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_2023 г.

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

повышение квалификации

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

Программа профессионального обучения
Корпоративная защита от внутренних угроз информационной безопасности
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);

Программа повышения квалификации направлена на совершенствование и (или) формирование у слушателей новой компетенции: осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLP IWTM

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;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;

- основные функции системы DLP IWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;
- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;
- технику безопасности и экологию производства.

уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLP IWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

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

1.1. 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. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	2	2	-	-	-
2.	Модуль 2. Исследование (аудит) организации с целью защиты от внутренних угроз	9	4	4	1	зачет

3.	Модуль 3. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	13	4	8	1	зачет
4.	Модуль 4. Технологии анализа и защиты сетевого трафика	14	4	9	1	зачет
5.	Модуль 5. Технологии агентского мониторинга	17	6	10	1	зачет
6.	Модуль 6. Анализ выявленных инцидентов	9	2	6	1	зачет
7.	Итоговая аттестация (Квалификационный экзамен)	8	-	-	8	
	ИТОГО:	**72**	**22**	**37**	**13**	

3.1. 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. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз**	**2**	**2**	**-**	**-**	**-**
1.1	Конфигурация сетевой инфраструктуры	1	1	-	-	-
1.2	Установка и настройка системы корпоративной	1	1	-	-	-

	защиты от внутренних угроз					
2.	**Модуль 2. Исследование (аудит) организации с целью защиты от внутренних угроз**	**9**	**4**	**4**	**1**	**-**
2.1	Угрозы информационной безопасности	2	2	-	-	-
2.2	Модели угроз	3	1	2	-	-
2.3	Нормативно -правовые документы организации по легальному применению корпоративной защиты от внутренних угроз информационной безопасности .	3	1	2	-	-
2.4	Промежуточная аттестация	1	-	-	1	Зачет
3.	**Модуль 3. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз**	**13**	**4**	**8**	**1**	**-**
3.1	Политика безопасности	5	2	3	-	-
3.2	Технологии защиты: печатей, бланков, графических объектов, баз данных	5	2	3	-	-
3.3	Работа с интерфейсом управления системы	2	-	2	-	-

	корпоративной защиты информации .					
3.4	Промежуточная аттестация	1	-	-	1	Зачет
4.	**Модуль 4. Технологии анализа и защиты сетевого трафика**	**14**	**4**	**9**	**1**	**-**
4.1	Технологии анализа и защиты сетевого трафика .	7	2	5	-	
4.2	Межсетевое взаимодействие и туннелированные.	6	2	4	-	
4.3	Промежуточная аттестация	1	-	-	1	Зачет
5.	**Модуль 5. Технологии агентского мониторинга**	**17**	**6**	**10**	**1**	**-**
5.1	Технологии агентского мониторинга.	10	4	6	-	-
5.2	Работа с исключениями из перехвата	6	2	4	-	-
5.3	Промежуточная аттестация	1	-	-	1	Зачет
6.	**Модуль 6. Анализ выявленных инцидентов**	**9**	**2**	**6**	**1**	**-**
6.1	Классификацию уровня угроз инцидентов	2	2		-	-
6.2	Законодательство в области защиты конфиденциальной информации.	7	1	6	-	-

	Промежуточная аттестация	1	-	-	1	Зачет
7.	**Итоговая аттестация (Квалификационный экзамен)**	**8**	**-**	**-**	**8**	
	ИТОГО:	**72**	**22**	**37**	**13**	

3.2. Учебная программа

Модуль 1. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Тема 1.1 Конфигурация сетевой инфраструктуры

Лекция. Конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п.. Установка и настройка системы корпоративной защиты от внутренних угроз.

Практическое занятие. Поиск и устранение неисправностей при развёртывании и настройке. Установка и настройка агентского мониторинга. Синхронизация с LDAP-сервером, раздел персоны заполнен корректно.

Тема 1.2 Установка и настройка системы корпоративной защиты от внутренних угроз

Лекция. Установка и настройка агентского мониторинга. Синхронизация с LDAP-сервером. Система корпоративной защиты от внутренних угроз. Процесс утечки конфиденциальной информации в системе.

Практическое занятие. Изучение структуры организации на основании полученных материалов («модели организации»), обследование корпоративных информационных систем. Определение каналов передачи данных и потенциальных утечек.

Модуль 2. Исследование (аудит) организации с целью защиты от внутренних угроз

Тема 2.1 Угрозы информационной безопасности.

Лекция. Угрозы информационной безопасности. Объекты защиты.

Практическое занятие. Провести обследование корпоративных информационных систем. Определить объекты защиты. Типы циркулирующих данных.

Тема 2.2 Модели угроз

Лекция. Модели угроз

Практическое занятие. Заполнить шаблон модели угроз. Подготовить отчёт о результатах аудита, включая потоки данных, потенциальные каналы утечек, уровни рисков роли пользователей, объекты защиты (с привязкой к нормативной базе и методикам оценки последствий), ролями пользователей и т.п.

Тема 2.3 Нормативно -правовые документы организации по легальному применению корпоративной защиты от внутренних угроз информационной безопасности .

Лекция. Перечень нормативных актов РФ, задействованных в рамках модели угроз.

Практическое занятие. Разработка перечня, описание и шаблоны нормативно-правовых документов организации по легальному применению корпоративной защиты от внутренних угроз информационной безопасности

Промежуточный контроль

Модуль 3. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Тема 3.1 Политика безопасности

Лекция. Политика безопасности.

Практическое занятие. Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты

Тема 3.2 Технологии защиты: печатей, бланков, графических объектов, баз данных

Лекция. Технологии защиты информации

Практическое занятие. Разработать или/и модифицировать объекты защиты, категории, технологии защиты в DLP - системе и т.п. Использовать различные технологии защиты: печатей, бланков, графических объектов, баз данных и т.п.

Тема 3.3 Работа с интерфейсом управления системы корпоративной защиты информации.

Лекция. Интерфейс управления системы корпоративной защиты информации.

Практическое занятие. Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности. Работа с интерфейсом управления системы корпоративной защиты информации.

Промежуточный контроль

Модуль 4. Технологии анализа и защиты сетевого трафика

Тема 4.1 Технологии анализа и защиты сетевого трафика.

Лекция. Технологии анализа и защиты сетевого трафика

Практическое занятие. Развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре.

Тема 4.2 Межсетевое взаимодействие и туннелированние.

Лекция. Межсетевое взаимодействие и туннелированние.

Практическое занятие. Централизованные политики безопасности. Защита рабочих мест. IDS. Выявление большей части инцидентов безопасности

Промежуточный контроль

Модуль 5. Технологии агентского мониторинга

Тема 5.1 Технологии агентского мониторинга.

Лекция. Технологии агентского мониторинга.

Практическое занятие. Механизмы работы агентского мониторинга.

Тема 5.2 Работа с исключениями из перехвата.

Лекция. Работа с исключениями из перехвата.

Практическое занятие. Разработать и применить политики агентского мониторинга для работы с файлами.

Промежуточный контроль

Модуль 6. Анализ выявленных инцидентов

Тема 6.1 Классификацию уровня угроз инцидентов.

Лекция. Классификацию уровня угроз инцидентов.

Практическое занятие. Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов. Проведение классификацию уровня угроз инцидентов. Оценка ущерба.

Тема 6.2 Законодательство в области защиты конфиденциальной информации.

Лекция. Виды информации ограниченного доступа. Персональные данные. Коммерческая тайна.

Практическое занятие. Разработка план по дальнейшему расследованию выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу.

Промежуточный контроль

3.4. Календарный учебный график (порядок освоения модулей)

Период обучения (недели)*	Наименование модуля
1 неделя	Модуль 1. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз. Модуль 2. Исследование (аудит) организации с целью защиты от внутренних угроз
2 неделя	Модуль 3. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз
3 неделя	Модуль 4. Технологии анализа и защиты сетевого трафика Модуль 5. Технологии агентского мониторинга
4 неделя	Модуль 6. Анализ выявленных инцидентов
	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	Практические занятия (лабораторные работы)	комплект деталей, кабелей, инструментов и приспособлений.

"Строительство", зона под вид работ «Информационные кабельные сети»		
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).