компьютера. В основном трояны используются для кражи, изменения или удаления личных данных пользователя. Отличительной особенностью вируса-трояна является то, что он не может самостоятельно размножаться.

Современные антивирусные программы обладают необходимым функционалом для обнаружения и обезвреживания различных вирусных программ и обеспечивают надежную защиту компьютеру пользователя.

Контроль знаний:

-Презентация на тему – «Самые опасные компьютерные вирусы 90х-2000х».

-Онлайн-урок. Опрос учеников, проверка тетрадей.

Дополнительные материалы:

https://www.youtube.com/watch?v=QL37JlK10X8 – компьютерные вирусы (Павел Мудрый)

2. Тема: Сервисное обслуживание ПК и сети. Резервное копирование. Защита данных

Цели занятия:

-Научится предоставлять общий доступ к файлам и папкам.

-Научится подключать ресурсы в виде сетевых дисков

-Познакомится с принципами резервного копирования

План занятия:

-Рассказ о сетевых ресурсах

-Создание общих папках и предоставление к ним доступа

-Создание точки восстановления

-Создание резервной копии системы и диска

Методические материалы:

Общий ресурс, или **общий сетевой ресурс**, — в информатике, это устройство или часть информации, к которой может быть осуществлён удалённый доступ с другого компьютера, обычно через локальную компьютерную сеть или посредством корпоративного интернета, как если бы ресурс находился на локальной машине.

Резервное копирование — процесс создания копии данных на носителе (жёстком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Полное резервное копирование

Полное копирование обычно затрагивает всю систему и все файлы. Еженедельное, ежемесячное и ежеквартальное резервное копирование подразумевает создание полной копии всех данных. Обычно оно выполняется тогда, когда копирование большого объёма данных не влияет на работу организации. Для предотвращения большого объёма использованных ресурсов используют алгоритмы сжатия, а также сочетание этого вида с другими: дифференциальным или инкрементным. Полное резервное копирование незаменимо в случае, когда нужно подготовить резервную копию для быстрого восстановления системы с нуля.

Дифференциальное резервное копирование

При дифференциальном («разностном») резервном копировании каждый файл, который был изменён с момента последнего полного резервного копирования, копируется каждый раз заново. Дифференциальное копирование ускоряет процесс восстановления. Все копии файлов делаются в определённые моменты времени, что, например, важно при заражении вирусами.

Инкрементное резервное копирование

При добавочном («инкрементном») резервном копировании происходит копирование только тех файлов, которые были изменены с тех пор, как в последний раз выполнялось полное или добавочное резервное копирование. Последующее инкрементное резервное копирование добавляет только файлы, которые были изменены с момента предыдущего. Инкрементное резервное копирование занимает меньше времени, так как копируется меньшее количество файлов. Однако процесс восстановления данных занимает больше времени, так как должны быть

восстановлены данные последнего полного резервного копирования, а также данные всех последующих инкрементных резервных копирований. В отличие от дифференциального копирования, изменившиеся или новые файлы не замещают старые, а добавляются на носитель независимо.

Клонирование

Клонирование позволяет скопировать целый раздел или носитель (устройство) со всеми файлами и каталогами в другой раздел или на другой носитель. Если раздел является загрузочным, то клонированный раздел тоже будет загрузочным

Резервное копирование в виде образа

Образ — точная копия всего раздела или носителя (устройства), хранящаяся в одном файле

Резервное копирование в режиме реального времени

Резервное копирование в режиме реального времени позволяет создавать копии файлов, каталогов и томов, не прерывая работу, без перезагрузки компьютера

Холодное резервирование

При холодном резервировании база данных выключена или закрыта для потребителей. Файлы данных не изменяются, и копия базы данных находится в согласованном состоянии при последующем включении.

Горячее резервирование

При горячем резервировании база данных включена и открыта для потребителей. Копия базы данных приводится в согласованное состояние путём автоматического приложения к ней журналов резервирования по окончании копирования файлов данных

Точка восстановления — это представление сохраненного состояния системных файлов компьютера. Точку восстановления можно использовать для восстановления системных файлов компьютера в состояние, соответствующее моменту времени в прошлом.

Контроль знаний:

-Доклад на 2-3 страницы по одной из тем:

- RAID-массивы и ZFS в помощь хранения резервной информации
- Ленточные магнитные носители (DDS, DAT)

-онлайн-урок. Опрос учеников, проверка тетрадей.

Дополнительные материалы:

https://www.youtube.com/watch?v=9DfDlz0PcD4 – Магнитная лента и DDS (Максим Крюков)

https://www.youtube.com/watch?v=EiKafkUcajs – ZFS и файловый сервер (Дмитрий Бачило)