План урока

Тема: Обеспечение безопасности пользовательских компьютеров

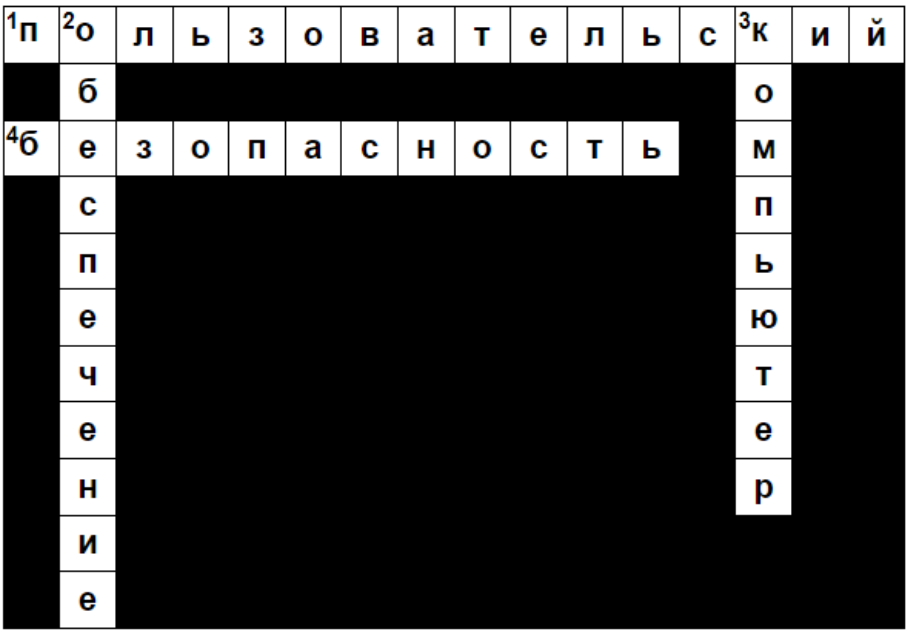
1. Организационный момент (1 мин.)

Приветствие, проверка присутствующих. Настрой учащихся на работу

2. Актуализация знаний (6 мин.)

«Для того, чтобы начать изучать что-то новое, необходимо вспомнить ранее освоенный материал. Для этого мы с вами разгадаем кроссворд. Право ответа на каждый вопрос переходит по очереди. И в конце, самые активные получат положительные оценки».

Разгадывание кроссворда (на ответ дается 30 сек). Подсчет плюсов. Выставление оценок за кроссворд.



3. Введение в тему занятия и целеполагание (5 мин.)

«Кроссворд разгадан. Подумайте, почему именно этот кроссворд мы сегодня разгадывали? Почему именно на этих определениях сегодня акцентировал Ваше внимание?

Пользовательский

Обеспечение

Безопасность

Компьютер

«Как можно связать все эти слова в одно смысловое предложение»

Наводящими вопросами учитель формируем тему сегодняшнего занятия.

Обеспечение безопасности пользовательских компьютеров

«Посмотрите на тему занятия. Скажите, что вы сегодня будете изучать? (учащиеся предполагают, что безопасность ПК и ПО. Уточняем, что не простое ПО, а ПО для защиты информации).

Что вы будете знать по окончанию урока?»

4. Первичное введение материала

Учителем даются начальные краткие теоретические сведения:

Программные средства - это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения

Программными называются средства защиты данных, функционирующие в составе программного обеспечения.

Среди них можно выделить и подробнее рассмотреть следующие:

- средства архивации данных;
- антивирусные программы;
- криптографические средства;
- средства идентификации и аутентификации пользователей;
- средства управления доступом;
- протоколирование и аудит.

После кратких теоретических данных, учащимся выдается задание для самостоятельного изучения теоретического материала по основному ПО и заполнения таблицы. (Можно использовать материал из Интернета, сайта с лекциями, раздаточный материал) (12 мин.)

ПО средств защиты информации	Вопросы
1. Средства архивации информации	1. Что это такое? 2. Как, используя это ПО, можно защитить информацию? 3. Приведите примеры программ
2. Антивирусные программы	
3. Криптографические средства	
4. Средства идентификации и аутентификации	
5. Защита информации от НСД	
6. Межсетевые экраны, proxy, VPN	

5. Первичное закрепление материала (5 мин.)

«Сейчас, я спрошу ответы на поставленные вопросы в таблице, некоторых учащихся. Остальные внимательно слушаете ответы товарища. Если есть замечания или дополнения к ответу сообщаете об этом».

Учитель выборочно опрашивает отдельные учащиеся по заполненной таблице.

5.1. Как с помощью средств архивации можно защитить информацию?

5.2. Какое программное обеспечение защищает систему от вторжения вредоносных программ?

5.3. Какое назначение криптографических средств защиты информации?

5.4. Назначение средств идентификации и аутентификации

Остальные учащиеся внимательно слушают ответы. Если есть замечания и дополнения сообщают об этом всем присутствующим. По итогам опроса учитель подводит иэтого тоги блока.

6. Контроль результатов первичного запоминания (10 мин.)

Для проверки знаний, полученных сегодня на уроке пройдете тест. Тест состоит из 10 практико-ориентированных задач. Время на тест 10 минут. Если имеются отрицательные оценки за тест, происходит разбор заданий теста.

7. Подведение итогов (2 мин.)

Сегодня на уроке Вы узнали, что для защиты информации используется различное программное обеспечение: от архиваторов до VPN- серверов. А какое ПО стоит в нашем техникуме, обеспечивающее защиту информации?

8. Домашнее задание (3 мин.) «Разработайте систему мер по защите информации в ЛВС организации»

9. Рефлексия (2 мин.)

Учащимся предлагается продолжить следующие фразы.

- Мне запомнилось ...
- Сегодня я узнал…
- Урок дал мне …
- Теперь я могу…

Список использованных источников

Основные источники:

1. Палмер, М. Проектирование и внедрение компьютерных сетей. Учебный курс [электронная версия] - / М. Палмер, Р.Б. Синклер. - 2-е изд., перераб. и доп.: Пер с англ. – СПб.: БХВ- Петербург, 2018.
2. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2017. — 224 с.
3. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2018. – 437 с.

4. Цирлов, В.Л. Основы информационной безопасности автоматизированных систем [электронная версия]/ В.Л. Цирлов – Ростов-на-Дону: Феникс, 2017.- 173 с.
1. Национальный Открытый Университет «ИНТУИТ» [Электронный ресурс]. — Режим доступа: URL: http://www.intuit.ru/ (дата обращения: 14.02.22).

Теоретический материал

1. Средства архивации информации

Иногда резервные копии информации приходится выполнять при общей ограниченности ресурсов размещения данных, например владельцам персональных компьютеров. В этих случаях используют программную архивацию.

Архивация это слияние нескольких файлов и даже каталогов в единый файл — архив, одновременно с сокращением общего объема исходных файлов путем устранения избыточности, но без потерь информации, т. е. с возможностью точного восстановления исходных файлов. Действие большинства средств архивации основано на использовании алгоритмов сжатия, предложенных в 80-х гг. Абрахамом Лемпелем и Якобом Зивом. Наиболее известны и популярны следующие архивные форматы:

- ZIP, ARJ для операционных систем DOS и Windows;
- TAR для операционной системы Unix;
- межплатформный формат JAR (Java ARchive);
- RAR

Пользователю следует лишь выбрать для себя подходящую программу, обеспечивающую работу с выбранным форматом, путем оценки ее характеристик – быстродействия, степени сжатия, совместимости с большим количеством форматов, удобности интерфейса, выбора операционной системы и т.д. Список таких программ очень велик – PKZIP, PKUNZIP, ARJ, RAR, WinZip, WinArj, ZipMagic, WinRar и много других. Большинство из этих программ не надо специально покупать, так как они предлагаются как программы условно-бесплатные (Shareware) или свободного распространения (Freeware). Также очень важно установить постоянный график проведения таких работ по архивации данных или выполнять их после большого обновления данных.

2. Антивирусные программы

Это программы разработанные для защиты информации от вирусов. Неискушенные пользователи обычно считают, что компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять нежелательные различные действия на компьютере.

Специалисты по компьютерной вирусологии определяют, что обязательным (необходимым) свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты.

При этом дубликаты сохраняют способность к дальнейшему распространению. Следует отметить, что это условие не является достаточным, т.е. окончательным. Вот по-

чему точного определения вируса нет до сих пор, и вряд ли оно появится в обозримом будущем. Следовательно, нет точно определенного закона, по которому “хорошие” файлы можно отличить от “вирусов”. Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

Особую проблему представляют собой компьютерные вирусы. Это отдельный класс программ, направленных на нарушение работы системы и порчу данных. Среди вирусов выделяют ряд разновидностей. Некоторые из них постоянно находятся в памяти компьютера, некоторые производят деструктивные действия разовыми "ударами".

Существует так же целый класс программ, внешне вполне благопристойных, но на самом деле портящих систему. Такие программы называют "троянскими конями". Одним из основных свойств компьютерных вирусов является способность к "размножению" - т.е. самораспространению внутри компьютера и компьютерной сети.

С тех пор, как различные офисные прикладные программные средства получили возможность работать со специально для них написанными программами (например, для Microsoft Office можно писать приложения на языке Visual Basic) появилась новая разновидность вредоносных программ - МакроВирусы. Вирусы этого типа распространяются вместе с обычными файлами документов, и содержатся внутри них в качестве обычных подпрограмм.

С учетом мощного развития средств коммуникации и резко возросших объемов обмена данными проблема защиты от вирусов становится очень актуальной. Практически, с каждым полученным, например, по электронной почте документом может быть получен макровирус, а каждая запущенная программа может (теоретически) заразить компьютер и сделать систему неработоспособной.

Поэтому среди систем безопасности важнейшим направлением является борьба с вирусами. Существует целый ряд средств, специально предназначенных для решения этой задачи. Некоторые из них запускаются в режиме сканирования и просматривают содержимое жестких дисков и оперативной памяти компьютера на предмет наличия вирусов. Некоторые же должны быть постоянно запущены и находиться в памяти компьютера. При этом они стараются следить за всеми выполняющимися задачами.

Существуют следующие виды антивирусов : Acronis AntiVirus, AhnLab Internet Security, AOL Virus Protection, ArcaVir, Ashampoo AntiMalware, Avast!, Avira AntiVir, A-square anti-malware, BitDefender, CA Antivirus, Clam Antivirus, Command Anti-Malware, Comodo Antivirus, Dr.Web, eScan Antivirus, F-Secure Anti-Virus, G-DATA Antivirus, Graugon Antivirus, IKARUS virus.utilities, Антивирус Касперского, McAfee VirusScan, Microsoft Security Essentials, Moon Secure AV, Multicore antivirus, NOD32, Norman Virus Control, Norton AntiVirus, Outpost Antivirus, Panda и т.д.

Методы обнаружения и удаления компьютерных вирусов.

Способы противодействия компьютерным вирусам можно разделить на несколько групп:

- профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения;
- методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса;

Способы обнаружения и удаления неизвестного вируса:

- Профилактика заражения компьютера;

- Восстановление пораженных объектов;
- Антивирусные программы.

3. Криптографические средства

Механизмами шифрования данных для обеспечения информационной безопасности общества является криптографическая защита информации посредством криптографического шифрования.

Криптографические методы защиты информации применяются для обработки, хранения и передачи информации на носителях и по сетям связи. Криптографическая защита информации при передаче данных на большие расстояния является единственно надежным способом шифрования.

Криптография – это наука, которая изучает и описывает модель информационной безопасности данных. Криптография открывает решения многих проблем информационной безопасности сети: аутентификация, конфиденциальность, целостность и контроль взаимодействующих участников.

Термин «Шифрование» означает преобразование данных в форму, не читабельную для человека и программных комплексов без ключа шифрования-расшифровки. Криптографические методы защиты информации дают средства информационной безопасности, поэтому она является частью концепции информационной безопасности.

Криптографическая защита информации (конфиденциальность)

Цели защиты информации в итоге сводятся к обеспечению конфиденциальности информации и защите информации в компьютерных системах в процессе передачи информации по сети между пользователями системы.

Защита конфиденциальной информации, основанная на криптографической защите информации, шифрует данные при помощи семейства обратимых преобразований, каждое из которых описывается параметром, именуемым «ключом» и порядком, определяющим очередность применения каждого преобразования.

Важнейшим компонентом криптографического метода защиты информации является ключ, который отвечает за выбор преобразования и порядок его выполнения. Ключ – это некоторая последовательность символов, настраивающая шифрующий и дешифрующий алгоритм системы криптографической защиты информации. Каждое такое преобразование однозначно определяется ключом, который определяет криптографический алгоритм, обеспечивающий защиту информации и информационную безопасность информационной системы.

Один и тот же алгоритм криптографической защиты информации может работать в разных режимах, каждый из которых обладает определенными преимуществами и недостатками, влияющими на надежность информационной безопасности.

4. Идентификация и аутентификация пользователя

Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс представления компьютерной системе, который включает две стадии:

• идентификацию - пользователь сообщает системе по ее запросу свое имя (идентификатор);

• аутентификацию - пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль).

Для проведения процедур идентификации и аутентификации пользователя необходимы:

• наличие соответствующего субъекта (модуля) аутентификации;

• наличие аутентифицирующего объекта, хранящего уникальную информацию для аутентификации пользователя.

Различают две формы представления объектов, аутентифицирующих пользователя:

• внешний аутентифицирующий объект, не принадлежащий системе;

• внутренний объект, принадлежащий системе, в который переносится информация из внешнего объекта.

Внешние объекты могут быть технически реализованы на различных носителях информации - магнитных дисках, пластиковых картах и т. п. Естественно, что внешняя и внутренняя формы представления аутентифицирующего объекта должны быть семантически тождественны.

5. Защита информации в КС от несанкционированного доступа

Для осуществления несанкционированного доступа злоумышленник не применяет никаких аппаратных или программных средств, не входящих в состав КС. Он осуществляет несанкционированный доступ, используя:

• знания о КС и умения работать с ней;

• сведения о системе защиты информации;

• сбои, отказы технических и программных средств;

• ошибки, небрежность обслуживающего персонала и пользователей.

Для защиты информации от несанкционированного доступа создается система разграничения доступа к информации. Получить несанкционированный доступ к информации при наличии системы разграничения доступа возможно только при сбоях и отказах КС, а также используя слабые места в комплексной системе защиты информации. Чтобы использовать слабости в системе защиты, злоумышленник должен знать о них.

Одним из путей добывания информации о недостатках системы защиты является изучение механизмов защиты. Злоумышленник может тестировать систему защиты путем непосредственного контакта с ней. В этом случае велика вероятность обнаружения системой защиты попыток ее тестирования. В результате этого службой безопасности могут быть предприняты дополнительные меры защиты.

Гораздо более привлекательным для злоумышленника является другой подход. Сначала получается копия программного средства системы защиты или техническое средство защиты, а затем производится их исследование в лабораторных условиях. Кроме того, создание неучтенных копий на съемных носителях информации является одним из распространенных и удобных способов хищения информации. Этим способом осуществ-

ляется несанкционированное тиражирование программ. Скрытно получить техническое средство защиты для исследования гораздо сложнее, чем программное, и такая угроза блокируется средствами и методами обеспечивающими целостность технической структуры КС. Для блокирования несанкционированного исследования и копирования информации КС используется комплекс средств и мер защиты, которые объединяются в систему защиты от исследования и копирования информации. Таким образом, система разграничения доступа к информации и система защиты информации могут рассматриваться как подсистемы системы защиты от несанкционированного доступа к информации.

6. Другие программные средства защиты информации

Межсетевые экраны (также называемые брандмауэрами или файрволами — от нем. Brandmauer, англ. firewall — «противопожарная стена»). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода — это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

Межсетевые экраны

Бесплатные	Ashampoo FireWall Free • Comodo • Core Force (англ.) • Online Armor • PC Tools • PeerGuardian (англ.) • Sygate (англ.)
Проприетарные	Ashampoo FireWall Pro • AVG Internet Security • CA Personal Firewall • Jetico (англ.) • Kaspersky • Microsoft ISA Server • Norton • Outpost • Trend Micro (англ.) • Windows Firewall • Sunbelt (англ.) • WinRoute (англ.) • ZoneAlarm
Аппаратные	Fortinet • Cisco • Juniper • Check Point
FreeBSD	Ipfw • IPFilter • PF
Mac OS	NetBarrier X4 (англ.)
Linux	Netfilter (Iptables • Firestarter • Iplist • NuFW • Shorewall) • Uncomplicated Firewall

Proxy-servers (proxy - доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях — например, на уровне приложения (вирусы, код Java и JavaScript).

VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.