Минобрнауки России
ФГБОУ ВО «Тульский государственный университет»
Технический колледж им. С.И. Мосина

УТВЕРЖДАЮ
Заместитель директора колледжа по учебной и производственной практике
_____ **М.В. Хмелевский**
«21» 01 **2023 г.**

УТВЕРЖДАЮ
Заместитель директора колледжа по учебной работе
_____ **И.В. Миляева**
«21» 01 **2023 г.**

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

по профессиональному модулю
«Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

2023 г.

РАССМОТРЕНА

цикловой комиссией информационных технологий

Протокол от «13» января 2023 № 6

Председатель цикловой комиссии _____И.В. Миляева

1.1. Рабочая программа производственной практики по профилю специальности является частью основной профессиональной образовательной программы по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем

1.2. Место производственной практики в структуре основной профессиональной образовательной программы: входит в профессиональный цикл, является частью профессионального модуля ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении».

1.3. Цели и задачи производственной практики – требования к результатам освоения производственной практики по профилю специальности:

В результате освоения производственной практики обучающийся 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.

Результат освоения рабочей программы производственной практики (по профилю специальности) влияет на формирование у студентов профессиональных (ПК) и общих (ОК) компетенций.

Код	**Наименование результата обучения**
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу 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.
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 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
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 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

Код	Наименование результата обучения
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 12.	Способен применять проектный подход в профессиональной деятельности

1.4. Количество часов на освоение программы производственной практики (по профилю специальности) ПП 01.01: 162 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ) ПП 01.01

2.1. Объем производственной практики и виды работы

Вид учебной работы	*Объем часов*
Обязательная учебная нагрузка (всего)	162
в том числе:	
практические занятия	154
Итоговая аттестация в форме зачета	**8**

2.2. Тематический план и содержание производственной практики (по профилю специальности) ПП 01.01

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Тема 1 Вводное занятие	**Практические занятия**	8	
	Инструктаж по технике безопасности противопожарным мероприятиям		
	Ознакомление с предприятием.		
	Изучение организационной структуры предприятия		
	Изучение должностных инструкций на рабочих местах, документооборота		
Тема 2 Выполнение работ по эксплуатации подсистем безопасности автоматизированных систем	**Практические занятия**	54	
	Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации		
	Обслуживание средств защиты информации прикладного и системного программного обеспечения		
	Настройка программного обеспечения с соблюдением требований по защите информации		
	Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам		
	Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением		
	Настройка встроенных средств защиты информации программного обеспечения		
	Проверка функционирования встроенных средств защиты информации программного обеспечения		
	Своевременное обнаружение признаков наличия вредоносного программного обеспечения		
	Обслуживание средств защиты информации в компьютерных системах и сетях		
	Обслуживание систем защиты информации в автоматизированных системах		
	Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем		
	Проверка работоспособности системы защиты информации автоматизированной системы		
	Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации		
	Контроль стабильности характеристик системы защиты информации автоматизированной системы		
	Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем		

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
	Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем		
Тема 3 Выполнение работ по эксплуатации компьютерных сетей	**Практические занятия**	42	
	Ознакомление с размером и структурой компьютерной сети		
	Ознакомление с аппаратными компонентами компьютерной сети		
	Ознакомление с программным обеспечением компьютерной сети		
	Анализ используемых стандартов компьютерных сетей		
	Адресация в компьютерной сети		
	Принципы работы в сети		
	Администрирование сети		
	Изучение технологии функционирования локальной сети на предприятии		
	Изучение технологии функционирования виртуальных сетей на предприятии		
	Изучение особенностей использования глобальных сетей на предприятии		
	Профилактическое обслуживание компьютерных сетей		
	Ознакомление с методами диагностики компьютерной сети на предприятии		
	Модернизация компьютерной сети		
	Оформление технической документации		
Тема 4 Производственная работа на рабочих местах	**Практические занятия**	34	
	выполнение производственных заданий сбор материала по индивидуальному заданию		
Тема 5 Оформление отчёта по практике	**Практические занятия**	16	
	Оформление отчёта по практике		
	Консультации		
Тематика индивидуальных заданий: 1.Особенности организации эксплуатации автоматизированных систем на предприятии 2.Анализ видов атак на автоматизированную систему 3.Построение изолированной программной среды в автоматизированной системе 4.Контроль работы и диагностика неисправностей подсистем защиты информации на предприятии 5.Электропитание компьютерных сетей и средств защиты информации на предприятии 6.Организация системы компьютерной и информационной безопасности подразделения 7.Организация планирования и проведения технических мероприятий, направленных на повышение эффективности функционирования системы компьютерной и информационной безопасности			

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
	8.Технология, анализ технических каналов утечки информации в компьютерных системах подразделения 9.Описание нормативно-методических документов по организационной защите информации в подразделении. 10. Методика выявления возможных способов нарушения информационной безопасности при работе автоматизированных систем обработки информации на предприятии 11. Анализ надежности системы защиты информации в компьютерных системах 12. Реализация системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем 13. Организация защиты информации в системах управления базами данных 14. Особенности эксплуатации технических, программных и аппаратных средств информации в автоматизированных системах 15. Организация аудита базы данных и контроль целостности данных 16. Особенности организации работы подразделений по защите информации на предприятии 17. Анализ угроз и формирование требований к политике безопасности предприятия 18. Особенности организации адекватной политики безопасности на предприятии 19. Поиск уязвимостей и анализ безопасности в автоматизированных системах 20. Реализация разграничения доступа к ресурсам автоматизированных систем 21. Информационная модель нарушителя в автоматизированной системе 22. Способы и методы реализации программной защиты информации в СУБД 23. Организация защиты автоматизированных систем от сетевых угроз 24. Неформальное описание политики безопасности вычислительной системы организации 25. Анализ защищенности автоматизированных систем на предприятии 26. Анализ информационных ресурсов объекта защиты 27. Оценка вероятности атак и случайного разрушения информации 28. Составление вероятностно-временной модели системы защиты объекта 29. Составление субъектно-объектной модели системы защиты объекта 30. Выбор средств защиты информации от неблагоприятных воздействий и атак 31. Организация эксплуатации средств защиты информации		
Зачет		**8**	
Всего		**162**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Оборудование подразделений предприятий и организаций:

- персональные компьютеры, соединенные в локальную компьютерную сеть;
- доступ в глобальные компьютерные сети;
- программно-аппаратное обеспечение общего и профессионального назначения;
- комплект должностных инструкций;
- техническая документация.

.

3.2. Информационное обеспечение обучения

3.2.1. Основные источники

3.2.1. Основные источники

1 Староверова, Н. А. Операционные системы : учебник / Н. А. Староверова. — Санкт-Петербург : Лань, 2019. — 308 с. — ISBN 978-5-8114-4000-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125737

2 Гостев, И. М. Операционные системы : учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453469

3 Операционные системы. Программное обеспечение : учебник / составитель Т. П. Куль. — Санкт-Петербург : Лань, 2020. — 248 с. — ISBN 978-5-8114-4290-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131045

4 Кумскова, И.А. Базы данных : учебник / Кумскова И.А. — Москва : КноРус, 2020. — 400 с. — ISBN 978-5-406-07467-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://book.ru/book/932493

5 Волк, В. К. Базы данных. Проектирование, программирование, управление и администрирование : учебник / В. К. Волк. — Санкт-Петербург : Лань, 2020. — 244 с. — ISBN 978-5-8114-4189-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126933

6 Нестеров, С. А. Базы данных : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва : Издательство Юрайт, 2020. — 230 с. — (Профессиональное образование). — ISBN 978-5-534-11629-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457142

7 Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456638

8 Кутузов, О. И. Инфокоммуникационные системы и сети : учебник / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — Санкт-Петербург : Лань, 2020. — 244 с. — ISBN 978-5-8114-4546-2. — Текст : электронный // Лань : электронно-библиотечная систем— URL: https://e.lanbook.com/book/136177

9 Зараменских, Е. П. Информационные системы: управление жизненным циклом : учебник и практикум для среднего профессионального образования / Е. П. Зараменских. — Москва : Издательство Юрайт, 2020. — 431 с. — (Профессиональное образование). — ISBN 978-5-534-11624-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457148

10Кучуганов, В. Н. Информационные системы: методы и средства поддержки принятия решений : учебное пособие / В. Н. Кучуганов, А. В. Кучуганов. — Москва : Ай Пи Ар Медиа, 2020. — 247 с. — ISBN 978-5-4497-0530-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97179.html

11Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — Санкт-Петербург : Лань, 2020. — 392 с. — ISBN 978-5-8114-5342-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147334

12Журавлев, А. Е. Инфокоммуникационные системы. Программное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — Санкт-Петербург : Лань, 2020. — 376 с. — ISBN 978-5-8114-5343-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147335

13Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453

3.2.2. Дополнительные источники:

1 Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский. — Санкт-Петербург : Лань, 2020. — 120 с. — ISBN 978-5-8114-4192-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126937

2 Операционные системы. Программное обеспечение : учебник / составитель Т. П. Куль. — Санкт-Петербург : Лань, 2020. — 248 с. — ISBN 978-5-8114-4290-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131045

3 Назаров, С. В. Современные операционные системы : учебное пособие / С. В. Назаров, А. И. Широков. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 351 с. — ISBN 978-5-4497-0385-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89474.html

4 Назаров, С.В. Операционные системы. Практикум : учебное пособие / Назаров С.В., Гудыно Л.П., Кириченко А.А. — Москва : КноРус, 2020. — 372 с. — ISBN 978-5-406-07707-8. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/933567

5 Гордеев, С. И. Организация баз данных в 2 ч. Часть 1 : учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 310 с. — (Профессиональное образование). — ISBN 978-5-534-11626-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457145

6 Гордеев, С. И. Организация баз данных в 2 ч. Часть 2 : учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 513 с. — (Профессиональное образование). — ISBN 978-5-534-11625-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457146

7 Нестеров, С. А. Базы данных : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва : Издательство Юрайт, 2020. — 230 с. — (Профессиональное образование). — ISBN 978-5-534-11629-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457142

8 Советов, Б. Я. Базы данных : учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 420 с. — (Профессиональное образование). — ISBN 978-5-

534-09324-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453635

9 Гребешков, А. Ю. Вычислительная техника, сети и телекоммуникации : учебное пособие / А. Ю. Гребешков. — Москва : Горячая линия-Телеком, 2017. — 190 с. — ISBN 978-5-9912-0492-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111047

10 Крук, Б. И. Телекоммуникационные системы и сети : учебное пособие : в 3 томах. Том 1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под редакцией В. П. Шувалова. — 4-е изд., испр. и доп. — Москва : Горячая линия-Телеком, 2018. — 620 с. — ISBN 978-5-9912-0208-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111070

11 Пуговкин, А. В. Основы построения инфокоммуникационных сетей и систем : учебное пособие для вузов / А. В. Пуговкин, Д. А. Покаместов, Я. В. Крюков. — 2-е изд., перераб. и доп. — Санкт-Петербург : Лань, 2020. — 176 с. — ISBN 978-5-8114-5905-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156402

12 Будылдина, Н. В. Сетевые технологии высокоскоростной передачи данных : учебное пособие / Н. В. Будылдина, В. П. Шувалов ; под редакцией В. П. Шувалова. — Москва : Горячая линия-Телеком, 2018. — 342 с. — ISBN 978-5-9912-0536-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111025

13 Гагарина, Л. Г. Разработка и эксплуатация автоматизированных информационных систем : учебное пособие для среднего профобразования / Л. Г. Гагарина, Д. В. Киселев, Е. Л. Федотова ; под ред. Л. Г. Гагариной. - Москва : Форум : Инфра-М, 2007, 2009. - 384 с. : ил.- (Профессиональное образование) . - ISBN 978-5-8199-0316-2. -ISBN 978-5-16-003008-1

14 Симоненко, И. В. Основы технического обслуживания телекоммуникационных систем связи и автоматизации : учебное пособие / И. В. Симоненко, О. В. Петров, В. С. Озарчук. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2020. — 62 с. — ISBN 978-5-7422-6875-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/99826.html

15 Попов, А.А. Эргономика пользовательских интерфейсов в информационных системах : учебное пособие пособие для среднего профобразования / Попов А.А. — Москва : КноРус, 2020. — 304 с. — ISBN

978-5-406-07634-7. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/935936

16 Исаев, Г.Н. Управление информационными системами : учебное пособие / Исаев Г.Н., Роганов А.А. — Москва : КноРус, 2020. — 346 с. — ISBN 978-5-406-07674-3. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/935943

17 Тенгайкин, Е. А. Организация сетевого администрирования. Сетевые операционные системы, серверы, службы и протоколы. Практические работы : учебное пособие / Е. А. Тенгайкин. — Санкт-Петербург : Лань, 2020. — 100 с. — ISBN 978-5-8114-4763-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/139326

18 Оливер, Ибе Компьютерные сети и службы удаленного доступа / Ибе Оливер ; перевод И. В. Синицын. — 2-е изд. — Саратов : Профобразование, 2019. — 335 с. — ISBN 978-5-4488-0054-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87999.html

19 Сергеев, А. Н. Основы локальных компьютерных сетей : учебное пособие для вузов / А. Н. Сергеев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-6475-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147339

20 Ершова, Н. Ю. Организация вычислительных систем : учебное пособие / Н. Ю. Ершова, А. В. Соловьев. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 221 с. — ISBN 978-5-4497-0904-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102024.html

3.2.3. Периодические издания:

1 Системный администратор : [журнал]. - Москва, 2020

2 Программирование : научный журнал / учредители : ФГБОУ ВО МГУ им. М.В.Ломоносова, РАН, Отделение информатики, вычислительной техники и автоматизации РАН. - Москва : Наука, 2020 - . - ISSN 0132-3474. - Текст : электронный // НЭБ eLibrary [сайт]. — URL: https://www.elibrary.ru/title_about_new.asp?id=7966

3 Информационно-управляющие системы : научный журнал / учредитель : ООО «Информационно[управляющие системы». - Санкт-Петербург : Изд-во Санкт-Петербургского государственного университета

978-5-406-07634-7. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/935936

16 Исаев, Г.Н. Управление информационными системами : учебное пособие / Исаев Г.Н., Роганов А.А. — Москва : КноРус, 2020. — 346 с. — ISBN 978-5-406-07674-3. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/935943

17 Тенгайкин, Е. А. Организация сетевого администрирования. Сетевые операционные системы, серверы, службы и протоколы. Практические работы : учебное пособие / Е. А. Тенгайкин. — Санкт-Петербург : Лань, 2020. — 100 с. — ISBN 978-5-8114-4763-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/139326

18 Оливер, Ибе Компьютерные сети и службы удаленного доступа / Ибе Оливер ; перевод И. В. Синицын. — 2-е изд. — Саратов : Профобразование, 2019. — 335 с. — ISBN 978-5-4488-0054-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87999.html

19 Сергеев, А. Н. Основы локальных компьютерных сетей : учебное пособие для вузов / А. Н. Сергеев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-6475-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147339

20 Ершова, Н. Ю. Организация вычислительных систем : учебное пособие / Н. Ю. Ершова, А. В. Соловьев. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 221 с. — ISBN 978-5-4497-0904-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102024.html

3.2.3. Периодические издания:

1 Системный администратор : [журнал]. - Москва, 2020

3.2.4. Интернет-ресурсы:

1 ЭБС Юрайт. - Интернет- ссылка https://urait.ru/

2 ЭБС BOOK.ru. - Интернет- ссылка https://www.book.ru/

3 ЭБС Лань. - Интернет-ссылка https://e.lanbook.com/

4 ЭБС IPRBooks. - Интернет- ссылка http://www.iprbookshop.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Контроль и оценка результатов освоения производственной практики (по профилю специальности) осуществляется руководителем производственной практики от колледжа на основании предварительной оценки руководителя практики от организации, характеристики, наблюдений за самостоятельной работой практиканта и выполнения индивидуальных заданий.

Контроль и оценка результатов освоения профессиональных компетенций

Код и наименование профессиональных компетенций	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	экспертное наблюдение выполнения практических работ, 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	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике

Код и наименование профессиональных компетенций	Критерии оценки	Методы оценки
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	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике

Контроль и оценка результатов освоения общих компетенций

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК 1	- выбор и применение методов и способов решения профессиональных задач в области применения программно-аппаратных и технических средств защиты информации; - оценка эффективности и качества выполнения;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения программы практики - - выполнение заданий практики. - положительный отзыв руководителя практики от предприятия
ОК2	- эффективный поиск необходимой информации; - использование различных источников, включая электронные	
ОК 3	- демонстрация целеустремленности, самообразования и саморазвития	
ОК 4	- демонстрация личной ответственности при принятии коллективных решений	
ОК 5	- демонстрация позитивных коммуникативных навыков и социальной адаптации; - качество принятых организационных решений	
ОК 6	- рейтинг участия во внеаудиторных мероприятиях патриотической направленности	
ОК 7	- демонстрация содействия сохранению окружающей среды;	
ОК 8	- результаты медицинского обследования	
ОК 9	- демонстрация результативного использования информационных технологий в профессиональной деятельности	
ОК 10	- использование профессиональной документацией на государственном и иностранном языках	
ОК 12.	Эффективность организация работы в решении профессиональных задач	

Минобрнауки России
ФГБОУ ВО «Тульский государственный университет»
Технический колледж им. С.И. Мосина

Заместитель директора колледжа по учебной и производственной практике	**Заместитель директора колледжа по учебной работе**
_____**М.В. Хмелевский**	_____**И.В. Миляева**
«21» 01 **2023 г.**	«21» 01 **2023 г.**

Рабочая программа производственной практики (по профилю специальности)

по профессиональному модулю
«Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Тула 2023

РАССМОТРЕНА
Цикловой комиссией информационных технологий

Протокол от «13» января 2023 г. № 6

Председатель цикловой комиссии И.В. Миляева

1.1. Рабочая программа производственной практики по профилю специальности является частью основной профессиональной образовательной программы по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем

1.2. Место производственной практики в структуре основной профессиональной образовательной программы: входит в профессиональный цикл, является частью профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

1.3. Цели и задачи производственной практики – требования к результатам освоения производственной практики по профилю специальности:

В результате освоения производственной практики обучающийся должен иметь практический опыт:

- установки, настройки программных средств защиты информации в автоматизированной системе;
- обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;
- тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ;
- решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;
- применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;
- учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;
- работы с подсистемами регистрации событий;
- выявления событий и инцидентов безопасности в автоматизированной системе

уметь:

- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- применять программные и программно-аппаратные средства для защиты информации в базах данных;

- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
- применять математический аппарат для выполнения криптографических преобразований;
- использовать типовые программные криптографические средства, в том числе электронную подпись;
- применять средства гарантированного уничтожения информации;
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Результат освоения рабочей программы производственной практики (по профилю специальности) влияет на формирование у студентов профессиональных (ПК) и общих (ОК) компетенций.

Код	**Наименование результата обучения**
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
ПК 2.7.	Разрабатывать проектные решения защиты информации на объекте программно-аппаратными средствами
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.

Код	Наименование результата обучения
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
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 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 12.	Способен применять проектный подход в профессиональной деятельности

1.4. Количество часов на освоение программы производственной практики (по профилю специальности) ПП 02.01: 234 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ) ПП 01.01

2.1. Объем производственной практики и виды работы

Вид учебной работы	*Объем часов*
Обязательная учебная нагрузка (всего)	**234**
в том числе:	
практические занятия	226
Итоговая аттестация в форме зачета	**8**

2.2. Тематический план и содержание производственной практики (по профилю специальности) ПП 02.01

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Тема 1 Вводное занятие	**Практические занятия**		
	Инструктаж по технике безопасности противопожарным мероприятиям	**8**	
	Ознакомление с предприятием. Изучение организационной структуры предприятия		
	Изучение должностных инструкций на рабочих местах, документооборота		
Тема 2 Выполнение работ по применению программно-аппаратных средств защиты информации	**Практические занятия**	**108**	
	Комплексный подход к обеспечению информационной безопасности на объекте		
	Методы и средства защиты информации от несанкционированного доступа на объекте		
	Защита информации от несанкционированного доступа в операционных системах на объекте		
	Защита компьютерных систем от вредоносных программ на объекте		
	Защита программных средств от несанкционированного использования и копирования на объекте		
	Средства защиты в вычислительных сетях на объекте		
	Средства обеспечения защиты информации в системах управления базами данных на объекте		
	Анализ принципов построения систем информационной защиты производственных подразделений.		
	Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.		
	Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;		
	Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении		
	Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации		
	Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики		

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
Тема 3 Производственная работа на рабочих местах	**Практические занятия**	**94**	
	Ознакомление с особенностями функционирования систем обеспечения безопасности организации		
	Ознакомление с политикой безопасности организации		
	Изучение внутренних нормативных документов по применению программно-аппаратных средств защиты информации на объекте		
	Участие в организации работ по эксплуатации подсистем безопасности операционных систем		
	Участие в организации работ по эксплуатации программно-аппаратных средств защиты информации		
	Участие в организации работ по выявлению технических каналов утечки информации		
	Ознакомление с методами построения виртуальных частных сетей организации, настройки и эксплуатации межсетевых экранов		
	Ознакомление с маршрутом согласования основных внутренних документов по эксплуатации систем защиты информации		
	Участие в основных этапах проектирования политики безопасности организации;		
	Принимать участие в оформлении технической и технологической документации		
Тема 4 Оформление отчёта по практике	**Практические занятия**	**16**	
	Оформление отчёта по практике		
	Консультации		
Тематика индивидуальных заданий для самостоятельной работы: 1. Архитектура подсистемы безопасности операционной системы и её функции. 2. Идентификация, аутентификация, авторизация. 3. Виды разграничения доступа. 4. Аудит. 5. Критерии защищённости компьютерных систем. 6. Адекватная политика безопасности. 7. Способы аутентификации пользователей в компьютерных системах. 8. Модели разграничения доступа в компьютерных системах. 9. Защита от вирусов и программных закладок. 10. Системы защиты от копирования. 11. Методы противодействия атак на вычислительные сети 12. Исследование алгоритма работы систем защиты. 13. Анализ защищённости компьютерных систем. 14. Межсетевые экраны. 15. Виртуальные частные сети. 16. Модели атак на вычислительные сети.			

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
	17. Виды атак на вычислительные сети. 18. Системы обнаружения атак и вторжений. 19. Обеспечение целостности, достоверности и непротиворечивости данных. 20. Встроенные механизмы защиты информации в системах управления базами данных. 21. Организация защиты локальной сети предприятия от внешних вторжений. 22. Организация защиты персонального компьютера от несанкционированного доступа к данным. 23. Разграничение прав доступа к ресурсам в локальной сети. 24. Организация аудита базы данных и контроль целостности данных. 25. Методы несанкционированного доступа к базам данных и способы защиты от них. 26. Сетевые атаки, средства и методы защиты от них.		
Дифференцированный зачет		**8**	
Всего		**234**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Оборудование подразделений предприятий и организаций:

- персональные компьютеры, соединенные в локальную компьютерную сеть;
- доступ в глобальные компьютерные сети;
- программно-аппаратное обеспечение общего и профессионального назначения;
- комплект должностных инструкций;
- техническая документация.

3.2. Информационное обеспечение обучения

3.2.1 Основные источники:

1 Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под редакцией А. В. Душкина. — Москва : Горячая линия-Телеком, 2018. — 248 с. — ISBN 978-5-9912-0470-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111053

2 Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548

3 Бабаш, А.В. Криптографические методы защиты информации : учебник / Бабаш А.В., Баранова Е.К. — Москва : КноРус, 2020. — 189 с. — ISBN 978-5-406-00169-1.—— Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://book.ru/book/933943

4 Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2020. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450998

3.2.2. Дополнительные печатные источники:

1 Джонс, К. Д. Инструментальные средства обеспечения безопасности : учебное пособие / К. Д. Джонс, М. Шема, Б. С. Джонсон. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 913 с. — ISBN 978-5-4497-0871-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102011.html

2 Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие / С. Н. Никифоров. — 3-е изд., стер. — Санкт-

Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-6352-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/146885

3 Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 431 с. — ISBN 978-5-4497-0935-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102070.html

4 Гельбух, С. С. Сети ЭВМ и телекоммуникации. Архитектура и организация : учебное пособие / С. С. Гельбух. — Санкт-Петербург : Лань, 2019. — 208 с. — ISBN 978-5-8114-3474-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118646

5 Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102069.html

6 Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453

7 Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие / С. Н. Никифоров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-6352-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/146885

8 Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97571.html

9 Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2020. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450277

10 Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин,

А. А. Тарасов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450538

11 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

12 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

13 Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

14 Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

15 Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

16 Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

17 Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

18 Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

19 Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

20 Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

21 Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

22 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

23 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

24 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

25 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

26 Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

27 Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

28 Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

29 Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

30 Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

31 Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

32 ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

33 ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

34 ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

35 ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

36 ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

37 ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

38 ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

39 ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

40 ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

41 ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

42 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

43 ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

44 ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

45 ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

46 ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

47 ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
Номенклатура показателей качества. Ростехрегулирование, 2005.

48 ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

49 ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

50 ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

51 ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

52 ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

53 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

54 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

55 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

56 ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

57 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

58 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

59 Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

60 Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

3.2.3. Периодические издания:

1 Системный администратор : [журнал]. - Москва, 2020

3.2.4. Интернет-ресурсы:

1. ЭБС Юрайт. - Интернет- ссылка https://urait.ru/
2. ЭБС BOOK.ru. - Интернет- ссылка https://www.book.ru/
3. ЭБС Лань. - Интернет-ссылка https://e.lanbook.com/
4. ЭБС IPRBooks. - Интернет- ссылка http://www.iprbookshop.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Контроль и оценка результатов освоения производственной практики (по профилю специальности) осуществляется руководителем производственной практики от колледжа на основании предварительной оценки руководителя практики от организации, характеристики, наблюдений за самостоятельной работой практиканта и выполнения индивидуальных заданий.

Контроль и оценка результатов освоения профессиональных компетенций

Код и наименование профессиональных компетенций	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике

Код и наименование профессиональных компетенций	Критерии оценки	Методы оценки
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 2.7. Разрабатывать проектные решения защиты информации на объекте программно-аппаратными средствами	Демонстрация алгоритма проведения проектных работ по защите информации на объекте программно-аппаратными средствами	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике

Контроль и оценка результатов освоения общих компетенций

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения программы практики - выполнение индивидуальных заданий для самостоятельной работы, - выполнение заданий практики, - положительный отзыв
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и	Демонстрация ответственности за принятые решения, обоснованность самоанализа и	

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
личностное развитие.	коррекция результатов собственной работы	руководителя практики
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Грамотность устной и письменной речи, ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	Соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	Эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	Эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	
ОК 10. Пользоваться профессиональной	Эффективность использования в профессиональной деятельности	

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
документацией на государственном и иностранном языках.	необходимой технической документации, в том числе на английском языке.	
ОК 12. Способен применять проектный подход в профессиональной деятельности	Эффективность организация работы в решении профессиональных задач	

Минобрнауки России
ФГБОУ ВО «Тульский государственный университет»
Технический колледж им. С.И. Мосина

Заместитель директора колледжа по учебной и производственной практике

_____**М.В. Хмелевский**

«21» 01 **2023 г.**

Заместитель директора колледжа по учебной работе

_____**И.В. Миляева**

«21» 01 **2023 г.**

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Тула 2023

РАССМОРЕНА
Цикловой комиссией информационных технологий

Протокол от «13» января 2026 г. № 6

Председатель цикловой комиссии И.В. Миляева

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. Производственная практика (преддипломная), завершает обучение по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.2. Цели и задачи производственной практики (преддипломной) – требования к результатам освоения:

Производственная практика (преддипломная) направлена на углубление первоначального практического опыта обучающегося, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности, а также на подготовку к выполнению выпускной квалификационной работы.

Студенты проходят практику в организациях различных организационно-правовых форм.

В процессе прохождения студентом производственнаяой практики (преддипломной) производится сбор фактического материала по тематике дипломной работы.

1.3. Требования к результатам производственной практики (преддипломной).

Практика имеет целью комплексное освоение обучающимися всех видов профессиональной деятельности по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, формирование общих и профессиональных компетенций, а также приобретение необходимых умений и опыта практической работы по данной специальности.

Техник должен обладать общими компетенциями, включающими в себя способность:

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 3. Планировать и реализовывать собственное профессиональное и личностное развитие.

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 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 9. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

ОК 12 Способен применять проектный подход в профессиональной деятельности

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу 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.

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

ПК 2.7. Разрабатывать проектные решения защиты информации на объекте программно-аппаратными средствами

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.
ПК 3.6. Применять биометрические системы безопасности
ПК 3.7. Разрабатывать проектные решения защиты информации на объекте техническими средствами
ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК 4.4. Обеспечивать применение средств защиты информации в компьютерной системе

По результатам практики руководителями практики от организации и от образовательной организации формируется аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций, а также характеристика на обучающегося по освоению профессиональных компетенций в период прохождения практики.

В период прохождения практики обучающимся ведется дневник практики. По результатам практики обучающимся составляется отчет, который утверждается организацией.

В качестве приложения к дневнику практики обучающийся оформляет графические, аудио-, фото-, видео-, материалы, наглядные образцы изделий, подтверждающие практический опыт, полученный на практике.

1.4. Аттестация по итогам производственной практики

Аттестация по итогам производственной практики проводится с учетом (или на основании) результатов ее прохождения, подтверждаемых документами соответствующих организаций.

Практика завершается зачетом при условии положительного аттестационного листа по практике руководителей практики от организации и образовательной организации об уровне освоения профессиональных компетенций; наличия положительной характеристики организации на обучающегося по освоению общих компетенций в период прохождения практики; полноты и своевременности представления дневника практики и отчета о практике в соответствии с заданием на практику.

Результаты прохождения практики представляются обучающимся в образовательную организацию и учитываются при прохождении государственной итоговой аттестации.

Обучающиеся, не прошедшие практику или получившие отрицательную оценку, не допускаются к прохождению государственной итоговой аттестации.

1.5. Рекомендуемое количество часов на прохождение производственной практики (преддипломной): 144 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

Наименование разделов и тем	Содержание учебного материала.	Объем часов
1	2	3
Производственная практика (преддипломная)		**144**
	Организация перевозки грузов. **Организация перевозки пассажиров.**	
Тема 1. Ознакомление с предприятием	**Содержание учебного материала.**	8
	Инструктаж по технике безопасности противопожарным мероприятиям Ознакомление с предприятием. Изучение организационной структуры предприятия Изучение объекта защиты информации	
Тема 2. Работа в качестве помощников (дублеров) инженерно-технического персонала.	**Содержание учебного материала.**	104
	Анализ возможных угроз информационной безопасности объекта Разработка комплекса мер по обеспечению информационной безопасности объекта	
Тема 3. Систематизация материалов собранных для выполнения отчета по практике и дипломной работы	**Содержание учебного материала.**	24
	Оформление отчёта по практике	
Зачет по практике		**8**

3. Информационное обеспечение обучения
Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

3.2.1. Основные источники

1 Староверова, Н. А. Операционные системы : учебник / Н. А. Староверова. — Санкт-Петербург : Лань, 2019. — 308 с. — ISBN 978-5-8114-4000-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125737

2 Гостев, И. М. Операционные системы : учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453469

3 Операционные системы. Программное обеспечение : учебник / составитель Т. П. Куль. — Санкт-Петербург : Лань, 2020. — 248 с. — ISBN 978-5-8114-4290-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131045

4 Кумскова, И.А. Базы данных : учебник / Кумскова И.А. — Москва : КноРус, 2020. — 400 с. — ISBN 978-5-406-07467-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://book.ru/book/932493

5 Волк, В. К. Базы данных. Проектирование, программирование, управление и администрирование : учебник / В. К. Волк. — Санкт-Петербург : Лань, 2020. — 244 с. — ISBN 978-5-8114-4189-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126933

6 Нестеров, С. А. Базы данных : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва : Издательство Юрайт, 2020. — 230 с. — (Профессиональное образование). — ISBN 978-5-534-11629-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457142

7 Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456638

8 Кутузов, О. И. Инфокоммуникационные системы и сети : учебник / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — Санкт-Петербург : Лань, 2020. — 244 с. — ISBN 978-5-8114-4546-2. — Текст : электронный // Лань : электронно-библиотечная систем— URL: https://e.lanbook.com/book/136177

9 Зараменских, Е. П. Информационные системы: управление жизненным циклом : учебник и практикум для среднего профессионального образования / Е. П. Зараменских. — Москва : Издательство Юрайт, 2020. — 431 с. — (Профессиональное образование). — ISBN 978-5-534-11624-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457148

10 Кучуганов, В. Н. Информационные системы: методы и средства поддержки принятия решений : учебное пособие / В. Н. Кучуганов, А. В. Кучуганов. — Москва : Ай Пи Ар Медиа, 2020. — 247 с. — ISBN 978-5-4497-0530-3. — Текст : электронный //

Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97179.html

11 Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — Санкт-Петербург : Лань, 2020. — 392 с. — ISBN 978-5-8114-5342-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147334

12 Журавлев, А. Е. Инфокоммуникационные системы. Программное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — Санкт-Петербург : Лань, 2020. — 376 с. — ISBN 978-5-8114-5343-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147335

13 Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453

14 Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под редакцией А. В. Душкина. — Москва : Горячая линия-Телеком, 2018. — 248 с. — ISBN 978-5-9912-0470-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111053

15 Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548

16 Бабаш, А.В. Криптографические методы защиты информации : учебник / Бабаш А.В., Баранова Е.К. — Москва : КноРус, 2020. — 189 с. — ISBN 978-5-406-00169-1.—— Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://book.ru/book/933943

17 Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2020. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450998

18 Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с. — ISBN 978-5-4497-0340-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89455.html

19 Мельников, В.П. Информационная безопасность : учебник для среднего профессионального образования / Мельников В.П., Куприянов А.И. — Москва : КноРус, 2018. — 267 с. — ISBN 978-5-406-05072-9.-Текст : электронный // ЭБС Юрайт [сайт]. —— URL: https://book.ru/book/924214

20 Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467356

21 Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 c. — ISBN 978-5-4497-0336-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89451.html

22 Бурькова, Е. В. Физическая защита объектов информатизации : учебное пособие / Е. В. Бурькова. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2017. — 158 с. — ISBN 978-5-7410-1697-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/71349.html

23 Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057

24 Скрипник, Д. А. Обеспечение безопасности персональных данных : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 121 c. — ISBN 978-5-4497-0334-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89449.html

3.2.2. Дополнительные источники:

1 Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский. — Санкт-Петербург : Лань, 2020. — 120 с. — ISBN 978-5-8114-4192-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126937

2 Операционные системы. Программное обеспечение : учебник / составитель Т. П. Куль. — Санкт-Петербург : Лань, 2020. — 248 с. — ISBN 978-5-8114-4290-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131045

3 Назаров, С. В. Современные операционные системы : учебное пособие / С. В. Назаров, А. И. Широков. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 351 c. — ISBN 978-5-4497-0385-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89474.html

4 Назаров, С.В. Операционные системы. Практикум : учебное пособие / Назаров С.В., Гудыно Л.П., Кириченко А.А. — Москва : КноРус, 2020. — 372 с. — ISBN 978-5-406-07707-8. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/933567

5 Гордеев, С. И. Организация баз данных в 2 ч. Часть 1 : учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 310 с. — (Профессиональное образование). — ISBN 978-5-534-11626-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457145

6 Гордеев, С. И. Организация баз данных в 2 ч. Часть 2 : учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 513 с. — (Профессиональное

образование). — ISBN 978-5-534-11625-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457146

7 Нестеров, С. А. Базы данных : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва : Издательство Юрайт, 2020. — 230 с. — (Профессиональное образование). — ISBN 978-5-534-11629-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/457142

8 Советов, Б. Я. Базы данных : учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 420 с. — (Профессиональное образование). — ISBN 978-5-534-09324-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453635

9 Гребешков, А. Ю. Вычислительная техника, сети и телекоммуникации : учебное пособие / А. Ю. Гребешков. — Москва : Горячая линия-Телеком, 2017. — 190 с. — ISBN 978-5-9912-0492-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111047

10 Крук, Б. И. Телекоммуникационные системы и сети : учебное пособие : в 3 томах. Том 1 : Современные технологии / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под редакцией В. П. Шувалова. — 4-е изд., испр. и доп. — Москва : Горячая линия-Телеком, 2018. — 620 с. — ISBN 978-5-9912-0208-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111070

11 Пуговкин, А. В. Основы построения инфокоммуникационных сетей и систем : учебное пособие для вузов / А. В. Пуговкин, Д. А. Покаместов, Я. В. Крюков. — 2-е изд., перераб. и доп. — Санкт-Петербург : Лань, 2020. — 176 с. — ISBN 978-5-8114-5905-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156402

12 Будылдина, Н. В. Сетевые технологии высокоскоростной передачи данных : учебное пособие / Н. В. Будылдина, В. П. Шувалов ; под редакцией В. П. Шувалова. — Москва : Горячая линия-Телеком, 2018. — 342 с. — ISBN 978-5-9912-0536-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111025

13 Гагарина, Л. Г. Разработка и эксплуатация автоматизированных информационных систем : учебное пособие для среднего профобразования / Л. Г. Гагарина, Д. В. Киселев, Е. Л. Федотова ; под ред. Л. Г. Гагариной. -Москва : Форум : Инфра-М, 2007, 2009. - 384 с. : ил.- (Профессиональное образование) . - ISBN 978-5-8199-0316-2. -ISBN 978-5-16-003008-1

14 Симоненко, И. В. Основы технического обслуживания телекоммуникационных систем связи и автоматизации : учебное пособие / И. В. Симоненко, О. В. Петров, В. С. Озарчук. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2020. — 62 с. — ISBN 978-5-7422-6875-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/99826.html

15 Попов, А.А. Эргономика пользовательских интерфейсов в информационных системах : учебное пособие пособие для среднего профобразования / Попов А.А. — Москва : КноРус, 2020. — 304 с. — ISBN 978-5-406-07634-7. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/935936

16 Исаев, Г.Н. Управление информационными системами : учебное пособие / Исаев Г.Н., Роганов А.А. — Москва : КноРус, 2020. — 346 с. — ISBN 978-5-406-07674-3. — Текст : электронный // ЭБС Book.ru [сайт]. — URL: https://book.ru/book/935943

17 Тенгайкин, Е. А. Организация сетевого администрирования. Сетевые операционные системы, серверы, службы и протоколы. Практические работы : учебное пособие / Е. А. Тенгайкин. — Санкт-Петербург : Лань, 2020. — 100 с. — ISBN 978-5-8114-4763-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/139326

18 Оливер, Ибе Компьютерные сети и службы удаленного доступа / Ибе Оливер ; перевод И. В. Синицын. — 2-е изд. — Саратов : Профобразование, 2019. — 335 с. — ISBN 978-5-4488-0054-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87999.html

19 Сергеев, А. Н. Основы локальных компьютерных сетей : учебное пособие для вузов / А. Н. Сергеев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-6475-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147339

20 Ершова, Н. Ю. Организация вычислительных систем : учебное пособие / Н. Ю. Ершова, А. В. Соловьев. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 221 с. — ISBN 978-5-4497-0904-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102024.html

21 Джонс, К. Д. Инструментальные средства обеспечения безопасности : учебное пособие / К. Д. Джонс, М. Шема, Б. С. Джонсон. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 913 с. — ISBN 978-5-4497-0871-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102011.html

22 Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие / С. Н. Никифоров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-6352-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/146885

23 Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 431 с. — ISBN 978-5-4497-0935-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102070.html

24 Гельбух, С. С. Сети ЭВМ и телекоммуникации. Архитектура и организация : учебное пособие / С. С. Гельбух. — Санкт-Петербург : Лань, 2019. — 208 с. — ISBN 978-5-8114-3474-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118646

25 Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102069.html

26 Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97571.html

27 Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2020. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450277

28 Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450538

29 ГОСТ Р 52633-2006.Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. Введ.2007-04-01. М. : Стандартинформ, 2007. IV,20с. : ил. (Защита информации) .

30 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

31 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

32 Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

33 Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

34 Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

35 Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

36 Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

37 Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

38 Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

39 Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

40 Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

41 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

42 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

43 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

44 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

45 Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

46 Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

47 Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

48 Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007г.

49 Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

50 Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

51 ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

52 ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

53 ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

54 ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

55 ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

56 ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

57 ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

58 ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

59 ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

60 ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

61 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

62 ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

63 ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

64 ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

65 ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

66 ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

67 ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

68 ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

69 ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

70 ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

71 ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

72 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

73 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

74 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

75 ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

76 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

77 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

78 Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

79 Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

3.2.3. Периодические издания:

1 Системный администратор : [журнал]. - Москва, 2020

3.2.4. Интернет-ресурсы:

1 ЭБС Юрайт. - Интернет- ссылка https://urait.ru/

2 ЭБС BOOK.ru. - Интернет- ссылка https://www.book.ru/

3 ЭБС Лань. - Интернет-ссылка https://e.lanbook.com/

4 ЭБС IPRBooks. - Интернет- ссылка http://www.iprbookshop.ru/

Минобрнауки России
ФГБОУ ВО «Тульский государственный университет»
Технический колледж им. С.И. Мосина

Заместитель директора колледжа по учебной и производственной практике

_____ **М.В. Хмелевский**

«21» 01 **2023 г.**

Заместитель директора колледжа по учебной работе

_____ **И.В. Миляева**

«21» 01 **2023 г.**

Рабочая программа учебной практики

по профессиональному модулю
«Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Тула 2023

РАССМОТРЕНА
Цикловой комиссией информационных технологий

Протокол от «13» февраля 2023 г. № 6

Председатель цикловой комиссии И.В. Миляеав

Авторы: Борзенкова С.Ю., преподаватель, канд.техн.наук

1.1. Рабочая программа учебной практики по криптографии является частью программы подготовки специалистов среднего звена по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем

1.2. Место учебной практики в структуре основной профессиональной образовательной программы: входит в профессиональный учебный цикл, является частью профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

1.3. Цели и задачи учебной практики – требования к результатам освоения учебной практики:

В результате освоения учебной практики обучающийся должен
иметь практический опыт:

- обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;
- тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ;
- решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;
- применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

уметь:

- применять математический аппарат для выполнения криптографических преобразований;
- использовать типовые программные криптографические средства, в том числе электронную подпись

знать:

- основные понятия криптографии и типовых криптографических методов и средств защиты информации.

Результат освоения рабочей программы учебной практики влияет на формирование студентами общих (ОК) и профессиональных (ПК) компетенций.

Код	Наименование результата обучения
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации,

Код	Наименование результата обучения
	необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
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 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.4. Количество часов на освоение рабочей программы учебной практики:

Максимальная нагрузка студента - 108 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

2.1. Объем учебной практики и виды учебной работы

Вид учебной работы	***Объем часов***
Обязательная аудиторная учебная нагрузка (всего)	108
в том числе:	
практические занятия	102
Итоговая аттестация в форме зачета	6

2.2. Тематический план и содержание учебной практики УП 02.01

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Тема 1 Вводное занятие	**Практические занятия**	2	
	Требования к криптографическим системам защиты информации. Реализация криптографических методов.		
Тема 2 Методы замены	**Практические занятия**	12	
	Одноалфавитная замена Написания алгоритма. Программная реализация метода..		
	Многоалфавитные подстановки. Написания алгоритма. Программная реализация метода..		
	Пропорциональные шифры Написания алгоритма. Программная реализация метода..		
	Метод гаммирования. Написания алгоритма. Программная реализация метода.		
Тема 3 Методы перестановки	**Практические занятия**	10	
	Перестановка с фиксированным периодом d. Написания алгоритма. Программная реализация метода.		
	Перестановка по таблице. Написания алгоритма. Программная реализация метода.		
Тема 4 Блочные шифры с закрытым ключом	**Практические занятия**	30	
	Использование операций в блочных алгоритмах симметричного шифрования. Сеть Фейштеля.		
	Алгоритмы шифрования и расшифрования DES. Написания алгоритма. Программная реализация метода.		
	Алгоритм криптографического преобразования данных ГОСТ 28147-89. Написания алгоритма. Программная реализация метода.		
Тема 5 Поточные шифры и генераторы псевдослучайных чисел	**Практические занятия**	18	
	Поточные шифры. Использование генераторов ПСЧ при потоковом шифровании. Написания алгоритма. Программная реализация метода.		
	Метод Фибоначчи с запаздыванием. Написания алгоритма. Программная реализация метода.		
	Генераторы ПСЧ на основе сдвиговых регистров с обратной связью. Написания алгоритма. Программная реализация метода.		
	Генератор ПСЧ на основе алгоритма BBS. Написания алгоритма. Программная реализация метода.		
	Алгоритм RC4. Написания алгоритма. Программная реализация метода.		

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
Тема 6 Алгоритмы шифрования с открытым ключом	**Практические занятия**	30	
	Алгоритм RSA. Написания алгоритма. Программная реализация метода.		
	Алгоритм Диффи-Хеллана. Написания алгоритма. Программная реализация метода.		
	Алгоритм Эль-Гамаля. Написания алгоритма. Программная реализация метода.		
Зачет		**6**	
Всего		**108**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ПРАКТИКИ

3.1. Оборудование учебной лаборатории программных и программно-аппаратных средств защиты информации и технологий обеспечения информационной безопасности и защищенных информационных систем.

Оборудование лаборатории программных и программно-аппаратных средств защиты информации:

- общее количество посадочных мест;
- рабочие места с персональными компьютерами и сетевым оборудованием;
- рабочее место преподавателя;
- антивирусные программные комплексы; программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности;
- программные и программно-аппаратные средства обнаружения вторжений;
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства выявления уязвимостей в автоматизированных системах и средствах вычислительной техники;
- программные средства криптографической защиты информации;
- комплект демонстрационных стендов.

Оборудование лаборатории технологий обеспечения информационной безопасности и защищенных информационных систем:

- рабочие места с персональными компьютерами и сетевым оборудованием;
- доска для написания маркером;
- проектор;
- экран настенный;
- программно-аппаратные комплексы ФПСУ-IP;
- спектральный анализатор с набором антенн;
- комплект, шумомер с октавными фильтрами;
- нановольтметр;
- аппаратно-программные средства управления доступом к данным;
- средства дублирования и восстановления данных;
- средства мониторинга состояния автоматизированных систем;

- источники бесперебойного и аварийного питания;
- охранная и пожарная сигнализация;
- специализированное оборудование по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок;
- технические средства контроля эффективности защиты информации от утечки по акустическому каналу;
- технические средства контроля эффективности защиты информации от утечки по каналу побочных электромагнитных излучений и наводок;
- средства сканирования защищенности компьютерных сетей;
- устройства чтения смарт-карт и радиометок;
- программно-аппаратный комплекс защиты информации, включая криптографические средства защиты информации.

3.2. Информационное обеспечение обучения

3.2.1 Основные источники:

1 Бабаш, А.В. Криптографические методы защиты информации : учебник / Бабаш А.В., Баранова Е.К. — Москва : КноРус, 2020. — 189 с. — ISBN 978-5-406-00169-1.—— Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://book.ru/book/933943

2 Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2020. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450998

3 Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с. — ISBN 978-5-4497-0340-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89455.html

3.2.2. Дополнительные печатные источники:

1 Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие / С. Н. Никифоров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-6352-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/146885

2 Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97571.html

3 Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2020. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450277

4 Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450538

5 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

7 Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

8 Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

9 Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

10 Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

11 Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

12 Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

13 Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

14 Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

15 Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

16 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

17 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

18 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

19 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

20 Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

21 Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

22 Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

23 Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода

персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

24 Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

25 Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

26 ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

27 ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

28 ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

29 ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

30 ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

31 ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

32 ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

33 ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

34 ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

35 ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

36 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

37 ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

38 ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

39 ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

40 ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

41 ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

42 ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

43 ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

44 ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

45 ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

46 ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

47 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

48 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

49 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

50 ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

51 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

52 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

53 Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

54 Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

3.2.3. Периодические издания:

1 Системный администратор : [журнал]. - Москва, 2020

3.2.4. Интернет-ресурсы:

1. ЭБС Юрайт. - Интернет- ссылка https://urait.ru/
2. ЭБС BOOK.ru. - Интернет- ссылка https://www.book.ru/
3. ЭБС Лань. - Интернет-ссылка https://e.lanbook.com/
4. ЭБС IPRBooks. - Интернет- ссылка http://www.iprbookshop.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения учебной практики осуществляется руководителем учебной практики в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.

Контроль и оценка результатов освоения профессиональных компетенций

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	-- умение применять математический аппарат для выполнения криптографических преобразований; -- умение использовать типовые программные криптографические средства, в том числе электронную подпись - знание основных понятий криптографии и типовых криптографических методов и средств защиты информации	Зачет по учебной практике Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения программы учебной практики - выполнение индивидуальных заданий для самостоятельной работы, - выполнение заданий учебной практики. - положительный отзыв руководителя учебной практики.

Контроль и оценка результатов освоения общих компетенций

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1	- выбор и применение методов и способов решения профессиональных задач в области применения программно-аппаратных и технических средств защиты информации; - оценка эффективности и качества выполнения;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения программы учебной практики - выполнение индивидуальных
ОК2	- эффективный поиск необходимой информации; - использование различных источников, включая электронные	

ОК 3	- демонстрация целеустремленности, самообразования и саморазвития	заданий для самостоятельной работы, - выполнение заданий учебной практики. - положительный отзыв руководителя учебной практики
ОК 4	- демонстрация личной ответственности при принятии коллективных решений	
ОК 5	- демонстрация позитивных коммуникативных навыков и социальной адаптации; - качество принятых организационных решений	
ОК 6	- рейтинг участия во внеаудиторных мероприятиях патриотической направленности	
ОК 7	- демонстрация содействия сохранению окружающей среды;	
ОК 8	- результаты медицинского обследования	
ОК 9	- демонстрация результативного использования информационных технологий в профессиональной деятельности	
ОК 10	- использование профессиональной документацией на государственном и иностранном языках	

Минобрнауки России
ФГБОУ ВО «Тульский государственный университет»
Технический колледж им. С.И. Мосина

Заместитель директора колледжа по учебной и производственной практике

_____**М.В. Хмелевский**

«21» 01 **2023 г.**

Заместитель директора колледжа по учебной работе

_____**И.В. Миляева**

«__» _____ **2023 г.**

Рабочая программа производственной практики (по профилю специальности)

по профессиональному модулю
«Защита информации техническими средствами»

специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Тула 2023

РАССМОТРЕНА
Цикловой комиссией информационных технологий

Протокол от «13» февраля 2023 г. № 6

Председатель цикловой комиссии И.В. Миляева

1.1. Рабочая программа производственной практики по профилю специальности является частью основной профессиональной образовательной программы по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем

1.2. Место производственной практики в структуре основной профессиональной образовательной программы: входит в профессиональный цикл, является частью профессионального модуля ПМ.02 «Защита информации техническими средствами».

1.3. Цели и задачи производственной практики – требования к результатам освоения производственной практики по профилю специальности:

В результате освоения производственной практики обучающийся должен иметь практический опыт:

- установки, монтажа и настройки технических средств защиты информации;
- технического обслуживания технических средств защиты информации;
- применения основных типов технических средств защиты информации;
- выявления технических каналов утечки информации;
- участия в мониторинге эффективности технических средств защиты информации;
- диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;
- проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
- проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;
- установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты

уметь:

- применять технические средства для криптографической защиты информации конфиденциального характера;
- применять технические средства для уничтожения информации и носителей информации;

- применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;
- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
- применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
- применять инженерно-технические средства физической защиты объектов информатизации.

Результат освоения рабочей программы производственной практики (по профилю специальности) влияет на формирование у студентов профессиональных (ПК) и общих (ОК) компетенций.

Код	**Наименование результата обучения**
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.
ПК 3.6.	Применять биометрические системы безопасности
ПК 3.7.	Разрабатывать проектные решения защиты информации на объекте техническими средствами
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 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на

Код	Наименование результата обучения
	государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 12.	Способен применять проектный подход в профессиональной деятельности

1.4. Количество часов на освоение программы производственной практики (по профилю специальности) ПП 03.01: 234 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ) ПП 01.01

2.1. Объем производственной практики и виды работы

Вид учебной работы	*Объем часов*
Обязательная учебная нагрузка (всего)	**234**
в том числе:	
практические занятия	226
Итоговая аттестация в форме зачета	**8**

2.2. Тематический план и содержание производственной практики (по профилю специальности) ПП 03.01

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Тема 1 Вводное занятие	**Практические занятия**		
	Комплексный инструктаж по технике безопасности	**8**	
	Ознакомление с предприятием. Изучение организационной структуры предприятия		
	Изучение должностных инструкций на рабочих местах, документооборота		
Тема 2 Анализ применение инженерно технических средств защиты информации на предприятии (в структурном подразделении)	**Практические занятия**	**108**	
	Комплексный подход к обеспечению информационной безопасности на объекте		
	Инженерно-технические методы и средства защиты информации от несанкционированного доступа		
	Запирающие устройства, организация управления системой		
	Датчиковые оконечные устройства, подсистема сбора и анализа информации		
	Аналоговые оконечные устройства		
	Цифровые оконечные устройства		
	Требования руководящих документов по обеспечению защиты информации		
	Архитектурный анализ объекта		
	Зонирование объекта		
	Методы и средства защиты информации от несанкционированного доступа на объекте		
	Контроль технического состояния (настройки) устройств приборов и агрегатов подсистемы СКУД		
	Расчёт и основание вывода о инженерно-техническом обеспечении и защищённости объекта		
	Обоснование перечня инженерно-технических требований по обеспечению соответствия СКУД объекта требованиям руководящих документов		
Тема 3 Производственная работа на рабочих местах	**Практические занятия**	**94**	
	Ознакомление с особенностями функционирования систем обеспечения безопасности организации		
	Ознакомление с политикой безопасности организации		
	Изучение внутренних нормативных документов по применению инженерно-технических средств защиты информации на объекте		
	Участие в организации работ по обслуживанию подсистем безопасности		
	Участие в организации работ по техническому регламенту и ремонту технических средств		
	Участие в организации работ по выявлению технических каналов утечки информации		

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
	Ознакомление с методами подготовки, настройки и эксплуатации технических средств		
	Ознакомление с маршрутом согласования основных внутренних документов по эксплуатации систем защиты информации		
	Участие в основных этапах проектирования политики безопасности организации;		
	Принимать участие в оформлении технической и технологической документации		
	Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации.		
	Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения, биометрических систем		
	Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам		
	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами		
Тема 4 Оформление отчёта по практике	**Практические занятия**	**16**	
	Оформление отчёта по практике		
	Консультации		
Тематика индивидуальных заданий для самостоятельной работы: 1. Разработка системы технической защиты информации типового объекта 2. Организация инженерно – технической защиты объекта 3. Системы обнаружения вторжений 4. Реализации контрольно-пропускного режима на предприятии 5. Угрозы информации и информационным системам на объекте 6. Методы и средства защиты информации от несанкционированного доступа 7. Демаскирующие признаки объектов защиты информации 8. Теория и методология защиты информации в офисе 9. Применение инженерно-технических средств защиты информации на объекте 10. Защита информации от несанкционированного доступа на объекте 11. Разработка защиты кабинета руководителя 12. Организация контрольно-пропускной системы защиты на объекте 13. Инженерно – техническая защита макро- биосистем			
Зачет		**8**	
Всего		**234**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Оборудование подразделений предприятий и организаций:

- персональные компьютеры, соединенные в локальную компьютерную сеть;
- доступ в глобальные компьютерные сети;
- инженерно-технические средства защиты информации;
- комплект должностных инструкций;
- техническая документация.

.

3.2. Информационное обеспечение обучения

3.2.1. Основные источники:

1 Мельников, В.П. Информационная безопасность : учебник для среднего профессионального образования / Мельников В.П., Куприянов А.И. — Москва : КноРус, 2018. — 267 с. — ISBN 978-5-406-05072-9.-Текст : электронный // ЭБС Юрайт [сайт]. — — URL: https://book.ru/book/924214

2 Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467356

3 Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89451.html

4 Бурькова, Е. В. Физическая защита объектов информатизации : учебное пособие / Е. В. Бурькова. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2017. — 158 с. — ISBN 978-5-7410-1697-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/71349.html

5 Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057

6 Скрипник, Д. А. Обеспечение безопасности персональных данных : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар

Медиа, 2020. — 121 c. — ISBN 978-5-4497-0334-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89449.html

1.2.2. Дополнительные источники:

1 Гельбух, С. С. Сети ЭВМ и телекоммуникации. Архитектура и организация : учебное пособие / С. С. Гельбух. — Санкт-Петербург : Лань, 2019. — 208 с. — ISBN 978-5-8114-3474-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118646

2 Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 368 c. — ISBN 978-5-4497-0931-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102069.html

3 ГОСТ Р 52633-2006.Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. Введ.2007-04-01. М. : Стандартинформ, 2007. IV,20с. : ил. (Защита информации) .

4 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

6 Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

7 Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

8 Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

9 Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

10 Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

11 Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

12 Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

13 Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

14 Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

15 Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

16 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

17 Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

18 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

19 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

20 Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

21 Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

22 Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

23 Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

24 Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

25 ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

26 ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

27 ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

28 ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

29 ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

30 ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

31 ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

32 ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

33 ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

34 ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

35 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

36 ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

37 ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

38 ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

39 ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

40 ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
Номенклатура показателей качества. Ростехрегулирование, 2005.

41 ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

42 ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

43 ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

44 ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

45 ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

46 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

47 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

48 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

49 ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

50 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

51 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

52 Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

53 Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

3.2.3. Периодические издания:

1. Системный администратор : [журнал]. - Москва, 2020

3.2.4 Интернет-ресурсы:

1. ЭБС Юрайт. - Интернет- ссылка https://urait.ru/
2. ЭБС BOOK.ru. - Интернет- ссылка https://www.book.ru/
3. ЭБС Лань. - Интернет-ссылка https://e.lanbook.com/
4. ЭБС IPRBooks. - Интернет- ссылка http://www.iprbookshop.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Контроль и оценка результатов освоения производственной практики (по профилю специальности) осуществляется руководителем производственной практики от колледжа на основании предварительной оценки руководителя практики от организации, характеристики, наблюдений за самостоятельной работой практиканта и выполнения индивидуальных заданий.

Контроль и оценка результатов освоения профессиональных компетенций

Код и наименование профессиональных компетенций	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке ипроведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике

Код и наименование профессиональных компетенций	Критерии оценки	Методы оценки
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 3.6 Применять биометрические системы безопасности	Проявлять умения в применении биометрических систем безопасности	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 3.7 Разрабатывать проектные решения защиты информации на объекте техническими средствами	Демонстрация алгоритма проведения проектных работ по защите информации на объекте техническими средствами	экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике

Контроль и оценка результатов освоения общих компетенций

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения программы практики

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	- выполнение индивидуальных заданий для самостоятельной работы, - выполнение заданий практики, - положительный отзыв руководителя практики
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Демонстрация ответственности за принятые решения, обоснованность самоанализа и коррекция результатов собственной работы	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Грамотность устной и письменной речи, ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	Соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Эффективность выполнения правил ТБ во время производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	Эффективность выполнения правил ТБ при прохождении производственной практики	
ОК 09. Использовать информационные	Эффективность использования информационно-	

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
технологии в профессиональной деятельности.	коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	Эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	
ОК 11. Способен применять проектный подход в профессиональной деятельности	Эффективность организация работы в решении профессиональных задач	