Министерство профессионального образования
и занятости населения Приморского края
КРАЕВОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ДАЛЬНЕВОСТОЧНЫЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ»
(КГА ПОУ «ДВТК»)

СОГЛАСОВАНО
Зам.директора по учебно-
методической и научной работе
_____Е.Н. Сухорукова
«_6_» _сентября_2023 г.

УТВЕРЖДАЮ
Директор КГА ПОУ «ДВТК»
_____Ю.И. Романько
«_8_» _сентября_2025 г.

ПРОГРАММА ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ
Корпоративная защита от внутренних угроз информационной безопасности (VPN технологии)
(наименование программы)

повышение квалификации

Составитель:
Косиенко О. А., методист КГА ПОУ «Дальневосточный технический колледж»

ПРОГРАММА ПРОФЕССИОНАЛЬНАЯ ОБУЧЕНИЯ
Корпоративная защита от внутренних угроз информационной безопасности (VPN технологии)
повышения квалификации

1. Цели реализации программы

Программа повышения квалификации по профессиям рабочих, должностям служащих направлена на обучение лиц, уже имеющих профессию рабочего, профессии рабочих или должность служащего, должности служащих, в целях последовательного совершенствования профессиональных знаний, умений и навыков по имеющейся профессии рабочего или имеющейся должности служащего без повышения образовательного уровня

2. Требования к результатам обучения. Планируемые результаты обучения

2.1. Характеристика нового вида профессиональной деятельности, трудовых функций и (или) уровней квалификации

Программа разработана в соответствии с:

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

Для лиц с ограниченными возможностями здоровья и лиц с инвалидностью разрабатывается индивидуальный план освоения программы

Присваиваемый квалификационный разряд (категория): не предусмотрено.

2.2. Требования к результатам освоения программы

В результате освоения дополнительной профессиональной программы у слушателя должны быть сформированы компетенции, в соответствии с разделом 2.1. 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;
- ключевая структура 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;
- логика обработки IP-трафика;
- настройка туннелирования на Координаторах;
- система резервирования. Проверка работы кластера с туннелируемым ресурсом;
- типовые схемы применения ПО ViPNet.

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

3. Содержание программы

Категория слушателей: лица, имеющие или получающие среднее профессиональное и (или) высшее образование.

Трудоемкость обучения: 72 академических часа.

Форма обучения: очная или очная с применением дистанционных образовательных технологий

3.1. 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. Требования охраны труда и техники безопасности	2	2	-	-	-
2.	Модуль 2. Основы цифровой гигиены	13	6	6	1	зачет
3.	Модуль 3. Современные технологии VPN. Система защиты информации VipNET.	22	9	12	1	зачет

4.	Модуль 4. Система VPN VipNET. Особенности криптосистемы и ключевой структуры	12	4	7	1	зачет
5.	Модуль 5. Технологии анализа и защиты сетевого трафика. Организация межсетевого взаимодействия и туннелированные ресурсы	15	4	10	1	зачет
6.	Итоговая аттестация (квалификационный экзамен)	8	-	-	8	
	ИТОГО:	**72**	25	35	12	

3.2. 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. Требования охраны труда и техники безопасности**	**2**	**2**	**-**	**-**	**-**
1.1	Требования охраны труда и техники безопасности	1	1	-	-	-
1.2	Специфичные требования охраны труда, техники безопасности и окружающей среды	1	1	-	-	-

2.	**Модуль 2. Основы цифровой гигиены**	**13**	**6**	**6**	**1**	**Зачет**
2.1	Цифровая гигиена.	4	2	2	-	-
2.2	Правила безопасного поведения в сети Интернет.	4	2	2	-	-
2.3	Программы защиты от вредоносного программного кода.	4	2	2	-	-
2.4	Промежуточный контроль	1	-	-	1	Зачет
3.	**Модуль 3. Современные технологии VPN. Система защиты информации VipNET.**	**22**	**9**	**12**	**1**	**Зачет**
3.1	Введение в технологию VipNET	7	3	4	-	-
3.2	Компоненты управления сети VipNET	6	2	4	-	-
3.3	Клиентские продукты VipNET	4	2	2	-	-
3.4	Серверные продукты VipNET	4	2	2	-	-
3.5	Промежуточный контроль	1	-	-	1	Зачет
4	**Модуль 4. Система VPN VipNET. Особенности криптосистемы и ключевой структуры**	**12**	**4**	**7**	**1**	**Зачет**

4.1	Основы инфраструктуры открытых ключей. Цифровые ключи и сертификаты.	5	2	3	-	-
4.2	Ключевая структура сети ViPNet. формирование и управление ключевой системой	6	2	4	-	-
4.3	Промежуточный контроль	1	-	-	1	Зачет
5	**Модуль 5. Технологии анализа и защиты сетевого трафика. Организация межсетевого взаимодействия и туннелированные ресурсы**	**15**	**4**	**10**	1	**Зачет**
5.1	Технологии анализа и защиты сетевого трафика. Организация межсетевого взаимодействия и туннелированные ресурсы	14	4	10	-	-
5.2	Промежуточный контроль	1	-	-	1	Зачет
6.	**Итоговая аттестация**	**8**	**-**	**-**	**8**	
	ИТОГО:	**72**	**25**	**35**	**12**	

3.3. Учебная программа

Модуль 1 Требования охраны труда и техники безопасности.

Тема 1.1 Культура безопасного труда.

Лекция. Культура безопасного труда

Тема 1.2 Специфичные требования охраны труда, техники безопасности и окружающей среды .

Лекция. Основы безопасного труда и эффективная организация рабочего места.

Модуль 2 Основы цифровой гигиены

Тема 2.1 Цифровая гигиена.

Лекция и практические занятия. Киберугрозы. Виды киберугроз. Интернет угрозы. Внешние (вредоносный программный код, спам, фишинг, сетевые атаки, взлом устройства, взлом аккаунтов и т.д.) и внутренние (интернет зависимость, интернет прокрастинация) интернет угрозы. Коммуникационные и технологические интернет угрозы.

Тема 2.2 Правила безопасного поведения в сети Интернет.

Лекция и практические занятия. Размещение и использование персональных и личных данных. Безопасные пароли. Настройки приватности в социальных сетях. Резервное копирование.

Тема 2.3 Программы защиты от вредоносного программного кода.

Лекция и практические занятия. Программы родительского контроля. Средства шифрования данных. Средства блокирования нежелательного контента.

Промежуточный контроль

Модуль 3 Современные технологии VPN. Система защиты информации VipNET.

Тема 3.1 Введение в технологию VipNET

Лекция и практические занятия. Основные функциональные возможности. Типовой порядок первичной конфигурации сети ViPNet. Подсистема адресной администрации сети. Подсистема прикладной администрации сети. Управление сетью.

Тема 3.2 Компоненты управления сети VipNET

Лекция и практические занятия. Лицензионное ограничение.Системные требования. Варианты развертывания. Выбор необходимого дополнительного программного обеспечения ViPNet. Ключевая структура ViPNet. Формирование ключевой информации в ViPNet. Обновление мастер-ключей в сети ViPNet.

Тема 3.3 Клиентские продукты VipNET

Лекция и практические занятия. . Назначение ПО ViPNet Client. Функции ПО ViPNet Client. Состав ПО ViPNet Client. ViPNet Монитор. Модули: ViPNet MFTP (Client). ViPNet Контроль приложений. Модули: ViPNet Деловая почта

Тема 3.4 Серверные продукты VipNET

Лекция и практические занятия. Назначение ПО ViPNet Coordinator. Состав ПО ViPNet Coordinator. ViPNet-драйвер. Принцип работы ViPNet-драйвера. ViPNet Монитор. ViPNet MFTP. ViPNet Контроль приложений. Функции координатора в защищенной сети ViPNet Сервер-маршрутизатор. Маршрутизатор VPN-пакетов. Сервер IP-адресов. Межсетевой экран. Туннелирование. NAT-сервер. Сервер Открытого Интернета. Принципы осуществления соединений в сети ViPNet. Виртуальные IP-адреса Назначение технологии виртуальных IP-адресов. Практические сценарии использования координатора. Использование DHCP-сервера в сети ViPNet. Организация DMZ. ViPNet Coordinator (Linux). Система защиты от сбоев

Промежуточный контроль

Модуль 4 Система VPN VipNET. Особенности криптосистемы и ключевой структуры

Тема 4.1 Основы инфраструктуры открытых ключей. Цифровые ключи и сертификаты.

Лекция и практические занятия. Формат сертификата открытого ключа, характеристика обязательных и опциональных полей сертификата, ограничивающие и информационные дополнения сертификата, альтернативные форматы сертификатов, принципы функционирования простой инфраструктуры открытых ключей, систем PGP и SET, атрибутные сертификаты.

Тема 4.2 Ключевая структура сети ViPNet.

Лекция и практические занятия. Формирование и управление ключевой системой

Промежуточный контроль

Модуль 5 Технологии анализа и защиты сетевого трафика. Организация межсетевого взаимодействия и туннелированные ресурсы

Тема 5. 1 Технологии анализа и защиты сетевого трафика.

Организация межсетевого взаимодействия и туннелированные ресурсы

Промежуточный контроль

3.4. Календарный учебный график (порядок освоения модулей)

Период обучения (недели)*	Наименование модуля
1 неделя	Модуль 1. Требования охраны труда и техники безопасности. Модуль 2. Основы цифровой гигиены
2 неделя	Модуль 3. Современные технологии VPN. Система защиты информации VipNET.
3 неделя	Модуль 4. Система VPN VipNET. Особенности криптосистемы и ключевой структуры
4 неделя	Модуль 5. Технологии анализа и защиты сетевого трафика. Организация межсетевого взаимодействия и туннелированные ресурсы
	Итоговая аттестация
*-Точный порядок реализации модулей (дисциплин) обучения определяется в расписании занятий.	

4. Организационно-педагогические условия реализации программы

4.1. Материально-технические условия реализации программы

Наименование специализированных аудиторий, кабинетов, мастерских, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
Учебный кабинет (аудитория)	Лекции	комплект учебно-методической документации (учебники и учебные пособия, сборники задач и упражнений, карточки-задания, комплекты тестовых заданий); комплекты инструкционно-технологических карт и бланков технологической документации;

		наглядные пособия (плакаты, в том числе электронные, демонстрационные и электрифицированные стенды, макеты и действующие устройства);
Образовательно-производственный центр "Строительство", зона под вид работ «Информационные кабельные сети»	Практические занятия (лабораторные работы)	комплект деталей, кабелей, инструментов и приспособлений.
Компьютерный класс	Практические и лабораторные занятия	Компьютеры, сетевое оборудование

4.2 Учебно-методическое обеспечение программы

1. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2020.

2. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2019. – 224 с.

3. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. - СПб.: Питер, 2021 - 703 с.

4. ГубенковА.А.Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2020. - 88 с.

5. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы – М.: Бином, 2021. – 1024 с.

6. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бином, 2021. –704 с.

7. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник.-М.: Горячая линия-Телеком., 2019

8. Кофлер М., Linux. Полное руководство – Питер, 2011. – 800 с.9. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2020

10. Лапонина О.Р. Основы сетевой безопасности: криптографическиеалгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.-М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2020.- 531 с.

11. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2020. – 656 с.

12. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2020.- 147 с.

13. Мельников Д. Информационная безопасность открытых систем.-М.: Форум, 2020.

14. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб. пос. для студентов СПО – М.: Форум, 2019. – 544 с.

15. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. – М.: Академия, 2019. – 240 с.

16. Руссинович М., Соломон Д., Внутреннее устройство MicrosoftWindows. Основные подсистемы операционной системы – Питер, 2021. – 672 с.

17. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008. – 368 с.

18. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2021.

19. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2021.

5 Оценка качества освоения программы

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

Итоговая аттестация проводится в форме квалификационного экзамена, который включает в себя практическую квалификационную работу (в форме демонстрационного экзамена) и проверку теоретических знаний (тестирование).