МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ХАБАРОВКОГО КРАЯ
Краевое государственное бюджетное профессиональное образовательное учреждение «Хабаровский техникум техносферной безопасности и промышленных технологий»

УТВЕРЖДАЮ
Директор КГБ ПОУ ХТТБПТ
_____ О.Б. Богданова
«01» сентября 2023 г.

Дополнительная профессиональная программа
повышения квалификации
«Корпоративная защита от внутренних угроз информационной безопасности с использованием современных VPN технологий»

г. Хабаровск
2023г.

Организация – разработчик: КГБ ПОУ ХТТБПТ

Разработчики:
Заведующий отделением К.В. Сташенко
Методист О.И. Дмитриева

Дата разработки: « » 2023 года

Дополнительная профессиональная программа повышения квалификации «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных VPN технологий» обсуждена и согласована на заседании научно-методического Совета КГБ ПОУ ХТТБПТ «___» _____ 2023 года

Протокол № _____

Содержание

1. Общие положения

Дополнительная профессиональная программа повышения квалификации «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных VPN технологий» разработана Краевым государственным бюджетным профессиональным образовательным учреждением «Хабаровский техникум техносферной безопасности и промышленных технологий» (далее КГБ ПОУ ХТТБПТ) в соответствии с требованиями:

– Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями);

– Федерального закона от 03.07.2016 № 238-ФЗ «О независимой оценке квалификации»;

– профессиональным стандартом «Специалист по безопасности компьютерных систем и сетей» (утвержден приказом Минтруда России от 1 ноября 2016 года N 598н);

– Приказа Министерства образования и науки Российской Федерации от 02.07.2013 г. № 513 «Об утверждении Перечня профессий рабочих, должностей служащих, по которым осуществляется профессиональное обучение»;

– Приказа Минобрнауки России, Минпросвещения России «Об организации и осуществлении образовательной деятельности при сетевой форме реализации образовательных программ» от 05.08.2020 № 882/391;

– положения о внутреннем распорядке обучающихся в КГБ ПОУ ХТТБПТ;

– положения о дополнительном профессиональном образовании в КГБ ПОУ ХТТБПТ;

– положения об итоговой аттестации по программам дополнительного профессионального образования;

– устава КГБ ПОУ ХТТБПТ.

К освоению программы допускаются лица, имеющие среднее профессиональное и (или) высшее образование. Медицинские ограничения регламентированы Перечнем медицинских противопоказаний Минздрава России.

Трудоемкость обучения: 144 академических часа. Для всех видов аудиторных занятий (лекции, практические занятия) устанавливается академический час продолжительностью 45 минут.

Форма обучения: очная или очная с применением дистанционных образовательных технологий.

Рабочие места, которые возможно занять по итогам обучения по программе (трудоустройство на вакансии в организации, самозанятость, работа в качестве индивидуального предпринимателя):

- администратор безопасности;
- специалист по защите информации;
- специалист по информационной безопасности;
- инженер по безопасности;
- офицер безопасности;
- специалист по защите персональных данных
- системный администратор;
- сетевой инженер;
- инженер технической поддержки;
- специалист по защите информации в компьютерных системах и сетях.

Программа рекомендуется к освоению лицами, имеющими среднее профессиональное и (или) высшее образование по следующим профессиям/специальностям/направлениям подготовки:

- информационные системы и технологии;
- информационная безопасность;
- информатика и вычислительная техника;
- информационная безопасность телекоммуникационных систем;

- инфокоммуникационные технологии и системы связи;

- компьютерные системы и комплексы;

- информационные системы и программирование.

Программа рекомендуется к освоению лицами, имеющими квалификацию и/или опыт профессиональной деятельности в области информационных технологий, сетевого администрирования, информационной безопасности.

1.1 Требования к результатам освоения программы

В результате освоения программы слушатель должен знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»;
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- общие положения об информационной безопасности для телекоммуникационных систем;
- организационно-технические и правовые основы использования электронного документооборота в информационных системах;
- структура виртуальной защищенной сети;
- назначение виртуальной защищенной сети. Особенности построения VPN-сетей; Основные типы классификаций VPN-сетей. VPN: определение, состав, характеристики, требования;
- технологии построения виртуальных защищенных сетей на основе программных и программно-аппаратных решений;
- основные компоненты системы защиты информации;
- система защиты информации ViPNet: общие сведения;
- технология ViPNet - концепция защиты и разграничения доступа;
- состав программного комплекса ViPNet (Administrator, Client, Coordinator);
- основные функции и возможности комплекса ViPNet;
- прикладные системы комплекса ViPNet;

- ключевую структуру сети ViPNet (ключевая система, формирование и управление ключевой системой);
- ЦУС и УКЦ: функции и условия их взаимодействия;
- формирование, модификация и межсетевое взаимодействие в сети ViPNet;
- функции ViPNet Coordinator. Первоначальные настройки в ЦУСе, логика взаимодействия сетевых узлов;
- логику обработки IP-трафика;
- настройку туннелирования на Координаторах;
- систему резервирования. Проверка работы кластера с туннелируемым ресурсом;
- типовые схемы применения ПО ViPNet.

В результате освоения программы слушатель должен уметь:

- правильно эксплуатировать системы и средства, предназначенные для эффективного функционирования комплексной системы защиты информации ViPNet в подразделениях организации;
- использовать методы и средства защиты данных ViPNet;
- планировать организационные мероприятия, проводимые при криптографической защите информации;
- устанавливать и настраивать средства защиты информации;
- администрировать системы защиты информации ViPNet;
- создавать и модифицировать защищенные сети по заданным схемам;
- организовывать межсетевое взаимодействие;
- организовывать взаимодействия всех объектов VPN между собой и функционирования туннеля;
- обеспечивать работу сервера защищенных соединений.

2. Содержание программы

2.1 Учебный план

№	Наименование модулей	Всего, ак.час.	В том числе			Форма контроля
			лекции	практ. занятия	промежут. и итог. контроль	
1	*2*	*3*	*4*	*5*	*6*	*7*
1.	Модуль 1. Актуальные требования рынка труда, современные технологии в профессиональной сфере	12	10	-	2	Тест
2.	Модуль 2. Требования охраны труда и техники безопасности	5	3	-	2	Тест
3.	Модуль 3. Практическое занятие на определение стартового уровня владения компетенцией	2		2		
4.	Модуль 4. Современные технологии VPN. Система защиты информации ViPNet.	58	29	27	2	Тест
5.	Модуль 5. Система VPN ViPNet. Особенности криптосистемы и ключевой структуры	10	4	4	2	Тест
6.	Модуль 6. Технологии анализа и защиты сетевого трафика. Организация межсетевого взаимодействия и туннелируемые ресурсы	49	14	33	2	Тест
7.	Итоговая аттестация (демонстрационный экзамен)	8	-	-	8	Экзамен
	ИТОГО:	**144**	**60**	**66**	**18**	

2.2. Учебно-тематический план

№	Наименование модулей	Всего, ак.час.	В том числе			Форма контроля
			лекции	практ. занятия	промежут. и итог. контроль	
1	*2*	*3*	*4*	*5*	*6*	*7*
1.	**Модуль 1. Актуальные требования рынка труда, современные технологии в профессиональной сфере**	**12**	**10**	**-**	**2**	**Тест**
1.1	Региональные меры содействия занятости в том числе поиска работы, осуществления индивидуальной предпринимательской деятельности, работы в качестве самозанятого	2	2	-	-	-
1.2	Актуальная ситуация на региональном рынке труда	2	2	-	-	-
1.3	Современные технологии в профессиональной сфере, соответствующей компетенции	6	6	-	-	-
1.4	Промежуточная аттестация	2	-	-	2	-
2.	**Модуль 2. Требования охраны труда и техники безопасности**	**5**	**3**	**-**	**2**	**Тест**
2.1	Требования охраны труда и техники безопасности	1,5	1,5	-	-	-
2.2	Специфичные требования охраны труда, техники безопасности и окружающей среды по компетенции	1,5	1,5	-	-	-

2.3	Промежуточная аттестация	2	-	-	2	Тест
3.	**Модуль 3. Практическое занятие на определение стартового уровня владения компетенцией**	**2**		**2**		
3.1.	Практическое занятие на определение стартового уровня владения компетенцией	2		2		Тест
4.	**Модуль 4. Современные технологии VPN. Система защиты информации ViPNet.**	**58**	**29**	**27**	**2**	**Тест**
4.1	Введение в технологию ViPNet	8	6	2	-	-
4.2	Компоненты управления сети ViPNet	12	6	6	-	-
4.3	Клиентские продукты ViPNet	10	6	5	-	-
4.4	Серверные продукты ViPNet	26	11	14	-	
4.5	Промежуточная аттестация	2	-	-	2	Тест
5.	**Модуль 5. Система VPN ViPNet. Особенности криптосистемы и ключевой структуры**	**10**	**4**	**4**	**2**	**Тест**
5.1	Ключевая структура сети ViPNet. Формирование и управление ключевой системой.	8	4	4	-	-
5.2	Промежуточная аттестация	2	-	-	2	Тест

6.	**Модуль 6. Технологии анализа и защиты сетевого трафика. Организация межсетевого взаимодействия и туннелируемые ресурсы**	**49**	**14**	**33**	**2**	**Тест**
6.1	Выполнение конкурсного задания по компетенции	37	14	23	-	-
6.2	Организация оценки конкурсного задания по компетенции	10	-	10	-	-
6.3	Промежуточная аттестация	2	-	-	2	-
7.	**Итоговая аттестация**	**8**	**-**	**-**	**8**	**Экзамен**
7.1	Демонстрационный экзамен по компетенции	8	-	-	8	ДЭ
	ИТОГО:	**144**	**60**	**66**	**18**	

2.3. Учебная программа

Модуль1. Актуальные требования рынка труда, современные технологии в профессиональной сфере

Тема 1.1. Региональные меры содействия занятости в том числе поиска работы, осуществления индивидуальной предпринимательской деятельности, работы в качестве самозанятого

Лекция:

1. Региональные меры содействия занятости в том числе поиска работы, осуществления индивидуальной предпринимательской деятельности, работы в качестве самозанятого

Тема 1.2. Актуальная ситуация на региональном рынке труда

Лекция:

1. Актуальная ситуация на региональном рынке труда

Тема 1.3. Современные технологии в профессиональной сфере. Основы защиты информации.

Лекция:

1. Актуальность защиты сведений ограниченного доступа.

2. Ответственность за правонарушения в области защиты информации.

3. Методы и средства защиты конфиденциальной информации. Криптографическая защита информации. Технология построения VPN. Межсетевое экранирование. Контроль и управление доступом. Защита информации от утечек по техническим каналам.

4. Средства защиты информации: технические, программные, организационные.

5. Организационно-правовые основы обеспечения защиты информации в РФ.

6. Ключевые алгоритмы и системы (симметричное шифрование, асимметричное шифрование, технология электронной подписи, технология построения VPN).

Модуль 2. Требования охраны труда и техники безопасности

Тема 2.1 Культура безопасного труда.

Лекция (вопросы, выносимые на занятие):

1. Негативные факторы при работе за компьютером.

2. Правила работы за компьютером.

3. Правила организации рабочего места.

4. Культура безопасного труда. Забота о здоровье во время работы за компьютером.

Тема 2.2 Основы безопасного труда и эффективная организация рабочего места.

Лекция (вопросы, выносимые на занятие):

1. Инфраструктурный лист. Схема и оборудование рабочих мест. Требования к технике безопасности на чемпионате по компетенции

«Корпоративная защита от внутренних угроз информационной безопасности».

Модуль 3. Практическое занятие на определение стартового уровня владения компетенцией

Тема 3.1. Практическое занятие на определение стартового уровня владения компетенцией

Практическое занятие, форма проведения: входное тестирование.

Вопросы:

1. Какие способы и средства защиты информации Вы знаете?

- *организационные, технические, криптографические.
- организационно-технические и инженерные.
- технические и экономические.
- организационные, технические, экономические.

2. Какие виды ответственности предусмотрены за нарушение Федеральных законов в сфере ЗИ?

- гражданско-правовая и личная.
- административная и уголовная.
- *гражданско-правовая, административная, уголовная.
- только личная ответственность.

3. Что такое головной УЦ?

- УЦ, который заверяет сертификат всем пользователям в сети
- *УЦ, который находится на вершине иерархической структуры доверительных отношений между УЦ и раздает права подчиненным УЦ
- УЦ, который использует самоподписанный сертификат
- УЦ, который выпускает кросс-сертификаты

4. Что такое точка распространения данных:

- сервер куда помещаются CRL
- путь, где размещаются сертификаты

- *Источник, доступный по общеизвестным протоколам (LDAP, FTP), используемый для размещения сертификатов и списков отозванных сертификатов
- нет правильных ответов

5. Назовите угрозы несанкционированного доступа:

- утечка акустической информации, утечка видовой информации.
- внедрение вредоносных программ.
- *перехват паролей, модификация BIOS, перехват управлением загрузки, внедрение вредоносных программ.
- перехват паролей, утечка по каналу ПЭМИН.

6. Какая технология, применяемая в продуктах VPN ViPNet, обеспечивает сокрытие информации о IP-пакете при передаче его по открытой сети?

- Технология межсетевого экранирования
- Технология хеширования
- *Технология туннелирования и инкапсуляции
- Технология аутентификации

7. Может ли ViPNet работать через VPN-каналы, организованные с помощью СЗИ других производителей?

- *Да, может
- Да, но информация будет передаваться в открытом виде
- Нет, это нарушает целостность системы защиты
- Нет, ViPNet работает только через VPN-каналы, организованные с помощью технологии VPN ViPNet

8. После установки ViPNet Client была потеряна связь с узлами локальной сети. Что необходимо сделать для восстановления соединения с узлами сети?

- В фильтрах Закрытой сети добавить разрешающее правило для ip-адресов.
- Перезагрузить ViPNet Client.

- *Настроить Межсетевой экран ViPNet Client на пропуск пакетов от узлов сети.
- Настроить транспортный модуль MFTP своего узла на передачу и пропуск пакетов от узлов сети.

9. Что такое головной УЦ?

- УЦ, который заверяет сертификат всем пользователям в сети
- *УЦ, который находится на вершине иерахической структуры доверительных отношений между УЦ и раздает права подчиненным УЦ
- УЦ, который использует самоподписанный сертификат
- УЦ, который выпускает кросс-сертификаты

10. В каком режиме загружается элемент кластера горячего резервирования после перезагрузки ОС?

- Всегда в активном режиме
- *Всегда в пассивном режиме
- Необходимо ручное указание режима после полной загрузки ПО ViPNet
- Устанавливается режим, выбранный до перезагрузки ОС

11. Назовите обязательные компоненты для построения защищённой сети на основе технологии ViPNet:

- *ViPNet Administrator, ViPNet Coordinator, ViPNet Client
- ViPNet Administrator, ViPNet Policy Manager, ViPNet Coordinator, ViPNet Client
- ViPNet Administrator, ViPNet Certification Authority, ViPNet Client
- ViPNet Administrator, ViPNet Coordinator, ViPNet CryptoFile

12. Какие сетевые фильтры обладают максимальным приоритетом?

- * Фильтры, определенные специальными конфигурациями
- Фильтры политик безопасности из Policy Manager
- Фильтры по умолчанию и фильтры, заданные пользователем
- Среди перечисленных вариантов ответов нет правильного

13. В какой программе задается количество туннелируемых узлов для координатора?

- * В ViPNet Центр управления сетью
- В ViPNet Удостоверяющий и ключевой центр
- В ViPNet Policy Manager
- В ViPNet Coordinator

14. Где содержится информация об объектах сети ViPNet (узлах, пользователях, их именах, идентификаторах, адресах, связях и т.д.)?

- * В справочниках
- В файле "Ключи пользователя"
- В сертификате ключа подписи
- В файле "Ключи узла"

15. Использование ViPNet IDS в локальной сети возможно:

- * все перечисленные варианты возможны
- до сетевого экрана
- после сетевого экрана
- после координатора ViPNet

16. Какие сетевые интерфейсы ViPNet IDS не нуждаются в настройке IP-адресов?

- * предназначенные для захвата сетевого трафика
- управляющие
- все нуждаются
- ни один не нуждается

17. В списке узлов защищенной сети программы ViPNet Монитор напротив некоторых из узлов не стоит номер сети. Это ошибка?

- * Нет, номер сети указывается только для "чужих" сетей, с которыми установлено межсетевое взаимодействие
- Нет, наличие номера сети в названии узла зависит от псевдонима этого СУ
- Да, обновления справочников на этом узле прошли некорректно

- Да, нарушена целостность справочников ViPNet этого узла

18. Нужно ли пересоздавать ключи узла при смене имени сетевого узла?

- * Нет, т.к. ключевая информация не изменилась.
- Да
- Нужно, если меняется имя узла и имя пользователя
- Да, но только при первой смене имени

19. Какие настройки нужно сделать при установке ПО ViPNet Client на туннелируемый компьютер?

- * Исключить IP-адрес из туннелируемых адресов
- Ничего делать не нужно, ViPNet автоматически сделает все замены
- Нужно прописать IP-адреса данного Клиента на других узлах
- Отключить защиту на данном ViPNet Client

20. Пароль Администратора ViPNet xFirewall формируется:

- * в программе ViPNet Administrator (Удостоверяющий и ключевой центр)
- в программе ViPNet Administrator (Центр управления сетью)
- непосредственно на ПАК ViPNet xFirewall в процессе распаковки дистрибутива ключей
- в программе ViPNet Policy Manager

Модуль 4 Современные технологии VPN. Система защиты информации ViPNet.

Тема 4.1 Введение в технологию ViPNet

Лекция (вопросы, выносимые на занятие):

1. История развития группы компаний «ИнфоТеКС». История развития продуктовой линейки ViPNet.

2. Технологии защиты конфиденциальной информации. Понятие VPN. Архитектура виртуальных защищённых сетей. Туннелирование и инкапсуляция трафика.

3. Основа технологии ViPNet – драйвер ViPNet. Принцип работы драйвера.

1. Модули защищённой сети ViPNet. Объекты защищённой сети ViPNet (сетевой узел, группа сетевых узлов, пользователь). Роли сетевых узлов и полномочия пользователей ViPNet. Разграничение доступа к конфиденциальной информации.

4. Лицензирование сети ViPNet. Идентификаторы объектов сети ViPNet.

Практическое занятие. План проведения занятия:

1. Установка ViPNet Administrator:

a. Установка серверного приложения ViPNet Центр управления сетью;

b. Установка клиентского приложения ViPNet Центр управления сетью;

c. Установка ViPNet Удостоверяющий и ключевой центр.

2. Первый запуск программы ViPNet Центр управления сетью. Загрузка лицензии на сеть ViPNet.

Тема 4.2 Компоненты управления сети ViPNet

Лекция (вопросы, выносимые на занятие):

2. Общие сведения, основные функции и назначение программы ViPNet Administrator.

3. Состав программного обеспечения ViPNet Administrator. ViPNet Центр управления сетью и ViPNet Удостоверяющий ключевой центр. База данных SQL-сервера.

4. Особенности взаимодействия ЦУС и УКЦ.

5. Система управления политиками безопасности ViPNet Policy Manager. Ролевая модель доступа. Полномочия пользователей в ViPNet Policy Manager. Работа с шаблонами политик безопасности защищённой сети.

Практическое занятие. План проведения занятия:

1. Формирование топологии защищённой сети в ПО ViPNet Центр управления сетью:

a. Создание координаторов.

b. Создание клиентов.

c. Создание межсерверных каналов и связей между пользователями.

d. Первичная инициализация ViPNet Удостоверяющего и ключевого центра.

e. Выдача дистрибутивов ключей пользователям защищённой сети.

f. Развёртывание ПО ViPNet Client на рабочем месте администратора защищённой сети.

g. Создание резервной копии ViPNet Administrator в ручном режиме. Настройка автоматического резервного копирования.

h. Развёртывание рабочего места помощника главного администратора. Проверка связи между сетевыми узлами главного администратора и помощника главного администратора.

i. Миграция ПО ViPNet Administrator.

j. Сохранение отчёта о структуре сети ViPNet в файл.

k. Настройка минимальных полномочий пользователей в сети ViPNet.

Тема 4.3 Клиентские продукты ViPNet

Лекция (вопросы, выносимые на занятие):

1. ViPNet Client – защита АРМ пользователя при работе в виртуальной частной сети ViPNet. Функции ViPNet Client, состав программного обеспечения.

2. Режимы установки ПО ViPNet Client и требования к системе. Интерактивная установка программного обеспечения. Аутентификация в ПО ViPNet Client.

3. Элементы интерфейса ПО ViPNet Client.

4. Настройки программы ViPNet Client (общие настройки, настройка дополнительных параметров, настройка обработки прикладных

протоколов, настройка параметров блокировки трафика, выбор сервера IP-адресов), настройка параметров подключения к сети, настройка параметров безопасности, настройка доступа к защищённым узлам).

5. Настройка сетевого экрана в ПО ViPNet Client. Использование групп объектов. Принципы фильтрации трафика. Создание правил фильтрации.

6. Работа с журналами в ПО ViPNet Client. Просмотр статистики IP-пакетов. Журнал IP-пакетов. Создание сетевого фильтра из журнала IP-пакетов.

7. Работа в ПО ViPNet Client с правами администратора сетевого узла.

8. Компоненты ПО ViPNet Client, их функции: ViPNet Контроль приложений, транспортный модуль ViPNet MFTP, система обновлений ViPNet.

9. Встроенные средства коммуникации ViPNet (обмен защищёнными сообщениями, файловый обмен, конференция).

10. Защита электронного документооборота с использованием ПО ViPNet Деловая почта. Функции и возможности программы. Настройки программы. Создание и просмотр писем. Автопроцессинг писем и файлов в ПО ViPNet Деловая почта.

11. Настройка архивации писем в ПО ViPNet Деловая почта.

12. Клиентские продукты ViPNet для защиты рабочих станций и мобильных устройств. Терминальный клиент ПАК ViPNet Terminal. ViPNet PKI Client – универсальный клиент для работы в инфраструктуре открытых ключей.

Практическое занятие. План проведения занятия:

1. Создание защищённой сети, состоящей из трёх сетевых узлов согласно схеме (главный администратор и два клиента).

2. Установка прямого взаимодействия между двумя сетевыми узлами по каналу MFTP.

3. Настройка автопроцессинга в программе ViPNet Деловая почта.

4. Ручная установка обновлений ключей и справочников на клиентах.

5. Дополнительно:

a. Блокировка IP-пакетов, передаваемых по протоколу ICMP;

b. Создание пропускающего фильтра для пакетов, передаваемых по протоколу RDP.

Тема 4.4 Серверные продукты ViPNet

Лекция (вопросы, выносимые на занятие):

1. Общие сведения, основные функции и назначение программы ViPNet Coordinator.

a. Назначение и состав программного комплекса ViPNet Coordinator. Назначение отдельных модулей (подпрограмм).

b. Функции ViPNet Coordinator: сервер IP-адресов, сервер-маршрутизатор, VPN-шлюз, межсетевой экран, защищённый интернет-шлюз, маршрутизатор VPN-пакетов.

c. Интерфейс программы. Структура каталога установки. Порядок лицензирования ViPNet Coordinator.

2. Логика взаимодействия Клиентов с Координаторами и координаторов между собой.

3. Общие сведения и принцип работы ViPNet Coordinator как сервера – маршрутизатора и межсетевого экрана.

a. Принципы работы ViPNet Coordinator как сервера – маршрутизатора. Организация межсерверных каналов. Транспортный модуль MFTP.

b. ViPNet Coordinator как межсетевой экран. Принципы фильтрации IP-трафика в ViPNet Coordinator. Антиспуфинг. Трансляция сетевых адресов.

4. Функция туннелирования открытого трафика локальной сети. Настройка туннеля и полутуннеля.

a. Технология туннелирования. Настройка туннеля и полутуннеля в ViPNet Coordinator. Основные схемы применения.

5. Назначение системы защиты от сбоев. Одиночный режим работы. Режим работы кластера горячего резервирования (ViPNet Failover).

6. Правила формирования виртуальных адресов. Назначение виртуальных IP-адресов. Правила формирования виртуальных IP-адресов. Стартовый виртуальный IP-адрес. Обработка виртуальных IP-адресов при передаче пакета по сети.

Практическое занятие. План проведения занятия:

1. Настройка локальных фильтров открытой сети.
2. Настройка транзитных фильтров открытой сети.
3. Настройка фильтров защищенной сети.
4. Настройка трансляции адресов (NAT).
5. Настройка туннелирования в ViPNet Coordinator: полутуннель, туннель.
6. Дополнительное задание: настройка антиспуфинга, настройка TCP-туннеля.

Модуль 5 Система VPN ViPNet. Особенности криптосистемы и ключевой структуры

Тема 5.1 Ключевая структура сети ViPNet. формирование и управление ключевой системой

Лекция (вопросы, выносимые на занятие):

1. Назначение криптографических функций.
2. Шифрование в технологии ViPNet. Использование симметричных и асимметричных алгоритмов шифрования. Проблема распределения симметричных ключей и алгоритм Диффи-Хеллмана. Поддерживаемые криптографические стандарты.
3. Виды шифрования в ViPNet. Типы ключей в системе ViPNet. Мастер-ключи. Виды симметричных ключей: ключи обмена, ключи защиты ключей обмена, персональные ключи, парольные ключи. Многоуровневая

защита ключевой информации в ViPNet. Дистрибутив ключей, ключи узла и ключи пользователя: формирование, состав, назначение, смена ключей.

4. Резервный набор персональных ключей. Компрометация ключей в системе ViPNet. Действия пользователя и администратора защищенной сети в случае компрометации ключей. Компрометация ключей администратора Удостоверяющего и ключевого центра.

5. Электронная подпись в технологии ViPNet. Процедуры формирования и проверки электронной подписи. Сертификат ключа проверки электронной подписи в системе ViPNet, его использование. Список отозванных сертификатов.

6. Требования регуляторов по эксплуатации СКЗИ. Основные документы, регламентирующие деятельность организации при эксплуатации СКЗИ. Мероприятия по организации эксплуатации СКЗИ. Типовые формы документов.

7. Криптопровайдер ViPNet CSP 4.x.

Практическое занятие. План проведения занятия:

1. Модификация защищённой сети ViPNet: добавление сетевого узла, создание групп узлов, добавление нового пользователя, удаление связей пользователей, изменение названия сетевого узла, изменение имени пользователя, удаление пользователя, удаление сетевого узла, смена пароля администратора УКЦ, смена мастер-ключей, формирование нового сертификата ключа проверки электронной подписи, обновление программного обеспечения на узлах.

2. Компрометация ключей пользователя.

3. Настройка политик безопасности в ПО ViPNet Policy Manager:

a. Установка ViPNet Policy Manager.

b. Создание подразделений в ПО ViPNet Policy Manager.

c. Создание политики безопасности, ограничивающей доступ работников компании к социальным сетям.

d. Создание политики безопасности, блокирующей весь открытый трафик на рабочем месте сотрудника.

4. Дополнительно: настройка автоматического режима работы ViPNet Удостоверяющий и ключевой центр.

Модуль 6 Технологии анализа и защиты сетевого трафика. Организация межсетевого взаимодействия и туннелированные ресурсы

Тема 6.1 Выполнение конкурсного задания по компетенции

Лекция (вопросы, выносимые на занятие):

1. Межсетевое взаимодействие защищённых сетей ViPNet.
2. Программно-аппаратный комплекс ПАК ViPNet HW.
3. Программно-аппаратный комплекс ViPNet IDS.
4. Программно-аппаратный комплекс ViPNet xFirewall.

Практическое занятие. План проведения занятия:

1. Межсетевое взаимодействие защищённых сетей ViPNet:

a. Установка ПО ViPNet Coordinator в защищённой сети.

b. Развёртывание партнёрской защищённой сети.

c. Первоначальная настройка межсетевого взаимодействия с использованием индивидуального симметричного межсетевого мастер-ключа.

d. Модификация межсетевого взаимодействия (установление связей между пользователями доверенных сетей, удаление связей между пользователями доверенных сетей, прекращение межсетевого взаимодействия).

2. Туннелирование в рамках межсетевого взаимодействия защищённых сетей ViPNet.

a. Подключение по одному незащищенному рабочему месту к защищённым сетям, участвующим в межсетевом взаимодействии.

b. Проверка доступности «своего» координатора с каждой из незащищённых машин командой ping.

c. Настройки туннелирующих координаторов.

d. Проверка доступности незащищённых машин друг другу командой ping.

3. Администрирование программно-аппаратного комплекса ПАК ViPNet IDS:

a. Подготовка и эксплуатация сетевого сенсора системы обнаружения атак ПАК ViPNet IDS NS.

b. Анализ данных в ViPNet IDS NS.

c. Настройка обнаружения угроз информационной безопасности.

d. Настройка сетевого трафика и порядок работы с ним.

e. Мониторинг, поиск и анализ событий информационной безопасности. Создание статистических отчетов.

f. Управление и настройка ViPNet IDS NS через веб-интерфейс.

g. Управление и настройка ViPNet IDS NS с помощью консоли.

h. Аудит ViPNet IDS NS.

4. Работа с ПАК ViPNet xFirewall: настройки правил фильтрации, просмотр журнала IP-пакетов.

Тема 6.2 Организация оценки конкурсного задания по компетенции

Лекция (вопросы, выносимые на занятие):

1. Организация оценки конкурсного задания по компетенции

Практическое занятие. План проведения занятия:

1. Оценивание конкурсного задания по компетенции.

3. Организационно-педагогические условия реализации программы

Для реализации учебного процесса в КГБ ПОУ ХТТБПТ имеются учебные классы, оснащённые необходимыми материально-техническими средствами для проведения занятий различных форм, оборудованные аудиовизуальными техническими средствами с учетом современных требований к образовательному процессу.

3.1 Материально-технические условия реализации программы

Наименование помещения	Вид занятий	Наименование оборудования, программного обеспечения
1	*2*	*3*
Аудитория	Лекции	Компьютер, мультимедийный проектор, экран, доска, флипчарт
Лаборатория, компьютерный класс	Лабораторные и практические занятия, тестирование, демонстрационный экзамен	Оборудование, оснащение рабочих мест, инструменты и расходные материалы.

3.2 Учебно-методическое обеспечение программы

- техническое описание компетенции;
- комплект оценочной документации по компетенции;
- печатные раздаточные материалы для слушателей;
- учебные пособия, изданных по отдельным разделам программы;
- профильная литература;
- отраслевые и другие нормативные документы;
- электронные ресурсы.

4. Оценка качества освоения программы

Промежуточная аттестация по программе предназначена для оценки освоения слушателем модулей программы и проводится в виде зачетов и (или) экзаменов. По результатам любого из видов итоговых промежуточных испытаний выставляются отметки по двухбалльной системе: «удовлетворительно» («зачтено»), «неудовлетворительно» («не зачтено») или четырехбалльной системе: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Итоговая аттестация осуществляется в виде экзамена или в иной форме, разработанной ведущим преподавателем. Лица, успешно освоившие программу и успешно прошедшие итоговую аттестацию, получают удостоверение о повышении квалификации установленного образца. Решение об аттестации слушателя принимается аттестационной комиссией при проверке знаний.