Министерство образования и науки Челябинской области
Государственное бюджетное профессиональное образовательное учреждение «Челябинский радиотехнический техникум»

РАБОЧАЯ ПРОГРАММА

Учебной дисциплины

«Основы сетевых технологий»

ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«СОВРЕМЕННЫЕ СЕТЕВЫЕ ТЕХНОЛОГИИ»

г. Челябинск

Рабочая программа «Основы сетевых технологий» дополнительной профессиональной программы повышения квалификации «Современные сетевые технологии» является авторской и направлена на формирование знаний о сетевых технологиях и навыков, которые можно применить в начале работы в качестве специалиста по сетям.

Разработчик:

Еретнов А.Е., преподаватель.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

1.1. Рабочая программа «Основы сетевых технологий» является частью программы дополнительного профессионального образования «Современные сетевые технологии» студентов второго года обучения по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

1.2. Цель программы – формирование знаний о сетевых технологиях и навыков, которые можно применить в начале работы в качестве специалиста по сетям.

1.3. Рекомендуемое количество часов на освоение программы.

Максимальная учебная нагрузка обучающегося – 40 часов.

1.2. Цель и планируемые результаты освоения:

Код ПК	Умения	Знания
ПК 3	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуата-ционной документации	Создание и настройка одноранговой сети, компьютерной сети с помощью маршрутизатора, беспроводной сети; создание подсетей и настройка обмена данными; использования основных команд для проверки подключения к сети Интернет, отслеживания сетевых пакетов, параметров IP-адресации.

2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

2.1. Объем учебной дисциплины и виды учебной работы.

Вид учебной работы	Объем в часах
Обязательная учебная нагрузка	40
в том числе:	
теоретическое обучение	20
практические занятия	20

2.2. Тематический план и содержание

Наименование разделов и тем	Содержание учебного материала, практические работы обучающихся	Объем часов
Тема 1.1. Компьютерные сети. Операционная система сетевого взаимодействия.	**Содержание учебного материала**	**8**
	Основные понятия. Виды компьютерных сетей.	2
	Технологии подключения к интернет. Конвергентные сети.	2
	Практические занятия	**4**
	Операционная система сетевого взаимодействия Cisco(IOS).	4
Тема 1.2. Сетевые протоколы и коммуникации.	**Содержание учебного материала**	**8**
	Кодирование и параметры сообщения.	2
	Набор протоколов TCP/IP и процесс обмена данными.	2
	Практические занятия:	**4**
	Инкапсулляция данных. Сетевая адресация. MAC IP адреса.	4
Тема 1.3. Сетевой доступ. Сетевые технологии Ethernet.	**Содержание учебного материала**	**8**
	Протоколы и стандарты физического уровня.	2
	Структура и особенности прокладки оптоволоконных кабелей.	2
	Практические занятия	**4**
	Управление доступом к среде передачи данных (CSMA).	4
Тема 1.4. Сетевой уровень.	**Содержание учебного материала**	**8**
	Протоколы сетевого уровня.	2
	Таблица маршрутизации узлов и маршрутизатора для протоколов IPv4 b IPv6.	2

	Практическое занятие: Устройство маршрутизатора.	**4**
Тема 1.5. Транспортный уровень.	**Содержание учебного материала**	**8**
	Назначение и задачи транспортного уровня.	2
	Обмен данными по TCP.	2
	Практическое занятие: Обмен данными и использование UDP и TCP.	**4**
Всего:		**40**

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ.

3.1. Для реализации программы должны быть предусмотрены следующие специальные помещения:

Реализация дисциплины предполагает наличие лаборатории инженерно-технических средств систем автоматизированного проектирования и мастерской «Корпоративная защита информации от внутренних угроз информационной безопасности»

Технические средства обучения:

- Монитор Dell 23.8" P2419H
- Микрокомпьютер Dell OptiPlex 7070 на базе процессора Intel Core i5-9500T/ 6 Cores/ 6 Threads/ 3.7 GHz/ 1x16 Gb DDR4/ SSD M.2 PCIe NVMe 512 Gb/ Intel® UHD Graphics 630/
- Интерактивный дисплей SMART Board серии MX SBID-MX265

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменамCCENT/CCNA ICND1 640-822, 3-е издание – Ь.: Издательство «Вильямс, 2013».

2. Олифер Н. Олифер В. Компьютерные сети. Принципы, протоколы, технологии. Спб, Питер, 2011 г.

3. Смелянский Р.Л. Компьютерные сети. Системы передачи данных. Москва, Академия, 2017 г.

3.2.2. Дополнительные печатные источники:

Интернет-ресурсы:

1. http://netacad.com

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Контроль и оценка результатов освоения рабочей программы осуществляется преподавателем в процессе проведения практических занятий и индивидуальных заданий.

Результаты обучения	Критерии оценки	Формы и методы оценки
Знания: – создание и настройка одноранговой сети, компьютерной сети с помощью маршрутизатора, беспроводной сети; – создание подсетей и настройка обмена данными; – использования основных команд для проверки подключения к сети Интернет, отслеживания сетевых пакетов, параметров IP-адресации.;	Демонстрация знаний классификации, сущности сетевых процессов, области применения, а также знаний создания и настройка одноранговой сети, создания подсетей, использования основных команд для проверки подключения к сети Интернет.	Оценка знаний в ходе проведения практических занятий, индивидуальные опросы

Умения: – выполнять задачи проектирования, развертывания и технического сопровождения локальных и глобальных сетей; – использовать общепризнанные мировые стандарты и решения в своей работе; – выполнять типовые задачи развертывания и технического сопровождения малой сети предприятия или ее фрагмента.	Уметь самостоятельно выполнять задачи проектирования, выполнять типовые задачи развертывания и технического сопровождения малой сети.	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий

Министерство образования и науки Челябинской области
Государственное бюджетное профессиональное образовательное учреждение «Челябинский радиотехнический техникум»

РАБОЧАЯ ПРОГРАММА

Учебной дисциплины

«Комплексная система защиты информационных систем и критической информационной инфраструктуры»

ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ

ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«СОВРЕМЕННЫЕ СЕТЕВЫЕ ТЕХНОЛОГИИ»

г. Челябинск

Рабочая программа «Комплексная система защиты информационных систем и критической информационной инфраструктуры» дополнительной профессиональной программы повышения квалификации «Современные сетевые технологии» является авторской и направлена на дополнение и углубление знаний и умений по построению комплексных систем защиты информационных систем.

Разработчик:

Лукашина Е.Ю., начальник Управления информационной безопасности Министерства информационных технологий и связи Челябинской области.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

1.1. Рабочая программа «Комплексная система защиты информационных систем и критической информационной инфраструктуры» является частью программы дополнительного профессионального образования «Современные сетевые технологии» студентов третьего года обучения по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»;

1.2. Цель программы – сформировать навыки построения комплексных систем защиты информационных систем.

1.3. Рекомендуемое количество часов на освоение программы.

Максимальная учебная нагрузка обучающегося – 40 часов

1.4. Цель и планируемые результаты освоения:

Код ПК	Умения	Знания
ОК 1 ОК 2 ОК 3 ОК 9 ОК 10 ПК 2.2 ПК 2.4	– выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. – осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. – планировать и реализовывать собственное профессиональное и личностное развитие. – использовать информационные технологии в профессиональной деятельности. – пользоваться профессиональной документацией на государственном и иностранном языках. – обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствам – осуществлять обработку, хранение и передачу информации ограниченного доступа.	– нормативные правовые акты в области информационной безопасности и защиты информационных систем и критической информационной инфраструктуры, методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; – основы организации комплексных систем защиты информации и информационных систем; – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

2.1. Объем учебной дисциплины и виды учебной работы.

Вид учебной работы	**Объем в часах**
Обязательная учебная нагрузка	40
в том числе:	
теоретическое обучение	40
практические занятия	0

2.2. Тематический план и содержание

Наименование разделов и тем	Содержание учебного материала, практические работы обучающихся	Объем часов
Тема 1.1. Информационные системы	**Содержание учебного материала**	**8**
	Виды информации и информационных систем	2
	Информационные системы персональных данных и государственные информационные системы. Моделирование угроз. Меры защиты	2
	Виды средств (систем) защиты информации. Сертификация средств защиты информации	2
	Требования при построении комплексной системы защиты информации	2
Тема 1.2. Критическая информационная инфраструктур	**Содержание учебного материала**	**24**
	История и законодательство в сфере критической информационной инфраструктуры	2
	Субъекты и объекты критической информационной инфраструктуры. Обязанности субъекта критической инфраструктуры	2
	Категорирование объектов критической информационной инфраструктуры	4
	Система безопасности значимого объекта критической информационной инфраструктуры	2
	Моделирование угроз безопасности объекта критической информационной инфраструктуры	2
	Состав требований и мер по обеспечению безопасности и их базовые наборы для соответствующей категории значимого объекта критической информационной инфраструктуры	4
	Средства (системы) защиты информации объекта критической информационной инфраструктуры.	4
	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)	4
Тема 1.3. Центр мониторинга и	**Содержание учебного материала**	**8**
	Построение центров мониторинга и реагирования на инциденты. Ведомственные и корпоративные центры ГосСОПКА. Организация взаимодействия с НКЦКИ ГосСОПКА	3

реагирования на инциденты (SOC)	Лицензирование в сфере информационной безопасности	3
	Обучение и повышение квалификации в сфере информационной безопасности	2
Всего:		**40**

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

3.1. Для реализации программы должны быть предусмотрены следующие специальные помещения:

Реализация дисциплины предполагает наличие лаборатории инженерно-технических средств систем автоматизированного проектирования.

Технические средства обучения:

– Монитор Dell 23.8" P2419H

– Микрокомпьютер Dell OptiPlex 7070 на базе процессора Intel Core i5-9500T/ 6 Cores/ 6 Threads/ 3.7 GHz/ 1x16 Gb DDR4/ SSD M.2 PCIe NVMe 512 Gb/ Intel® UHD Graphics 630/

– Интерактивный дисплей SMART Board серии MX SBID-MX265

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Федеральный закон от 27.12.2002 г. № 184-ФЗ «О техническом регулировании»
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
5. Постановление Правительства Российской Федерации от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. Постановление Правительства РФ от 6.07.2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»
7. Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»
8. Постановление Правительства РФ №162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»
9. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
10. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
11. Приказ ФСТЭК России №227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ»
12. Приказ ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»
13. Приказ ФСТЭК России №236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»
14. Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»

15. Информационное сообщение ФСТЭК России №240/22/2339 от 04.05.2018 «О методических документах по вопросам обеспечения безопасности информации в КСИИ РФ»

16. Информационное сообщение ФСТЭК России №240/25/3752 от 24.08.2018 «По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

17. Приказ ФСБ России №366 от 24.07.2018 «О НКЦКИ»

18. Приказ ФСБ России №367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»

19. Приказ ФСБ России №368 от 24.07.2018 «Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

20. Приказ ФСБ России №196 от 06.05.2019 «Об утверждении требований к средствам ГосСОПКА»

21. Приказ ФСБ России №281 от 19.06.2019 «Об утверждении Порядка, технических условий установки и эксплуатации средств ГосСОПКА»

22. Приказ ФСБ России №282 от 19.06.2019 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении ЗО КИИ РФ»

23. Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах».

24. Государственный реестр сертифицированных средств защиты информации ФСТЭК России.

25. Банк данных угроз безопасности информации ФСТЭК России

26. Гришина Н.В. Комплексная система защиты информации на предприятии: Учебное пособие. — М.: Издательский центр «Инфра-М», 2014. – 240 с.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ.

Контроль и оценка результатов освоения рабочей программы осуществляется преподавателем в процессе проведения практических занятий и индивидуальных заданий.

Результаты обучения	Критерии оценки	Формы и методы оценки
Знания: – нормативные правовые документы в области обеспечения безопасности информации ограниченного доступа, информационных систем и критической информационной инфраструктуры – нормативно-методические документы ФСТЭК России и ФСБ России; – методы анализа и оценки угроз защищаемой информации – технологическое и организационное построение комплексных систем защиты информационных систем – технологическое и организационное построение центров мониторинга и реагирования на инциденты	Демонстрация знаний о нормативной базе в области защиты информации в информационных системах. Демонстрация знаний об современных угрозах информационной безопасности. Демонстрация знаний о современных средствах защиты информации и требований к ним.	Оценка знаний в ходе проведения практических занятий, индивидуальные опросы
Умения: – определять состав защищаемой информации и объектов защиты – выявлять угрозы защищаемой информации; – определять состав организационных и технических мер по обеспечению безопасности информационных систем и критической информационной инфраструктуре; – выбирать методы и средства, необходимые для организации и функционирования систем защиты информации и центров мониторинга и реагирования на инциденты	Умение проводить анализ информации и объектов защиты, выделять актуальные угрозы. Умение выбирать меры защиты информационных систем и соответствующие им средства защиты информации.	Экспертная оценка результатов деятельности обучающегося при проведении опросов

Министерство образования и науки Челябинской области
Государственное бюджетное профессиональное образовательное учреждение «Челябинский радиотехнический техникум»

РАБОЧАЯ ПРОГРАММА

Учебной дисциплины

«Защита данных от утечек информации средствами InfoWatch Traffic Monitor»

ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ

ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«СОВРЕМЕННЫЕ СЕТЕВЫЕ ТЕХНОЛОГИИ»

г. Челябинск

Рабочая программа «Защита данных от утечек информации средствами InfoWatch Traffic Monitor» дополнительной профессиональной программы повышения квалификации «Современные сетевые технологии» является авторской и направлена на дополнение и углубление знаний и умений по построению комплексных систем защиты информационных систем.

Разработчик:
Метальников А.В., Заместитель директора ООО «ЦИТ «ОЗОН».

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

1.1. Рабочая программа «Защита данных от утечек информации средствами InfoWatch Traffic Monitor» является частью программы дополнительного профессионального образования «Современные сетевые технологии» студентов третьего года обучения по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

1.2. Цель программы – сформировать навыки построения комплексных систем защиты информационных систем.

1.3. Рекомендуемое количество часов на освоение программы.

Максимальная учебная нагрузка обучающегося – 38 часов.

1.2. Цель и планируемые результаты освоения

Код ПК	Умения	Знания
ОК 1 ОК 2 ОК 3 ОК 9 ОК 10 ПК 2.2 ПК 2.4	– выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. – осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. – планировать и реализовывать собственное профессиональное и личностное развитие. – использовать информационные технологии в профессиональной деятельности. – пользоваться профессиональной документацией на государственном и иностранном языках. – обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствам – осуществлять обработку, хранение и передачу информации ограниченного доступа.	– нормативные правовые акты в области информационной безопасности и защиты информационных систем и критической информационной инфраструктуры, методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; – основы организации комплексных систем защиты информации и информационных систем; – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

2.1. Объем учебной дисциплины и виды учебной работы.

Вид учебной работы	Объем в часах
Обязательная учебная нагрузка	38
в том числе:	
теоретическое обучение	8
практические занятия	30

2.2. Тематический план и содержание

Наименование разделов и тем	Содержание учебного материала, практические работы обучающихся	Объем часов
Тема 1.1. Теория построения системы защиты информации от утечек	**Содержание учебного материала**	**8**
	Законодательные требования по защите информации от утечек	2
	Основные требования к системам защиты информации от утечек	4
	Правовое обоснование внедрения системы защиты информации от утечек на предприятии	2
Тема 1.2. Использование системы защиты информации Infowatch Traffic Monitor	**Содержание учебного материала**	**22**
	Архитектура системы защиты информации от утечек Infowatch Traffic Monitor	2
	Назначение, порядок установки Infowatch Traffic Monitor	2
	Назначение, порядок установки Infowatch Device Monitor	2
	Порядок настройки каналов перехвата информации	2
	Развертывание тестового стенда для системы защиты информации от утечек Infowatch Traffic Monitor	2
	Установка, настройка Infowatch Traffic Monitor	4
	Установка, настройка Infowatch Device Monitor	4
	Настройка каналов перехвата информации	4
Тема 1.3. Демонстрация работы системы защиты информации Infowatch Traffic Monitor	**Содержание учебного материала**	**8**
	Проверка работоспособности перехвата информации в сетевом трафика	4
	Проверка работоспособности перехвата информации при копировании данных на съемные носители информации	2
	Использование возможностей по контролю сотрудников	2
Всего:		**38**

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ.

3.1. Для реализации программы должны быть предусмотрены следующие специальные помещения

Реализация дисциплины предполагает наличие лаборатории инженерно-технических средств систем автоматизированного проектирования и мастерской ««Корпоративная защита информации от внутренних угроз информационной безопасности»

Технические средства обучения:

– Монитор Dell 23.8" P2419H

– Микрокомпьютер Dell OptiPlex 7070 на базе процессора Intel Core i5-9500T/ 6 Cores/ 6 Threads/ 3.7 GHz/ 1x16 Gb DDR4/ SSD M.2 PCIe NVMe 512 Gb/ Intel® UHD Graphics 630/

– Интерактивный дисплей SMART Board серии MX SBID-MX265

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Федеральный закон от 27.12.2002 г. № 184-ФЗ «О техническом регулировании»
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
5. Постановление Правительства Российской Федерации от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»
7. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
8. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
9. Приказ ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»
10. Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»
11. InfoWatch Traffic Monitor 6.11. Руководство пользователя
12. InfoWatch Traffic Monitor 6.11. Руководство администратора
13. InfoWatch Traffic Monitor 6.11. Руководство по установке
14. InfoWatch. Работа в Консоли Управления Device Monitor

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ.

Контроль и оценка результатов освоения рабочей программы осуществляется преподавателем в процессе проведения практических занятий и индивидуальных заданий.

Результаты обучения	Критерии оценки	Формы и методы оценки
Знания: – нормативные правовые документы в области обеспечения безопасности информации ограниченного доступа, информационных систем – аналы утечки информации, основные угрозы информационной безопасности – современные средства защиты информации, включая средства защиты информации от утечек (DLP)	Демонстрация знаний о нормативной базе в области защиты информации в информационных системах. Демонстрация знаний об современных угрозах информационной безопасности. Демонстрация знаний о современных средствах защиты информации и требований к ним.	Оценка знаний в ходе проведения практических занятий, индивидуальные опросы
Умения: – устанавливать систему защиту информации Infowatch Traffic Monitor – настраивать систему защиту информации Infowatch Traffic Monitor – эмулировать потенциально возможные каналы утечки информации, обнаруживать утечку информацию и предотвращать факт утечки – расследовать факты утечки информации	Умение устанавливать, внедрять, проводить тонкую настройку средств защиты информации от утечек Умение выявлять утечки информации через различные каналы утечки	Экспертная оценка результатов деятельности обучающегося при проведени опросов