Министерство образования Ставропольского края

государственное бюджетное профессиональное

образовательное учреждение

«Георгиевский техникум механизации, автоматизации и управления»

(ГБПОУ ГТМАУ)

ОТЧЕТ

о прохождении практики производственной (по профилю специальности)

ПМ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Место прохождения \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ г. по «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_\_ г.

|  |  |  |
| --- | --- | --- |
|  |  | Выполнил студент \_\_\_\_\_\_\_\_\_\_ группы  Специальность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (ФИО)  Руководитель от техникума  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Руководитель от предприятия  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  МП |

Георгиевск 201\_\_\_

**СОДЕРЖАНИЕ**

Введение.

Техническое и программное обеспечение.

Описание выполняемых работ.

Заключение.

**Введение.**

Я проходил учебно-ознакомительную практику на базе Георгиевского техникума механизации, автоматизации и управления (ГБПОУ ГТМАУ). Продолжительность практики с 01 декабря по 28 декабря 2020 года.

Цель практики:

* закрепить теоретические знания и получить навыки их практического применения.
* ознакомление со спецификой деятельности системного администратора.
* практическое проведение теоретической и экспериментальной работы в качестве системного администратора.
* изучение выявление тенденции эмоционального и профессионального выгорания системного администратора.

**Техническое и программное обеспечение**

В учреждении есть 90 компьютеров.

Во время учебной практике был задействован один компьютер.

Процессор: i3 4150

Видеокарта: встроенная

ОЗУ: 4Гб

Жесткий диск: 500Гб

Сетевая карта: Acorp L100S

Монитор: ЖК 19д

Маршрутизатор.

Mikrotik RB2011UiAS-2HnD-IN

Cisco 2800 Series

Cisco 2960 Series

Коммутатор.

TP-Link TL-SF1005D

ПО компьютера.

ОС: Windows 10

Офис: MS Office 2010

ПО: WinBox

ПО: PuTTY

ПО: Packet tracer

**Описание выполняемых работ.**

**Построение модели информационной системы и описание её структуры.**

Полноценной информационной моделью является обычно сложная разработка, которая может иметь три основных типа:

1.Описательная. Сюда относятся модели, которые создаются на естественных языках. Они могут иметь любую произвольную структуру.

2.Формальная. Сюда относят модели, которые создаются на формальных языках. В качестве примеров можно привести такое: все виды таблиц, формул, граф, карт, схемы и прочих подобных структурных формаций.

3.Хроматические. Сюда относят модели, которые были созданы с применением естественного языка семантики цветовых концептов, а также их онтологических предикатов. В качестве примера хроматических моделей можно навести те, что были построены с использованием соответствующей теоретической базы и методологии.

В результате работы сделал формальное описание системы в виде совокупной модели.

**Установка и настройка платы сетевого адаптера.**

Установил сетевую карты Acorp L100S в слот PCI-e. Установил драйвер. Настроил. Проверил на отказоустойчивость.

**Расчет адресации в больших сетях.**

IP-адрес состоит из 32-бит, и делится на 4 октета по 8 бит.

Маска сети также представляет собой 32-битное бинарное число, где количество единиц, начиная со старшего октета , определяет размер сети. Двойка, возведенная в степень количества нулей, определяет количество возможных хостов без двух адресов: первый адрес — это адрес самой сети, последний адрес отводится для широковещательных запросов.

Для расчета адреса широковещательных запросов представим нашу сеть 158.4.73.39/23 в промежуточной форме. Так как 2 старших октета заданной маски сети состоят полностью из единиц, то нам нет необходимости преобразовывать старшие 2 октета IP-адреса в двоичную форму. Мы будем использовать для расчета адресации узлов младшие 2 октета.

Отсекаем слева старшие 23 бита из 32, так как они не участвуют в расчете разрешенных IP-адресов для [узлов нашей сети](https://14bytes.ru/kak-vkljuchit-telnet-klient-v-windows-10/).

Как результат, мы получаем промежуточную форму записи исходного IP-адреса 4 версии протокола для упрощения расчета: 158.4.0100 1001.0010 0111.

Таким образом мы получили: 158.4.01001001.00100111 — IP-адрес с маской 11111111.11111111.11111110.00000000; 158.4.0100100 0.00000000 — адрес сети; 158.4.0100100 0.00000001 — первый IP-адрес сети; 158.4.0100100 1.11111110 — последний IP-адрес; 158.4.0100100 1.11111111 — адрес для отправки широковещательных запросов в сеть.

**Обеспечение бесперебойной работы сети. Отказоустойчивость сети.**

Для обеспечения бесперебойной работы сети нам потребуется установить для каждого коммутатора и маршрутизатора антивандальный ящик и источник бесперебойного питания. Для отказоустойчивость сети необходимо резервирование LAN-соединений и резервирование WAN-соединений.

В нашем случаи для обеспечение бесперебойной работы сети нужно установить антивандальный ящик и источник бесперебойного питания для коммутатора (TP-Link TL-SF1005D) и маршрутизатора (Mikrotik RB2011UiAS-2HnD-IN). Для отказоустойчивость сети нужно установить резервирование LAN-соединений и резервирование WAN-соединений.

**Настройка коммутаторов локальной сети.**

Очистка конфигурации: после извлечения коммутатора из коробки, подключаемся к нему [с помощью консольного кабеля](http://deltaconfig.ru/begin-to-configure-cisco/) и очищаем текущую конфигурацию. После выполнения коммутатор должен перезагрузиться в течение 3ех минут.

Имя коммутатора: присвоим коммутатору имя **SW-LOCAL-1.**

Интерфейс для удаленного управления: настраиваем интерфейс для управления коммутатором. По умолчанию это **Vlan 1**. Для этого присваиваем **ip** адрес интерфейсу и включаем его.

Авторизация пользователей: настраиваем авторизацию для доступа к устройству. Для этого задаем пароль доступа к привилегированному режиму, а также создаем учетную запись пользователя и пароль для удаленного подключения. Задаем пароль для доступа к привилегированному режиму. Создаем учетную запись для удаленного управления и пароль для нее. Включение авторизации, с использованием локальной базы данных пользователей и паролей.

Создание Vlan: создаем нужное количество Vlan и присваиваем им порядковые номера и названия. Сеть **Vlan 1** всегда присутствует на коммутаторе по умолчанию. Она будет использоваться для удаленного управления. Убеждаемся, что все созданные нами сети присутствуют.

Привязка портов: Соотносим порты доступа коммутатора (**access port**) нужным сетям. На коммутаторе Cisco 2960 Series 24 порта **Fast Ethernet** и 2 порта **Gigabit Ethernet**. Для подключения пользователей будут использоваться только **Fast Ethernet**.

Распределим их следующим образом:

* первые 6 из них в сеть администраторов (Vlan 100)
* 12 в сеть отдела продаж (Vlan 10)
* 6 следующих в сеть для бухгалтерии (Vlan 20).

На каждом интерфейсе для удобства дальнейшего администрирования добавим примечания командой description. Это обычное текстовое поле, которое никак не влияет на другие настройки.

После этого рядом с каждым **Vlan** будут указаны принадлежащие ему порты. Введенными командами мы разделили один физический коммутатор на 4 логических.

Сохраним настройки.

**Обеспечение комплексной безопасности в инфокоммуникационных системах.**

Информационная безопасность сетей представляет собой "состояние защищённости сбалансированных интересов производителей информационно-коммуникационных технологий и конкретно сетей, потребителей, операторов и органов государственной власти в информационной сфере. В свою очередь информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования отношений, возникающих при использовании сетей связи.

Можно выделить ряд особенностей, которые делают сети уязвимыми, а нарушителей — практически неуловимыми:

* возможность действия нарушителей на расстоянии в сочетании с возможностью сокрытия своих истинных персональных данных;
* возможность пропаганды и распространения средств нарушения сетевой безопасности;
* возможность многократного повторения атакующих сеть воздействий.

Наиболее часто встречающиеся дефекты защиты, отмеченные компаниями, работающими в области электронного бизнеса и защиты информации:

* общие проблемы в брандмауэрах, операционных системах, сетях и стандартных приложениях;
* неопознанные машины или приложения в сети;
* использование старых версий программного обеспечения на машинах сети;
* неполная информация обо всех точках входа в сеть из внешней среды;
* неполное изъятие прав доступа при увольнении сотрудников, наличие идентификаторов пользователей, используемых по умолчанию, неверно обслуживаемые права доступа;
* неоправданно открытые порты в брандмауэрах;
* необоснованный общий доступ к файловым системам;
* недостаточные требования к идентификации пользователя, собирающегося изменить регистрационные записи пользователей;
* присутствие ненужных сервисов или приложений на машинах, требующих высокой степени защиты;
* использование слабозащищенных установочных параметров, присваиваемых по умолчанию при инсталляции приложений, ввиду чего становятся известны идентификаторы и пароли пользователей, установленные по умолчанию;
* отсутствие защиты от взаимодействия внутреннего и внешнего трафика сети;
* отсутствие проверок после внесения изменений в среду (например, после инсталляции новых приложений или машин);
* отсутствие контроля вносимых изменений;
* отсутствие информации о внутренних угрозах безопасности;
* отсутствие информации о слабых местах различных методик аутентификации при организации мощной защиты.

Причинами появления уязвимостей в сетях могут быть:

* уязвимые зоны в поставляемом программном продукте;
* нарушение технологий передачи информации и управления;
* внедрение компонентов и программ, реализующих не декларированные функции и нарушающих нормальное функционирование сетей;
* невыполнение реализованными механизмами защиты сети заданных требований к процессу обеспечения информационной безопасности или предъявление непродуманного набора требований;
* использование не сертифицированных в соответствии с требованиями безопасности отечественных и зарубежных информационных технологий, средств информатизации и связи, а также средств защиты информации и контроля их эффективности.

В этих условиях обеспечение информационной безопасности сетей становится триединой задачей, включающей мониторинг функционирования, обнаружение атак и принятие адекватных мер противодействия.

Адекватные меры противодействия могут носить технический характер и предусматривать реконфигурацию информационной области сети. Они могут быть также организационными и предусматривать обращение операторов сетей связи к силовым структурам с предоставлением необходимой информации для выявления и привлечения к ответственности нарушителей.

Обеспечение информационной безопасности сетей, систем и средств связи означает создание процесса, которым необходимо постоянно управлять и который является неотъемлемой составной частью процесса функционирования компьютерных вычислительных устройств и сетей.

**Заключение.**

По итогу практики:

* Закрепил теоретические знания и получил навыки их практического применения.
* Ознакомился со спецификой деятельности системного администратора.
* Выполнил все поставленные задачи.