АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

УТВЕРЖДАЮ
ДИРЕКТОР АНО ПО «БИТ»
_____ В.В. СЕРГЕЕВ
«_____» _____ 20____ ГОДА
М.П.

ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности

Калининград
2022г.

Программа учебной дисциплины МДК.02.03 «Корпоративная защита от внутренних угроз информационной безопасности» разработана на основе Федерального государственного образовательного стандарта (далее — ФГОС) по специальностям среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного приказом Министерства образования и науки от 9 декабря 2016 года № 1553 и примерной основной образовательной программы СПО, разработанной ФУМО 2017 г.

Организация-разработчик: АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

Разработчик: _____ Околот Денис Ярославович, преподаватель

Рассмотрена
методической комиссией,
протокол № _____
от «____» _____2022 г.
председатель
_____Т.В. Славинская

СОДЕРЖАНИЕ

1.ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ «МДК.01.04 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ»

1.1. Место дисциплины в структуре основной профессиональной образовательной программы: Программа «МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности» является частью профессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности: 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

В результате изучения МДК студент должен освоить основной вид деятельности ВД.1, выполнение работ по проектированию сетевой инфраструктуры, соответствующие ему общие и профессиональные компетенции.

1.1.1. Перечень общих компетенций

Учебная дисциплина «МДК 02.03 Корпоративная защита от внутренних угроз информационной безопасности» наряду с другими учебными дисциплинами обеспечивает формирование следующих общих и профессиональных компетенций

Код	**Наименование общих компетенций**
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 9.	Использовать информационные технологии в профессиональной деятельности
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.

1.1.2. Перечень профессиональных компетенций

Код	**Наименование видов деятельности и профессиональных компетенций**
ВД. 1	*Эксплуатация автоматизированных (информационных) систем в защищенном исполнении*
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном

	исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

Общие требования к личностным результатам выпускников СПО

Личностные результаты реализации программы воспитания *(дескрипторы)*	**Код личностных результатов реализации программы воспитания**
Портрет выпускника СПО	
Осознающий себя гражданином и защитником великой страны.	**ЛР 1**
Готовый использовать свой личный и профессиональный потенциал для защиты национальных интересов России.	**ЛР 2**
Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.	**ЛР 3**
Принимающий семейные ценности своего народа, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания.	**ЛР 4**
Занимающий активную гражданскую позицию избирателя, волонтера, общественного деятеля.	**ЛР 5**
Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение.	**ЛР 6**
Готовый соответствовать ожиданиям работодателей: проектно мыслящий, эффективно взаимодействующий с членами команды и сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, ответственный, пунктуальный, дисциплинированный, трудолюбивый, критически мыслящий, нацеленный на достижение поставленных целей; демонстрирующий профессиональную жизнестойкость.	**ЛР 7**
Признающий ценность непрерывного образования, ориентирующийся в изменяющемся рынке труда, избегающий безработицы; управляющий собственным	**ЛР 8**

профессиональным развитием; рефлексивно оценивающий собственный жизненный опыт, критерии личной успешности.	
Уважающий этнокультурные, религиозные права человека, в том числе с особенностями развития; ценящий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности».	**ЛР 9**
Принимающий активное участие в социально значимых мероприятиях, соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России; готовый оказать поддержку нуждающимся.	**ЛР 10**
Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением.	**ЛР 11**
Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.	**ЛР 12**

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; администрирования автоматизированных систем в защищенном исполнении; эксплуатации компонентов систем защиты информации автоматизированных систем; диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении
уметь	осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы настраивать и устранять неисправности программно-

	аппаратных средств защиты информации в компьютерных сетях по заданным правилам; обеспечивать работоспособность, обнаруживать и устранять неисправности
знать	состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств; теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ «МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности»

2.1. Объем профессионального модуля МДК 02.03 и виды учебной работы

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.						
			Обучение по МДК, в час.				Практики		Самостоятельная работа
			всего, часов	в том числе			учебная практика, часов	производственная практика, часов	
				Лабораторных и практических занятий	Теоретическое обучение	курсовая работа (проект), часов			
ПК 1.1. ОК 1– ОК 10	Раздел 1 модуля. Установка и настройка автоматизированных (информационных) систем в защищенном исполнении	**100**	**76**	**76**	**-**	–	–	–	**12**

Количество часов, отводимое на освоение изучения дисциплины
Всего 100 часа, из них
в том числе на консультацию промежуточной аттестации по МДК 02.03 - 6 **часов**

2.2. Тематический план и содержание профессионального модуля «МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности»

Наименование	**Содержание учебного материала, лабораторные работы и**	**Объем**		

разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	практические занятия, самостоятельная работа обучающихся	часов	Уровень освоения	Осваиваемые элементы компетенций
МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		**123**		
Раздел 1. Разработка защищенных автоматизированных (информационных) систем				
Тема 1.1. Основы информационных систем как объекта защиты.	Содержание	**6**		
	Понятие автоматизированной (информационной) системы Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.		2	ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
	Основные особенности современных проектов АИС. Электронный документооборот.		2	
	Тематика практических занятий и лабораторных работ	**2**		
	Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)			
Тема 1.2. Жизненный цикл автоматизированных систем	**Содержание**	**6**		
	Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и		2	ОК.1; ОК.2; ОК.4; ОК.5;

	сопровождение. Модели жизненного цикла АИС.			ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
	Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.		2	
	Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.		2	
	Тематика практических занятий и лабораторных работ	**2**		
	Разработка технического задания на проектирование автоматизированной системы			
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	**Содержание**	**4**		
	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации		2	ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
	Понятие уязвимости угрозы. Классификация уязвимостей.		2	
	Тематика практических занятий и лабораторных работ	**6**		
	Категорирование информационных ресурсов			
	Анализ угроз безопасности информации			
	Построение модели угроз			
Тема 1.4. Основные меры защиты информации в автоматизированных системах	**Содержание**	**4**		
	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.		2	ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
	Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним		2	

Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	**Содержание**	**10**		
	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.		2	ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
	Ограничение программной среды. Защита машинных носителей информации		2	
	Регистрация событий безопасности		2	
	Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.		2	
	Обнаружение (предотвращение) вторжений		2	
	Контроль (анализ) защищенности информации Обеспечение целостности информационной системы и информации Обеспечение доступности информации		2	
	Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.		2	ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
	Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных		2	
	Резервное копирование и восстановление данных.		2	
	Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.		2	
Тема 1.6. Защита информации в распределенных автоматизированных системах	**Содержание**	**2**		
	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.		2	ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4

				ЛР 01-12
Тема 1.7. Особенности разработки информационных систем персональных данных	**Содержание**	**2**		
	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.		2	
	Тематика практических занятий и лабораторных работ	**2**		
	Определение уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.			
Раздел 2.Эксплуатация защищенных автоматизированных систем.				
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	**Содержание**	**6**		
	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.		2	ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
	Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.		2	
	Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении		2	
Тема 2.2. Администрирование автоматизированных систем	**Содержание**	**2**		
	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения		2	ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12

	отказоустойчивости автоматизированных систем.			
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	**Содержание**	**2**		
	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.		1	ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
Тема 2.4. Защита от несанкционированного доступа к информации	**Содержание**	**6**		ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.		2	
	Классификация автоматизированных систем. Требования по защите информации от НСД для АС		2	
	Требования защищенности СВТ от НСД к информации		1	
	Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ		2	
Промежуточная аттестация по МДК.01.04		**2**		
Тема 2.5. СЗИ от НСД	**Содержание**	**8**		
	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства		2	

	управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.			ОК.1; ОК.2; ОК.4; ОК.5; ЛР 01-12ОК.9; ОК.10 ПК 1.1-1.4
	Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности.		2	
	Обеспечение целостности информационной системы и информации		2	
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности		2	
	Тематика практических занятий и лабораторных работ	**12**		
	Установка и настройка СЗИ от НСД			ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
	Защита входа в систему (идентификация и аутентификация пользователей)			
	Разграничение доступа к устройствам			
	Управление доступом			
	Использование принтеров для печати конфиденциальных документов. Контроль печати			
	Настройка системы для задач аудита			
	Настройка контроля целостности и замкнутой программной среды			
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности			
Тема 2.6. Эксплуатация средств защиты информации в	**Содержание**	**4**		
	Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.		2	ОК.1; ОК.2; ОК.4; ОК.5;
	Принципы основных методов организации и проведения		1	

компьютерных сетях	технического обслуживания вычислительной техники и других технических средств информатизации			ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
	Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении		2	
	Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам		2	
	Тематика практических занятий и лабораторных работ	**2**		
	Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем			
Тема 2.7. Документация на защищаемую автоматизированную систему	**Содержание**	**2**		
	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.		1	ОК.1; ОК.2; ОК.4; ОК.5; ОК.9; ОК.10 ПК 1.1-1.4 ЛР 01-12
	Тематика практических занятий и лабораторных работ	**2**		
	Оформление основных эксплуатационных документов на автоматизированную систему.			
Примерная тематика самостоятельной работы при изучении МДК.01.04 1. Разработка концепции защиты автоматизированной (информационной) системы 2. Анализ банка данных угроз безопасности информации 3. Анализ журнала аудита ОС на рабочем месте 4. Построение сводной матрицы угроз автоматизированной (информационной) системы 5. Анализ политик безопасности информационного объекта		**6**		

6. Изучение аналитических обзоров в области построения систем безопасности 7. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации			
Промежуточная аттестация по МДК.02.03 в виде Экзамена	**12**		
Самостоятельные работы	**12**		
Всего:	**100**		

Для характеристики уровня освоения учебного материала используются следующие обозначения:

*1 – **ознакомительный** (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т.п.);*

*2 – **репродуктивный** (выполнение деятельности по образцу, инструкции или под руководством);*

*3 – **продуктивный** (самостоятельное планирование и выполнение деятельности, решение проблемных задач).*

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МДК 01.04

3.1. Для реализации программы МДК 02.03 должны быть предусмотрены следующие специальные помещения: Реализация программы предполагает наличие учебного кабинета, лабораторий информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации.

Оборудование учебного кабинета и рабочих мест кабинета:
рабочее место преподавателя;
посадочные места для обучающихся;
аудиовизуальный комплекс;
комплект обучающего материала (комплект презентаций).

Оборудование лаборатории и рабочих мест лаборатории информационных технологий, программирования и баз данных:
рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
дистрибутив устанавливаемой операционной системы;
виртуальная машина для работы с операционной системой (гипервизор);
СУБД;
CASE-средства для проектирования базы данных;
инструментальная среда программирования;
пакет прикладных программ.

Оборудование лаборатории и рабочих мест лаборатории сетей и систем передачи информации:
рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
стенды сетей передачи данных;
структурированная кабельная система;
эмулятор (эмуляторы) активного сетевого оборудования;
программное обеспечение сетевого оборудования.

Оборудование лаборатории и рабочих мест лаборатории программных и программно-аппаратных средств защиты информации:
рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
антивирусный программный комплекс;
программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности.

3.2. Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе.

3.2.1. Основные печатные источники

1.Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 2-е изд.- М.: Горячая линия-Телеком, 2017.
2.Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2017.
3.Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2017.
4.Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2017.

3.2.2. Дополнительные печатные источники:

Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2016.
Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2016. – 224 с.
Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. - СПб.: Питер, 2017 - 703 с.
ГубенковА.А.Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2016. - 88 с.
Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы – М.: Бином, 2017. – 1024 с.
Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бином, 2017. – 704 с.
Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник.-М.: Горячая линия-Телеком., 2016
Кофлер М., Linux. Полное руководство – Питер, 2017. – 800 с.
Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2017
Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.- М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2017.- 531 с.

3.2.3. Периодические издания:

1.Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2.Журналы Защита информации. Инсайд: Информационно-методический журнал
3.Информационная безопасность регионов: Научно-практический журнал

4.Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
5.Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

3.2.4. Электронные источники:

1. ЭБС – ipr.books. Доступ к электронной библиотечной системе для сотрудников техникума и студентов осуществляется при помощи авторизации бесплатно.

Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2.Информационный портал по безопасности www.SecurityLab.ru.
3.Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4.Российский биометрический портал www.biometrics.ru
5.Сайт журнала Информационная безопасность http://www.itsec.ru –
6.Сайт Научной электронной библиотеки www.elibrary.ru
7.Справочно-правовая система «Гарант» » www.garant.ru
8.Справочно-правовая система «Консультант Плюс» www.consultant.ru
9.Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10.Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
11.Федеральный портал «Российское образование www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ «МДК 01.04 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ»

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных)	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ,

систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	исполнении в соответствии с требованиями эксплуатационной документации	экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

Личностные результаты обучающихся фиксируются через сформированность личностных универсальных учебных действий, определяемую по трём основным блокам:

- сформированность основ гражданской идентичности личности;
- готовность к переходу к самообразованию на основе учебно-познавательной мотивации, в том числе готовность к выбранному направлению профильного образования;
- сформированность социальных компетенций, включая ценностно-смысловые установки и моральные нормы, опыт социальных и межличностных отношений, правосознание.

В соответствии с требованиями Стандарта достижение личностных результатов не выносится на итоговую оценку обучающихся, а является предметом оценки эффективности воспитательно-образовательной деятельности техникума. Оценка этих достижений проводится в форме, не представляющей угрозы личности, психологической безопасности и эмоциональному статусу учащегося, и может использоваться исключительно в целях оптимизации личностного развития обучающихся.

Комплексная характеристика общих, профессиональных, личностных результатов составляется на основе Портфолио ученика. Цель Портфолио - собрать, систематизировать и зафиксировать результаты развития ученика, его усилия и достижения в различных областях, демонстрировать весь спектр его способностей, интересов, склонностей, знаний и умений.