МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РБ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ
ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»

УТВЕРЖДАЮ

Замдиректора по УР

«____»_____20__ г.

МЕТОДИЧЕСКАЯ РАЗРАБОТКА ОТКРЫТОГО ЗАНЯТИЯ ПО ТЕМЕ:

«Информационная безопасность. Основные определения»

Разработал: Тенгайкин Е.А.,
преподаватель спец.дисциплин

г. Улан-Удэ

2021

ТЕХНОЛОГИЧЕСКАЯ КАРТА (ПРОЕКТ) АУДИТОРНОГО ЗАНЯТИЯ

ПМ.03 Эксплуатация объектов сетевой инфраструктуры

Ф.И.О. преподавателя: Тенгайкин Евгений Александрович

Группа: 146

Дата: 17,02.2021

Наименование изучаемого раздела **МДК 03.02.** Безопасность функционирования информационных систем

Наименование изучаемой темы Информационная безопасность. Основные определения.

Тип занятия Урок изучения нового материала

Вид занятия урок-диспут

Цель:

Образовательная планируется , что к окончанию урока обучающиеся будут знать понятие информационной безопасности, основные этапы защиты информации на уровне коммутатора; углубить знания о методах обеспечения информационной безопасности в компьютерных сетях;

Развивающая формирование ОК- 4, продолжить развитие умения анализировать, выделять главное, устанавливать причинно-следственные связи; приводить примеры, формировать умения работы с литературой, информационными ресурсами, таблицами, схемами (выполнение самостоятельной аудиторной работы), выступать перед аудиторией, работать над формированием умений и навыков у студентов по умению вести спор, дискуссию, выражать свое мнение

Воспитательная воспитание информационной культуры, формирование ОК- 2,3, развить у студентов навыки самостоятельного мышления; совершенствовать навыки общения

Валеологическая продолжить формирование ПК по соблюдению ТБ и ПП за компьютером, проводить минуты отдыха для снятия усталости

Методы обучения проблемно-поисковый, репродуктивный, словесный (рассказ, сценка), наглядный, диалогический, самостоятельная работа

Формы обучения индивидуальная, групповая

Средства обучения компьютер, интерактивная доска, программное обеспечение

Формы и методы контроля устный опрос

Междисциплинарные связи ПМ.02 Организация сетевого администрирования

Внутридисциплинарные связи МДК 03.01 Тема Организационные меры обеспечения безопасности Модель системы защиты. Идентификация и аутентификация. Разграничение доступа.

Обучающийся должен знать основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных, основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.

Обучающийся должен уметь эксплуатировать технические средства сетевой инфраструктуры; устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;
Обучающийся должен иметь практический опыт (Для МДК) по организации бесперебойной работы системы, резервного копирования и восстановления информации;

Подготовка к диспуту заняла три недели. Была создана творческая группа, которая заранее вместе с ведущими разработала под руководством преподавателя вопросы, а также составила список рекомендованной литературы к теме, которая обговаривалась, и сообщала о наработках студентам.

Аудитория была подготовлена к проведению диспута: цитаты специалистов по информационной безопасности, были распечатаны специальные термины с пояснениями. У студентов памятки - правила ведения дискуссии. Ведущим диспута был не только преподаватель, но и студент, участвующий в сценке и направляющий дискуссию в нужное русло.

Ход занятия

№ /№	Содержание и структура занятия	Время	Деятельность преподавателя	Деятельность обучающегося	Методы обучения и контроля	Формы обучения	Средства обучения	Формируемые компетенции	
								ПК	ОК
1	Орг. момент	1 м.	Приветствие, определение отсутствующих, организация внимания.	Слушают преподавателя, строят понятные для собеседника высказывания, принимают и сохраняют учебные цели занятия	словесный	Коллективная	Интерактивная доска	ПК 2	ОК 1
2	Формирование темы и цели урока	2 м.	Целеполагание	Слушают преподавателя	словесный	Коллективная	Интерактивная доска	ПК 2	ОК 2

3	Повторение ранее изученного материала	3 м	Актуализация	Отвечают на вопросы	Метод диалога , интерактивный	Коллективная	Интерактивная доска	ПК 2	ОК 2
4	Первичное введение материала и запоминание	15 м.	Ведет диалог с помощником и студентами	Слушают преподавателя, строят понятные для собеседника высказывания, принимают участие в диалоге, диспуте	Метод диалога, интерактивный	Индивидуальная	Интерактивная доска	ПК 2.	ОК 2. ОК 4. ОК 5
5	Первичное закрепление материала	16 м	Делит студентов на 2 команды	Члены каждой команды высказывают свое отношение к проблеме защиты информации		Коллективная	Интерактивная доска	ПК 3.	ОК 3.
6	Подведение итогов урока	3	Подводит итоги	Слушают	фронтальный	Коллективная	Интерактивная доска	ПК 2.	ОК 2. ОК 4. ОК 5
7	Домашнее задание	3	Организует запись домашнего задания	Слушают и записывают	фронтальный	Коллективная	Интерактивная доска	ПК 2.	ОК 2. ОК 4.

									ОК 5
8	Рефлексия	2	Дает оценку собственной деятельности на занятии	Дают оценку собственной деятельности и деятельности преподавателя на занятии	фронтальный	Коллективная	Интерактивная доска	ПК 3.	

Разработчик_____ _____ _____

(должность) (подпись) (расшифровка подписи)

Конспект урока

I. Организационный момент

Приветствие, контроль отсутствующих, пояснение плана урока.

Преподаватель: Добрый день уважаемые студенты и гости! Сегодня у нас необычный урок, вы наверно заметили, что у нас гости на уроке, столы стоят не как всегда и у меня есть помощник. Его зовут Системный администратор.

II.Формирование темы и целей урока

Давайте вспомним, что мы изучали на прошлом занятии? Мы с вами изучаем сейчас большую тему «Информационная безопасность». Далее преподаватель вместе со студентами формулирует и конкретизирует тему занятия.

Преподаватель: Итак, сегодня мы собрались, чтобы обсудить очень актуальную тему : «Информационная безопасность в локальных компьютерных сетях с использованием сетевого оборудования».

Цель: (формируется вместе со студентами) сформировать в ходе диспута ответ на вопрос: «Какое значение имеет управляемый коммутатор для обеспечения информационной безопасности в локальной сети?».

III. Актуализация знаний

Сегодня, прежде чем продолжить изучение темы, мы с вами повторим материал прошлого урока. И мы это сделаем с помощью небольшого опроса.

Ответьте на предложенные вопросы.

На выполнение этой работы вам отводится 3 минуты, а после мы продолжим.

1. Вспомним свойства информации (предлагается ответить студентам).

Свойства информации:

- конфиденциальность; (есть информация открытая)
- целостность;
- доступность.

Вся безопасность направлена на то, чтобы сохранить эти свойства информации.

2. Что может нарушить эти свойства? (Вопрос студентам).

Угроза - некий риск, который может произойти с информацией;

Уязвимость - свойство, которое может реализовать угрозу;

Атаки - это реализация угрозы, через эксплуатацию уязвимости;

После ответов студентов к преподавателю присоединяется помощник.

Помощник: Может быть, не стоит говорить об информационной безопасности? Можно встретить такое, например, мнение. «Что же будет через пару десятков лет, когда выросшие в социальных сетях современные дети станут управлять государствами? Дипломатия умрет, потому что дипломаты будут обо всем писать в Твиттере. Разведка умрет, потому что, во-первых, все секреты можно будет прочитать в Твиттере, а во-вторых, разведчики не смогут работать на нелегальном положении, поскольку они обо всем будут писать в Твиттере. А бизнес станет прозрачным настолько, что через него можно будет разглядеть звезды». Так считает Максим Кононенко, журналист, писатель.

Преподаватель: Возможна ли такая ситуация ? Что может этому помешать?

Помощник – нет, я думаю, что нет, всегда будет угроза информации, которая передаётся по сети, то есть трафику.

Преподаватель: Как же защитить трафик в сети?

Давайте представим, что мы все работаем в некой фирме, где есть системный администратор, технический директор, много компьютеров и специалистов.

У Сисадмина есть Учитель т.е Гуру

Далее между преподавателем и ведущим разыгрывается сценка.

И Однажды……..

Однажды Сисадмин пожаловался Учителю:

Сис. админ – Наш Тех.директор не хочет выполнять требования безопасности. Нужно заменить сетевой коммутатор L2 на L3, а он не хочет. Как на него повлиять?

– Попробуй его убедить, – сказал Гуру.

Сисадмин ушёл убеждать, но вскоре вернулся разочарованным:

– Я не смог убедить его, Учитель.

– Почему так случилось? – спросил Гуру и сразу же заметил. – Но только ответь честно, без пристрастия и обиды.

Сисадмин подумал, опустил глаза и тихо сказал:

– Наверное, потому, что он знает об информационной безопасности больше меня.

– Ну, если Тех.директор знает больше тебя, что совсем не удивительно, – заметил Учитель, – то ему виднее, нужен ли коммутатор L3.

– А как же тогда Политика безопасности! – воскликнул Сисадмин.

– А кто писал эту Политику?

Сисадмин потупился и сказал:

– Я.

Учитель мудро промолчал, и Сисадмин ушёл просветлённый.

Преподаватель: Так прав ли Тех.директор, что не хочет менять коммутаторы?

Вопрос к студентам:
Можно ли обеспечить безопасность сети одними только программными методами ?

(Основой, базисом, на который будут опираться средства защиты ОС, должно стать сетевое оборудование. Сегодня в подавляющем числе случаев локальные сети строятся с использованием коммутаторов (switch))

Преподаватель: Давайте вспомним определение коммутатора .(**Вопрос к студентам**)

(Под коммутаторами понимают переключающие устройства, которые служат для соединения нескольких узлов сети.)

Помощник: В локальной сети взаимное распознавание компьютеров происходит по нескольким признакам. Причиной тому – длительная эволюция сетевых технологий и протоколов. Впрочем, на сегодня TCP/IP, будучи наиболее гибким и универсальным протоколом сетевых коммуникаций, практически вытеснил своих конкурентов. В TCP всего 4 уровня

Преподаватель: какие уровни у модели TCP/IP? (**Вопрос к студентам**).

- канальный;
- сетевой;
- транспортный;
- прикладной.

Преподаватель: поговорим о защите трафика на канальном уровне т.к. безопасность канального уровня можно считать синонимом безопасности локальной сети.

Предлагаю разделиться на две команды: команда «оптимистов» и команда «пессимистов» и высказать свой взгляд на эту проблему (обосновать свое отношение к ней)

Оптимисты	**Пессимисты**
1.Как ни банально звучит, но канальный уровень — это краеугольный камень безопасности компьютерной сети. Принципы работы коммутаторов Ethernet, а также протоколы ARP и DHCP, использующие широковещательные рассылки, разработаны много лет назад. Говорить если спросят Ethernet- пакетная технология передачи данных преимущественно локальных компьютерных сетей. ARP- протокол в компьютерных сетях, предназначенный для определения MAC адреса по известному IP адресу. DHCP- (протокол динамической настройки узла) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.	В основе этих подходов — доверие участников сетевых взаимодействий друг к другу, что в сегодняшних реалиях неприемлемо. Атаковать узлы и/или нарушить работоспособность локальной сети, построенной на основе неуправляемых свитчей, — проще простого.

Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP, и получает от него нужные параметры Широковещательная рассылка знаю – это когда определённый пакет посылается не конкретному хосту, а всем хостам в подсети.	
Помощник: Как же противостоять атакам в сети ? Это сложный вопрос.	
Что же скажут оптимисты ? и Что возразят пессимисты?	
Коммутатор может быть и достаточно мощным средством защиты. Так как через него происходит всё взаимодействие в сети, то логично контролировать это на нем.	Сам коммутатор и протоколы, которые используют коммутаторы могут быть целью атак. Более того, некоторые настройки коммутаторов (как правило, это настройки по умолчанию) позволяют выполнить ряд атак и получить несанкционированный доступ к сети или вывести из строя сетевые устройства.
Конечно, использование коммутатора как средства защиты предполагает, что используется не простейший коммутатор 2го уровня, а коммутатор с соответствующими функциями для обеспечения безопасности.	Они с весьма ограниченными возможностями (как правило, нельзя подсчитать трафик, построить сложные фильтры, добавить скрипт)

Сегодня есть коммутаторы 3-го и более высокого уровня, способные в добавление к обычным функциям маршрутизировать трафик между портами на IP-уровне и обеспечить конфиденциальности трафика.	
Есть модели, которые имеют эти возможности	

Помощник: Вывод первый рубеж защиты приходится на уровень доступа к сетевой инфраструктуре. Основной инструмент борьбы со злом — управляемый коммутатор.

Вопрос к студентам : Так прав ли Тех.директор?

Интеллектуальности коммутаторов второго уровня достаточно только для пересылки кадров на основе MAC- адресов, но они не имеют представления о сети в целом. Коммутаторы третьего уровня обладают интеллектуальностью маршрутизатора. Они не только могут маршрутизировать пакеты на основе их IP-адресов, они также могут выбирать маршруты на основе их доступности и производительности. Коммутаторы третьего уровня – это «продвинутые» маршрутизаторы, т.к. они переводят функции анализа маршрутов на более эффективный аппаратный уровень.

Поскольку безопасность требует контроля доступа к определенным ресурсам, более интеллектуальные устройства обеспечивают более высокий уровень защиты, т.к. они могут принять больше ориентированных на детали решений о доступе к ресурсам. Если устройство может заглянуть глубже в пакеты, оно может узнать больше информации для принятия решения о возможности предоставления доступа, что обеспечивает более детальный контроль.

Преподаватель: Конечно, мы не говорим о серьезных операторских или корпоративных сетях. Там коммутаторы 3-го и последующих уровней, пожалуй, уже прошлый день. Речь идет скорее о внедрении технологий типа MPLS. Можно применить коммутаторы 3-го уровня в небольшой или средней бюджетной сети, но об этот мы поговорим на следующих уроках.

IV. Рефлексия.

Преподаватель: а теперь я прошу студентов сделать оценку сегодняшнего занятия и оценить свою работу на занятии. Оценивать предлагаю двумя способами:

1. Я работал очень хорошо, многому научился.
2. Я работал хорошо, но мне необходимо еще многому научиться

После проведения самоанализа подводится итог занятия.

Домашнее задание:

Подготовить сообщения или презентацию на темы:

1. Коммутаторы уровней 3 и 4.
2. Значение сетевого оборудование для обеспечения информационной безопасности.
3. Подготовить конспект на тему : «Коммутаторы как средство защиты в локальных сетях».

Памятка "Как вести дискуссию"

1. Перед тем, как спорить, подумай, что именно ты должен сказать.
2. Если ты пришел на диспут, обязательно выскажи и аргументируй свое мнение.
3. Говори просто и ясно, логично и последовательно
4. Говори только то, что тебя интересует, что ты знаешь, в чем ты уверен, не утверждай того, в чем сам не уверен.
5. Спорь честно: не перекручивай мысли человека, с которым ты не согласен.
6. Не повторяйся и не повторяй слов других.
7. Помни, что лучшие доказательства - точные факты.
8. Уважай того, кто спорит с тобой; твое тактичное поведение доказывает, что ты не только сильный оппонент, но и воспитанный человек.

Памятка для самоанализа занятия

А. Каков был замысел, план проведенного занятия и почему?

1. Каковы главные основания выбора именно такого замысла занятия?

1.1 Каково место данного занятия в теме, разделе, курсе, в системе занятий?(Как он связан с предыдущими занятиями, на что в них опирается, как он работает на последующие занятия, темы, разделы (в том числе других учебных дисциплин и МДК),

1.2. Как были учтены при подготовке к занятию программные требования, образовательные стандарты, стратегия развития техникума?

1.4. Какие особенности обучающихся, были учтены при подготовке к занятию (и почему именно эти особенности)?

1.3 Как (и почему) была выбрана именно предложенная форма занятия и технологии?

1.5. Чем обосновывается выбор структуры и темпа проведения занятия?

Б. Были ли изменения (отклонения, усовершенствования) по сравнению с данным планом в ходе занятия, если - да, какие, почему и к чему они привели?

В. Удалось ли:

• решить на необходимом (или даже оптимальном) уровне поставленные задачи занятия и получить соответствующие им результаты обучения;

• избежать перегрузки и переутомления учащихся;

• сохранить и развить продуктивную мотивацию учения, настроение, самочувствие? Какова общая самооценка занятия?

Г.Каковы причины успехов и недостатков проведенного занятия? Каковы неиспользованные, резервные возможности? Что в этом занятии следовало бы сделать иначе, по-другому?

Д.Какие выводы из занятия необходимо сделать на будущее?