Министерство образования и молодежной политики Свердловской области

государственное автономное профессиональное образовательное учреждение Свердловской области

«Уральский радиотехнический колледж им. А.С. Попова»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Применение инженерно-технических средств обеспечения информационной безопасности

для специальности среднего профессионального образования

10.02.03 Информационная безопасность автоматизированных систем программы базовой подготовки

2020 г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования

10.02.03 Информационная безопасность автоматизированных систем

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Д.В. Колесников

«30» июня 2020 г.

Рекомендована цикловой методической комиссией
«Электронных вычислительных машин»
Протокол от « 29 » августа 2020 г. № 6

Председатель ЦМК _____ Ю.Г. Котова

Разработчики:

Уймин А.Г., преподаватель УРТК им. А. С. Попова
Саматов К. М., преподаватель УРТК им. А. С. Попова

СОДЕРЖАНИЕ

1 ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ УЧАСТИЕ В ИНТЕГРАЦИИ ПРОГРАММНЫХ МОДУЛЕЙ

1.1 Область применения программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.03 «Информационная безопасность автоматизированных систем» в части освоения основного вида профессиональной деятельности (ВПД) «Применение инженерно-технических средств обеспечения информационной безопасности» и соответствующих профессиональных компетенций (ПК):

- ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности.
- ПК 3.2. Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
- ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.
- ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.
- ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

1.2 Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

– выявления технических каналов утечки информации;

– использования основных методов и средств инженерно-технической защиты информации;

– диагностики, устранения отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности;

– участия в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности;

– решения частных технических задач, возникающих при аттестации объектов, помещений, технических средств;

уметь:

– применять технические средства защиты информации;

– использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;

– использовать средства защиты информации от несанкционированного съёма и утечки по техническим каналам;

– применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами;

знать:

– физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

– номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации;

– основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам;

– номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

1.3. Количество часов на освоение программы профессионального модуля:

всего – 291 час, в том числе:

- максимальной учебной нагрузки обучающегося – 183 часов, включая:

- обязательной аудиторной учебной нагрузки обучающегося –122 часа;

- самостоятельной работы обучающегося – 61 час;

- учебной практики – 108 часов.

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения рабочей программы профессионального модуля является овладение обучающимися видом профессиональной деятельности «Применение инженерно-технических средств обеспечения информационной безопасности», в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1	. Применять инженерно-технические средства обеспечения информационной безопасности.
ПК 3.2.	Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
ПК 3.3.	Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.
ПК 3.4.	Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.
ПК 3.5.	Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10	Формулировать задачи логического характера и применять средства математической логики для их решения.
ОК 11	Владеть основными методами и средствами разработки программного обеспечения.

Код	Наименование результата обучения
ОК 12	Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.

3 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Тематический план профессионального модуля

Коды профессиональных компетенций	**Наименования разделов профессионального модуля***	**Всего часов** *(макс. учебная нагрузка и практики)*	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная (по профилю специальности),** часов *(если предусмотрена рассредоточенная практика)*
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов	**в т.ч., курсовая работа (проект),** часов	**Всего,** часов	**в т.ч., курсовая работа (проект),** часов		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
ПК 3.1-ПК 3.5	**Раздел 1 Применение инженерно – технических средств обеспечения информационной безопасности**	**291**	**122**	62	**-**	**61**		**108**	
	Производственная практика (по профилю специальности), часов	**-**							**-**
	Всего:	**291**	**122**	62		**61**		**108**	**-**

3.2. Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов	Уровень освоения
1	**2**		**3**	**4**
Раздел 1 Применение инженерно – технических средств обеспечения информационной безопасности			**291**	
МДК 03.01 Применение инженерно – технических средств обеспечения информационной безопасности			**122**	
Тема 1.1 Применение инженерно-технических средств обеспечения информационной безопасности	**Содержание**		58	2
	1.	Предмет и задачи курса. Основные термины и определения в области технических средств охраны.		
	2.	Цели и задачи технической охраны информационных и телекоммуникационных систем и сетей. Направления технической охраны.		
	3.	Назначение и классификация технических средств охраны объектов. Структура системы охраны объектов.		
	4.	Контрольно-пропускной режим. Организация и управление контрольно-пропускной системой. Порядок пропуска сотрудников предприятия и посетителей через КПП.		
	5.	Порядок допуска на объект транспортных средств, вывоза продукции, документов и материальных ценностей.		
	6.	Подразделение охраны. Виды охраны. Группы быстрого реагирования. Соотношение сил охраны и технических средств при охране объекта.		
	7.	Инженерно-технические сооружения, препятствующие умышленному или непреднамеренному доступу на территорию охраняемого объекта.		
	8.	Решетки и требования к ним. Механические средства защиты периметра.		
	9.	Двери и окна зданий и помещений. Классификация и требования надёжности дверей. Методы укрепления оконных проёмов (стекол).		
	10.	Классификация стеклянных полотен по прочности. Замки, их классификация и характеристики.		
	11.	Шкафы, рабочие столы, хранилища, металлические шкафы и сейфы. Назначение, особенности, конструктивное исполнение. Стойкость хранилищ и сейфов.		

1	2		3	4
	12.	Система охранной сигнализации. Структуры подсистем охранной и охранно-пожарной сигнализации. Извещатели охранных систем.		
	13.	Извещатели охранных систем.		
	14.	Системы видеонаблюдения. Структурная схема системы видеонаблюдения..		
	15.	Состав и основные функции системы видеонаблюдения. Параметры и характеристики систем видеонаблюдения		
	16.	Системы охраны периметра. Радиолучевые и радиоволновые системы охраны периметра, характеристики и особенности эксплуатации. Сейсмические системы охраны периметра, характеристики и особенности эксплуатации.		
	17.	Сейсмические системы охраны периметра, характеристики и особенности эксплуатации.		
	18.	Системы контроля и управления доступом (СКУД). Состав и структура СКУД.		
	19.	Классификация стеклянных полотен по прочности. Замки, их классификация и характеристики.		
	20.	Функции СКУД. Одноконтроллерные и многоконтроллерные СКУД.		
	21.	Технические каналы утечки информации		
	22.	Средства выявления каналов утечки информации		
	23.	Скрытие и защита информации от утечки по техническим каналам		
	24.	Контроль эффективности мер защиты информации		
	25.	Аттестация объектов информатизации		
	26.	Утечки информации и защита информации при использовании мобильных устройств		
	Практические работы		62	
	1.	Разработка плана обследования защищаемого объекта		
	2.	Разработка модели нарушителя		
	3.	Разработка плана размещения охраняемых зон и размещения рубежей защиты объекта		
	4.	Разработка регламента по режиму в организации		
	5.	Разработка структурной схемы системы охранной сигнализации		
	6.	Разработка схемы размещения видеокамер на охраняемом объекте		
	7.	Разработка схемы инженерно-технических укреплений объекта		
	8.	Определение технических каналов утечки информации на гипотетическом объекте		
	9.	Разработка методики контроля эффективности мер защиты информации		
	10.	Проведение аттестации объектов информатизации. Подготовка аттестата		

1	2		3	4
	11.	Деловая игра «Оборудование гипотетического объекта. Определение угроз и предмета защиты».		
	12.	Деловая игра «Оборудование гипотетического объекта. Анализ уязвимости и оценка эффективности средств физической защиты».		
	13.	Деловая игра «Оборудование гипотетического объекта. Защита проектов. Обсуждение докладов».		
Дифференцированный зачет			**2**	
Самостоятельная работа при изучении раздела 1 ПМ 03 Систематическая проработка конспектов занятий, учебной литературы по главам и параграфам, указанным преподавателем. Подготовка к практическим занятиям с использованием методических указаний преподавателя, оформление отчетов и подготовка к защите.			61	
Примерная тематика домашних заданий 1. Изучение литературы. 2.Офомление отчета по практической работе. 3.Подготовка к защите практической работы. 4 Подготовка к тестированию.				
УП.03.01 Учебная практика по эксплуатации объектов сетевой инфраструктуры **Виды работ** 1. Фундаментальные принципы безопасной сети 2. Современные угрозы сетевой безопасности 3. Вирусы, черви и троянские кони 4. Методы атак 5. Безопасность сетевых устройств OSI 6. Безопасный доступ к устройствам 7. Назначение административных ролей 8. Мониторинг и управление устройствами 9. Использование функция автоматизированной настройки безопасности 10. Авторизация, аутентификация и учет доступа (AAA) 11. Свойства AAA 12. Локальная AAA аутентификация 13. Server-based AAA 14. Реализация технологий брандмауэра 15. ACL 16. Технология брандмауэра 17. Контекстный контроль доступа (CBAC) 18. Политики брандмауэра основанные на зонах 19. Реализация технологий предотвращения вторжения 20. IPS технологии 21. IPS сигнатуры 22. Реализация IPS			108	

1	2	3	4
23. Проверка и мониторинг IPS 24. Безопасность локальной сети 25. Обеспечение безопасности пользовательских компьютеров 26. Соображения по безопасности второго уровня (Layer-2) 27. Конфигурация безопасности второго уровня 28. Безопасность беспроводных сетей, VoIP и SAN 29. Криптографические системы 30. Криптографические сервисы 31. Базовая целостность и аутентичность 32. Конфиденциальность 33. Криптография открытых ключей 34. Реализация технологий VPN 35. VPN 36. GRE VPN 37. Компоненты и функционирование IPSec VPN 38. Реализация Site-to-site IPSec VPN с использованием CLI 39. Реализация Site-to-site IPSec VPN с использованием CCP 40. Реализация Remote-access VPN 41. Управление безопасной сетью 42. Принципы безопасности сетевого дизайна. 43. Безопасная архитектура. 44. Управление процессами и безопасность 45. Тестирование сети на уязвимости 46. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. 47. Жизненный цикл сети и планирование. 48. Разработка регламентов компании и политик безопасности. 49. Введение в Адаптивное устройство безопасности ASA 50. Конфигурация межсетевого экрана на базе ASA с использованием графического интерфейса ASDM 51. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM			
	Всего:	**183**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – оз накомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1 Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы профессионального модуля предполагает наличие лаборатории «Аппаратных средств вычислительной техники, инженерно-технической средств обеспечения информационной безопасности» и мастерской «Корпоративная защита от внутренних угроз информационной безопасности».

Оборудование лаборатории «Аппаратных средств вычислительной техники, инженерно-технической средств обеспечения информационной безопасности»:

- персональный компьютер и мультимедийный проектор;
- персональные компьютеры с аппаратной поддержкой виртуализации и техническими характеристиками не ниже i7\16 Gb \SSD 128\HDD 1 Tb\VGA integrate\ Monitor 23”;
- аппаратное обеспечение ISR G2 (Cisco 2901);
- аппаратное обеспечение Cisco Catalyst WS-2960+24TC-L;
- аппаратное обеспечение Cisco ASA 5505;
- столы и стулья.

Программное обеспечение:

- Программное обеспечение VirtualBox, KVM
- Программное обеспечение OpenOffice.

Оборудование мастерской «Корпоративная защита от внутренних угроз информационной безопасности»:

- ПЭВМ в сборе (i7/32Gb MEM/ 256Gb + 1Tb nvme SSD/ Nvidia Qadro 1000 / Intel 4x1Gb/s Lan Card/ 27” Monitor)
- ViPNet Software (Coordinator for Windows 4.x + Client for Windows 4.x + Polic-y Man-ager 4.x + VPN HW Router)
- Видео проектор Epson EB-2247U
- Экран для проектора Lumien Master Picture 191x300 Matte White FiberGlass
- Рабочее место в сборе:

- стол (ШхД) 1200х750;
- рама задняя короткая;
- перфопанель – 2;
- набор держателей;

- электроблок на 8 розеток;
- полка приборная длинная;
- светильник светодиодный – 2 шт;
- кронштейн для монитора;
- полка для системного блока;
- стул тканевый с металлической крестовиной;
- металлические колеса для стула;
- набор подлокотников.

4.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники

1. В.Г. Олифер, Н.А. Олифер "Компьютерные сети. Принципы, технологии, протоколы". 5-е изд., – СПб: Питер, 2017.- 992с.
2. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278.
3. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 2-е изд., испр. и доп. – Москва: НТИ «Горячая линия–Телеком». – 2017; - 338стр
4. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – Москва: НТИ «Горячая линия–Телеком». – 2017; - 586стр.
5. Варлатая С.К., Шаханова М.В. Защита информационных процессов в компьютерных сетях. Учебно-методический комплекс. изд. Проспект, 2015. – 178с.
6. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии) Учебное пособие для вузов. . – Москва: НТИ «Горячая линия–Телеком». – 2016; - 220стр.

Дополнительные источники:

1. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии) Учебное пособие для вузов. . – Москва: НТИ «Горячая линия–Телеком». – 2016; - 220стр.
2. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учеб. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: https://e.lanbook.com/book/39990.
3. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2012. — 592 с. — Режим доступа: https://e.lanbook.com/book/3032.
4. Шаньгин, В.Ф. Защита компьютерной информации [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2010. — 544 с. — Режим доступа: https://e.lanbook.com/book/1122.
5. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578.

Интернет ресурсы

ИР 1 http://www.docload.ru (ГОСТы для оформление технической документации)

ИР 3 https://www.netacad.com/ (справочная информация по сетевым технологиям)

4.3 Общие требования к организации образовательного процесса

Занятия проводятся спаренными уроками продолжительностью один академический час, общая продолжительность спаренного урока - 2 академических часа (1,5 астрономических часа). Образовательный процесс включает в себя проведение лекционных, комбинированных, практических занятий, чередующихся друг с другом.

Учебная практика по эксплуатации объектов сетевой инфраструктуры реализуется концентрированно лабораториях колледжа. Каждый обучающийся должен быть обеспечен индивидуальным рабочим местом.

Реализация рабочей программы модуля должна обеспечиваться учебно методической документацией, доступом каждого обучающегося к базам данных и библиотечным фондам. Во время самостоятельной подготовки обучающиеся должны быть обеспечены доступом к сети Интернет.

Должны быть предусмотрены консультации в объеме не менее 0,5 часа в неделю по каждому МДК. Формы проведения консультаций: групповые, индивидуальные, письменные, устные.

Освоению данного модуля должно предшествовать изучение следующих дисциплин:

- ОП.01 Основы информационной безопасности;

-ОП.02 Технические средства информатизации;

- ОП.03 Организационно-правовое обеспечение информационной безопасности;

- ОП.04 Сети и системы передачи информации;

-ОП.05 Основы алгоритмизации и программирования

- ОП.07Операционные системы;

-ОП.08 Базы данных;

- ОП.14 Архитектура ЭВМ и вычислительных систем

4.4 Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу :

- наличие высшего профессионального образования, соответствующего профилю модуля «Применение инженерно-технических средств обеспечения информационной безопасности»

- дополнительное образование или повышение квалификации по профилю модуля.

Требования к квалификации педагогических кадров, осуществляющих руководство учебной практикой:

- дипломированные специалисты по профилю профессионального модуля;

- преподаватели междисциплинарных курсов.

5 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Применять инженерно - технические средства обеспечения информационной безопасности	Правильность применения инженерно - технических средств обеспечения информационной безопасности	Наблюдение за выполнением и защита практических работ по МДК 03.01 Наблюдение за выполнением и защита практических заданий по практике УП.03.01. Дифференцированный зачет. Возможна сдача ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» по КОД 1.1
Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.	Правильность эксплуатации инженерно-технических средств обеспечения информационной безопасности, проверки их технического состояния, проведения технического обслуживания и текущего ремонта, устранения отказов и восстановлении работоспособности	
Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.	Правильность проведения мониторинга эффективности применяемых инженерно-технических средств обеспечения информационной безопасности	
Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.	Правильное решение технических задач, возникающих при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств	
Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.	Правильное применение нормативных правовых актов, нормативно-методических документов по обеспечению информационной безопасности инженерно-техническими средствами.	

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	Демонстрация интереса к будущей профессии	Деловые игры, конкурсы-смотры, участие в семинарах, олимпиадах
ОК 2 Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	– выбор и применение методов и способов решения профессиональных задач в области применения инженерно - технических средств обеспечения информационной безопасности; – оценка эффективности и качества выполнения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 3 Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	решение стандартных и нестандартных профессиональных задач в области применения инженерно - технических средств обеспечения информационной безопасности	
ОК 4 Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	– эффективный поиск необходимой информации; – использование различных источников, включая электронные	
ОК 5 Использовать информационно-коммуникационные технологии в профессиональной деятельности.	– демонстрация навыков работы с информацией, представленной в электронном виде; – использование рациональных методы поиска и хранения информации в современных информационных массивах;	
ОК 6 Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.	взаимодействие с обучающимися, преподавателями в ходе обучения	
ОК 7 Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.	проведение регулярного самоанализа с последующей коррекцией результатов собственной работы	

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 8 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	организация самостоятельных занятий при изучении профессионального модуля	
ОК 9 Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	анализ инноваций в области применения программного обеспечения	