Приложение 7
Приказ об утверждении ООП СПО
№32/1-об от 26.08.2022

Программы практик

по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа учебной практики по профессиональному модулю ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553 и с учетом профессиональных стандартов:

- «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44449)
- «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный N 44464)
- «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный N 43857)
- «Специалист по технической защите информации», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44443)
- «Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 29 декабря 2015 г. N 1179н

Организация-разработчик: Автономная некоммерческая организация среднего профессионального образования «Колледж экономики, страхового дела и информационных технологий КЭСИ» (АНО ПО «КЭСИ»)

•

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ 3

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 6

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ 7

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ 9

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 15

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

1.1. Область применения рабочей программы

Рабочая программа учебной практики по профессиональному модулю ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида деятельности (ВД): ВД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующих общих и профессиональных компетенций (ПК):

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. 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.

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.

1.2. Место практики в структуре образовательной программы

Учебная практика проводится образовательным учреждением при освоении студентами профессиональных компетенций в рамках профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

1.3. Цели и задачи практики - требования к результатам освоения рабочей программы практики:

Практика является обязательным разделом образовательной программы. Она представляет собой вид учебной деятельности в форме практической подготовки, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

С целью овладения видом деятельности ВД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующими профессиональными компетенциями обучающийся в ходе освоения программы учебной практики должен:

Иметь практический опыт	– эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности; – администрировании автоматизированных систем в защищенном исполнении; – установке компонентов систем защиты информации автоматизированных информационных систем.

Уметь	– обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.
Знать	– состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных; – принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.

Планируемые личностные результаты освоения рабочей программы учебной практики

ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм

Количество часов на освоение рабочей программы учебной практики: 36 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Результатом освоения рабочей программы учебной практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении по основному виду деятельности - ВД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении для последующего освоения ими профессиональных компетенций (ПК).

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

Наименование разделов и тем / виды работ	**Содержание учебного материала / содержание работ**	**Объем часов, в том числе в форме практической подготовки**	**Коды компетенций, личностных результатов, формированию которых способствует элемент программы**
1	**2**	**3**	4
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Практические занятия 1. Установка программного обеспечения в соответствии с технической документацией. 2. Настройка параметров работы программного обеспечения, включая системы управления базами данных. 3. Настройка компонентов подсистем защиты информации операционных систем. 4. Управление учетными записями пользователей. 5. Работа в операционных системах с соблюдением действующих требований по защите информации. 6. Установка обновления программного обеспечения. 7. Контроль целостности подсистем защиты информации операционных систем. 8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных. 9. Использование программных средств для архивирования информации. 10. Проведение аудита защищенности автоматизированной системы. 11. Установка, настройка и эксплуатация сетевых операционных систем. 12. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. 13. Организация работ с удаленными хранилищами данных и базами данных. 14. Организация защищенной передачи данных в компьютерных сетях.	**34**	ОК 01-0К 10, ПК 1.1 – ПК 1.4, ЛР 13, ЛР 14

	15. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. 16. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.		
	Дифференцированный зачет	**2**	
	Всего:	**36**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

4.1. Требования к минимальному материально-техническому обеспечению реализации рабочей программы практики:

Учебная практика проводится в учебной организации.

Материально-техническая база соответствует действующим санитарным и противопожарным нормам.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение реализации рабочей программы учебной практики:

Основные источники:

4.2.1 Основные печатные источники:

Макаренко, С.И. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Часть 2. Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях : Учебное пособие / С.И. Макаренко, А.А. Ковальский, С.А. Краснов — Санкт-Петербург : Наукоемкие технологии, 2022. — 358 с. — ISBN 978-5-6044429-8-2. — URL: https://book.ru/book/942928 (дата обращения: 03.12.2022). — Текст : электронный.

Литвинская, О. С., Основы теории передачи информации : учебное пособие / О. С. Литвинская. — Москва : КноРус, 2022. — 194 с. — ISBN 978-5-406-11824-5. — URL: https://book.ru/book/949911 (дата обращения: 03.10.2022). — Текст : электронный.

Кумскова, И. А., Базы данных : учебник / И. А. Кумскова. — Москва : КноРус, 2022. — 400 с. — ISBN 978-5-406-15045-0. — URL: https://book.ru/book/958783 (дата обращения: 04.10.2022). — Текст : электронный.

Ткаченко, С. Н., Основы проектирования баз данных : учебник / С. Н. Ткаченко. — Москва : КноРус, 2022. — 176 с. — ISBN 978-5-406-14991-1. — URL: https://book.ru/book/958706 (дата обращения: 03.10.2022). — Текст : электронный.

Шитов, В. Н., Инженерно-техническая поддержка сопровождения информационных систем : учебник / В. Н. Шитов. — Москва : КноРус, 2022. — 280 с. — ISBN 978-5-406-12650-9. — URL: https://book.ru/book/952137 (дата обращения: 03.10.2022). — Текст : электронный.

Назаров, С. В. Операционные системы : учебное пособие / С. В. Назаров. – Москва : КНОРУС, 2022. – 372 с. : ил. – ISBN 978-5-406-09582-9. – Текст : электронный.

3.2.2. Дополнительные источники

1. Угринович, Н. Д. Информатика : учебник / Н. Д. Угринович. – Москва : КНОРУС, 2022. – 378 с. : ил. – ISBN 978-5-406-09590-4. – Текст : электронный.

2. Угринович, Н. Д. Информатика. Практикум : учебное пособие / Н. Д. Угринович. – Москва : КНОРУС, 2022. – 264 с. : ил. – ISBN 978-5-406-09794-6. – Текст : электронный.

3.2.3. Электронные ресурсы

1. Хабр : сайт. – Москва. – URL: https://habr.com/ru/feed/ (дата обращения: 30.08.2022). – Текст : электронный.

2. LINUX.ORG.RU : сайт. – Москва. – URL: https://www.linux.org.ru/ (дата обращения: 30.08.2022). – Текст : электронный.

4.2.2. Дополнительные печатные источники:

1. Федеральный закон от 29 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 29 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

4. Федеральный закон от 29 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

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

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

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

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

9. 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».

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

11. 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.

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

13. Административный регламент федеральной службы по

техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 г. N 133

14. Административный регламент Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 N 133

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

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

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

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

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

20. 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.

21. 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».

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

23. 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

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

25. ГОСТ Р 34.10-2012. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

26. ГОСТ Р 34-11-2012. "Информационная технология. Криптографическая защита информации. Функция хэширования"

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

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

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

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

31. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

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

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

34. 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.

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

36. 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.

37. 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.

38. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

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

40. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

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

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

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

44. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. Криптографическая защита информации в объектах информационной инфраструктуры. М.: Издательский центр «Академия», 2020.

45. Аверченков В. И., Рытов М. Ю., Шпичак С. А. Криптографические методы защиты информации. – 2-е издание, стереотипное. М.: Общество с ограниченной ответственностью "ФЛИНТА", 2017.

46. Антонов В. А., Абдрахимова Д. И., Новик М. Г. Теоретико-числовые методы в криптографии : Учебное пособие. – Челябинск : Издательский центр ЮУрГУ, 2018. – 51 с.

47. Баричев С.Г., Серов Р.Е., Гончаров В.В. Основы современной криптографии: учеб. пособие. М.: Горячая линия – Телеком, 2018.

48. Карпухин Е. О. Методы скрытой передачи информации: Учебное пособие. – М.: Горячая линия-Телеком, 2020.

49. Коржик В. И., Яковлев В. А. Основы криптографии : Учебное пособие. СПб: Интермедия, 2017.

50. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты

информации: учебное пособие. — 2-е изд., стер. М. : Горячая линия-Телеком, 2017.

4.2.3. Электронные источники:

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

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Контроль и оценка результатов освоения рабочей программы практики осуществляется руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий, выполнения практических проверочных работ.

В результате освоения практики в рамках профессионального модуля обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1 Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрация 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.	Выполнение администрирования программных и программно-аппаратных компоненты автоматизированной (информационной) системы	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.	Демонстрация настройки 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

ПК 1.4 Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Демонстрация проверки технического состояния, выполнение технического обслуживания и ремонта, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	экспертное наблюдение выполнения практических работ; оценка процесса и результатов выполнения видов работ на практике

Рабочая программа учебной практики по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553 и с учетом профессиональных стандартов:

- «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44449)
- «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный N 44464)
- «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный N 43857)
- «Специалист по технической защите информации», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44443)
- «Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 29 декабря 2015 г. N 1179н

Организация-разработчик: Автономная некоммерческая организация среднего профессионального образования «Колледж экономики, страхового дела и информационных технологий КЭСИ» (АНО ПО «КЭСИ»)

•

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ 3

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 6

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ 7

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ 9

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 15

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

1.1. Область применения рабочей программы

Рабочая программа учебной практики по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно - аппаратными средствами является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида деятельности (ВД): ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующих общих и профессиональных компетенций (ПК):

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. 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.

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.

1.2. Место практики в структуре образовательной программы

Учебная практика проводится образовательным учреждением при освоении студентами профессиональных компетенций в рамках профессионального модуля ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

1.3. Цели и задачи практики - требования к результатам освоения рабочей программы практики:

Практика является обязательным разделом образовательной программы. Она представляет собой вид учебной деятельности в форме практической подготовки, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

С целью овладения видом деятельности ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующими профессиональными компетенциями обучающийся в ходе освоения программы учебной практики должен:

иметь практический опыт:

– установке и настройке программных средств защиты информации;

– тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;

– учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

уметь:

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

– использовать типовые программные криптографические средства, в том числе электронную подпись;

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

– 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.

знать:

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

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

Планируемые личностные результаты освоения рабочей программы учебной практики

ЛР 1	Осознающий себя гражданином и защитником великой страны
ЛР 2	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций

Количество часов на освоение рабочей программы учебной практики: 72 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Результатом освоения рабочей программы учебной практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках профессионального модуля ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами по основному виду деятельности - Защита информации в автоматизированных системах программными и программно-аппаратными средствами для последующего освоения ими профессиональных компетенций (ПК).

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

Наименование разделов и тем / виды работ	**Содержание учебного материала / содержание работ**	**Объем часов, в том числе в форме практической подготовки**	**Коды компетенций, личностных результатов, формированию которых способствует элемент программы**
1	**2**	**3**	4
Тема 1.Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Практические занятия	**70**	ОК 01-0К 10, ПК 2.1 – ПК 2.6, ЛР 1, ЛР 2
	Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах. Диагностика, устранение отказов и обеспечение работоспособности программно - аппаратных средств обеспечения информационной безопасности. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. Устранение замечаний по результатам проверки. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.	**70**	

	Применение математических методов для оценки качества и выбора наилучшего программного средства Использование типовых криптографических средств и методов защиты информации. Использование электронной подписи.		
	Дифференцированный зачет	**2**	
	Всего:	**72**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

4.1. Требования к минимальному материально-техническому обеспечению реализации рабочей программы практики:

Учебная практика проводится в учебной организации.

Материально-техническая база соответствует действующим санитарным и противопожарным нормам.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение реализации рабочей программы учебной практики:

Основные источники:

4.2.1 Основные печатные источники:

1. Бабаш, А. В., Криптографические методы и средства защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2022. — 222 с. — ISBN 978-5-406-15474-8. — URL: https://book.ru/book/959682 (дата обращения: 08.12.2022). — Текст : электронный.

2. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2022. — 267 с. — ISBN 978-5-406-13756-7. — URL: https://book.ru/book/955528 (дата обращения: 08.10.2022). — Текст : электронный.

3. Шитов, В. Н., Инженерно-техническая поддержка сопровождения информационных систем : учебник / В. Н. Шитов. — Москва : КноРус, 2022. — 280 с. — ISBN 978-5-406-12650-9. — URL: https://book.ru/book/952137 (дата обращения: 06.09.2022). — Текст : электронный.

4.2.2. Дополнительные печатные источники:

1. Федеральный закон от 29 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 29 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

4. Федеральный закон от 29 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

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

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

7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085

«Вопросы Федеральной службы по техническому и экспортному контролю».

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

9. 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».

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

11. 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.

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

13. Административный регламент федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 г. N 133

14. Административный регламент Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 N 133

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

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

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

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

19. Руководящий документ. Геоинформационные системы. Защита

информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. 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.

21. 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».

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

23. 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

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

25. ГОСТ Р 34.10-2012. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

26. ГОСТ Р 34-11-2012. "Информационная технология. Криптографическая защита информации. Функция хэширования"

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

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

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

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

31. ГОСТ Р 51295-2006 Защита информации. Объект информатизации.

Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

32. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

Номенклатура показателей качества. Ростехрегулирование, 2005.

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

34. 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.

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

36. 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.

37. 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.

38. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

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

40. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

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

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

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

2006 г.

44. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. Криптографическая защита информации в объектах информационной инфраструктуры. М.: Издательский центр «Академия», 2020.

45. Аверченков В. И., Рытов М. Ю., Шпичак С. А. Криптографические методы защиты информации. – 2-е издание, стереотипное. М.: Общество с ограниченной ответственностью "ФЛИНТА", 2017.

46. Антонов В. А., Абдрахимова Д. И., Новик М. Г. Теоретико-числовые методы в криптографии : Учебное пособие. – Челябинск : Издательский центр ЮУрГУ, 2018. – 51 с.

47. Баричев С.Г., Серов Р.Е., Гончаров В.В. Основы современной криптографии: учеб. пособие. М.: Горячая линия – Телеком, 2018.

48. Карпухин Е. О. Методы скрытой передачи информации: Учебное пособие. – М.: Горячая линия-Телеком, 2020.

49. Коржик В. И., Яковлев В. А. Основы криптографии : Учебное пособие. СПб: Интермедия, 2017.

50. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации: учебное пособие. — 2-е изд., стер. М. : Горячая линия-Телеком, 2017.

4.2.3. Периодические издания:

1. Защита информации. Инсайд: Информационно-методический журнал. URL: http://www.inside-zi.ru/

2. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/

3. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

4. Прикладная информатика. Рецензируемый научно-практический журнал. URL: http://www.appliedinformatics.ru/

5. Проблемы информационной безопасности. Компьютерные системы. Ежеквартальный журнал издательства СПбПУ. URL: http://jisp.ru

4.2.4. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp//:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Контроль и оценка результатов освоения рабочей программы практики осуществляется руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий, выполнения практических проверочных работ.

В результате освоения практики в рамках профессионального модуля обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта	**Основные показатели оценки результата**	**Формы и методы контроля и 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
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

Рабочая программа учебной практики по профессиональному модулю ПМ.03 Защита информации техническими средствами разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553 и с учетом профессиональных стандартов:

- «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44449)
- «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный N 44464)
- «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный N 43857)
- «Специалист по технической защите информации», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44443)
- «Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 29 декабря 2015 г. N 1179н

Организация-разработчик: Автономная некоммерческая организация среднего профессионального образования «Колледж экономики, страхового дела и информационных технологий КЭСИ» (АНО ПО «КЭСИ»)

•

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ 3

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 7

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ 8

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ 9

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 15

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

1.1. Область применения рабочей программы

Рабочая программа учебной практики по профессиональному модулю ПМ.03 Защита информации техническими средствами является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида деятельности (ВД): ВД 3 Защита информации техническими средствами и соответствующих общих и профессиональных компетенций (ПК):

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. 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.

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, 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.

1.2. Место практики в структуре образовательной программы

Учебная практика проводится образовательным учреждением при освоении студентами профессиональных компетенций в рамках профессионального модуля ПМ.03 Защита информации техническими средствами.

1.3. Цели и задачи практики - требования к результатам освоения рабочей программы практики:

Практика является обязательным разделом образовательной программы. Она представляет собой вид учебной деятельности в форме практической подготовки, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

С целью овладения видом деятельности ВД.3 Защита информации техническими средствами и соответствующими профессиональными компетенциями обучающийся в ходе освоения программы производственной практики должен:

Иметь практический опыт	– выявлении технических каналов утечки информации; – применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации; – проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации

	объектов информатизации по требованиям безопасности информации; – проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
уметь	– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять инженерно-технические средства физической защиты объектов информатизации.
знать	– физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации; – основные способы физической защиты объектов информатизации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

Планируемые личностные результаты освоения рабочей программы производственной практики:

Код	Личностные результаты
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм

Количество часов на освоение рабочей программы учебной практики: 72 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Результатом освоения рабочей программы учебной практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках профессионального модуля ПМ 03 Защита информации техническими средствами по основному виду деятельности - ВД 3 Защита информации техническими средствами для последующего освоения ими профессиональных компетенций (ПК).

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, 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.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

Наименование разделов и тем / виды работ	Содержание учебного материала / содержание работ	Объем часов, в том числе в форме практической подготовки	Коды компетенций, личностных результатов, формированию которых способствует элемент программы
1	**2**	**3**	4
Защита информации техническими средствами	Практические занятия Измерение параметров физических полей. Определение каналов утечки ПЭМИН. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Установка и настройка технических средств защиты информации. Проведение измерений параметров побочных электромагнитных излучений и наводок. Проведение аттестации объектов информатизации. Анализ методов проведения атак голосового преобразования в биометрических системах верификации дикторов Акустические датчики и применение пьезодатчиков в задачах информационной безопасности Модели комплексной защиты информации с учетом особенностей коммерческой организации	**70**	ОК 01-0К 10, ПК 3.1 – ПК 3.5, ЛР 13, ЛР 14
	Дифференцированный зачет	**2**	
	Всего:	**72**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

4.1. Требования к минимальному материально-техническому обеспечению реализации рабочей программы практики:

Учебная практика проводится в учебной организации.

Материально-техническая база соответствует действующим санитарным и противопожарным нормам.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение реализации рабочей программы учебной практики:

Основные источники:

4.2.1 Основные печатные источники:

1. Бабаш, А. В., Криптографические методы и средства защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2022. — 222 с. — ISBN 978-5-406-15474-8. — URL: https://book.ru/book/959682 (дата обращения: 08.12.2022). — Текст : электронный.

2. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2022. — 267 с. — ISBN 978-5-406-13756-7. — URL: https://book.ru/book/955528 (дата обращения: 08.10.2022). — Текст : электронный.

3. Шитов, В. Н., Инженерно-техническая поддержка сопровождения информационных систем : учебник / В. Н. Шитов. — Москва : КноРус, 2022. — 280 с. — ISBN 978-5-406-12650-9. — URL: https://book.ru/book/952137 (дата обращения: 06.09.2022). — Текст : электронный.

4.2.2. Дополнительные печатные источники:

1. Федеральный закон от 29 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 29 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

4. Федеральный закон от 29 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

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

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

7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085

«Вопросы Федеральной службы по техническому и экспортному контролю».

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

9. 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».

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

11. 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.

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

13. Административный регламент федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 г. N 133

14. Административный регламент Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 N 133

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

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

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

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

19. Руководящий документ. Геоинформационные системы. Защита

информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. 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.

21. 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».

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

23. 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

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

25. ГОСТ Р 34.10-2012. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

26. ГОСТ Р 34-11-2012. "Информационная технология. Криптографическая защита информации. Функция хэширования"

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

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

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

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

31. ГОСТ Р 51295-2006 Защита информации. Объект информатизации.

Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

32. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

Номенклатура показателей качества. Ростехрегулирование, 2005.

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

34. 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.

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

36. 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.

37. 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.

38. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

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

40. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

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

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

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

2006 г.

44. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. Криптографическая защита информации в объектах информационной инфраструктуры. М.: Издательский центр «Академия», 2020.

45. Аверченков В. И., Рытов М. Ю., Шпичак С. А. Криптографические методы защиты информации. – 2-е издание, стереотипное. М.: Общество с ограниченной ответственностью "ФЛИНТА", 2017.

46. Антонов В. А., Абдрахимова Д. И., Новик М. Г. Теоретико-числовые методы в криптографии : Учебное пособие. – Челябинск : Издательский центр ЮУрГУ, 2018. – 51 с.

47. Баричев С.Г., Серов Р.Е., Гончаров В.В. Основы современной криптографии: учеб. пособие. М.: Горячая линия – Телеком, 2018.

48. Карпухин Е. О. Методы скрытой передачи информации: Учебное пособие. – М.: Горячая линия-Телеком, 2020.

49. Коржик В. И., Яковлев В. А. Основы криптографии : Учебное пособие. СПб: Интермедия, 2017.

50. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации: учебное пособие. — 2-е изд., стер. М. : Горячая линия-Телеком, 2017.

4.2.3. Периодические издания:

1. Защита информации. Инсайд: Информационно-методический журнал. URL: http://www.inside-zi.ru/

2. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/

3. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

4. Прикладная информатика. Рецензируемый научно-практический журнал. URL: http://www.appliedinformatics.ru/

5. Проблемы информационной безопасности. Компьютерные системы. Ежеквартальный журнал издательства СПбПУ. URL: http://jisp.ru

4.2.4. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp//:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Контроль и оценка результатов освоения рабочей программы практики осуществляется руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий, выполнения практических проверочных работ.

В результате освоения практики в рамках профессионального модуля обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрация умений по установке, монтажу, настройке и техническому обслуживанию технических средств защиты информации	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.	Осуществление 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, создаваемых техническими средствами обработки информации ограниченного доступа.	Демонстрация умений по измерению параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	экспертное наблюдение выполнения практических работ; оценка процесса и результатов выполнения видов работ на практике

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Демонстрация умений по измерению 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.	Организация работ по физической защите объектов информатизации.	экспертное наблюдение выполнения практических работ; оценка процесса и результатов выполнения видов работ на практике

Рабочая программа учебной практики по профессиональному модулю ПМ.04 Выполнение работ по должности служащего “Консультант в области развития цифровой грамотности населения (цифровой куратор)” разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553

Организация-разработчик: Автономная некоммерческая организация среднего профессионального образования «Колледж экономики, страхового дела и информационных технологий КЭСИ» (АНО ПО «КЭСИ»)

•

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ 3

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 9

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ 10

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ 12

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 14

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

1.1. Область применения рабочей программы

Рабочая программа учебной практики по профессиональному модулю ПМ.04 Выполнение работ по должности служащего “Консультант в области развития цифровой грамотности населения (цифровой куратор)” является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида деятельности (ВД): ВД 4 Консультант в области развития цифровой грамотности населения (цифровой куратор) и соответствующих общих и профессиональных компетенций (ПК):

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. 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.

ДПК 4.1Выполнение подготовительных работ по консультированию граждан в области применения информационно-коммуникационных технологий

ДПК 4.2Ознакомительное индивидуальное консультирование граждан в области информационно-коммуникационных технологий

ДПК 4.3Организационно-техническое обеспечение проведения информационно-просветительских мероприятий, направленных на развитие цифровой грамотности граждан

1.2. Место практики в структуре образовательной программы

Учебная практика проводится образовательным учреждением при освоении студентами профессиональных компетенций в рамках профессионального модуля ПМ.04 Выполнение работ по должности служащего “Консультант в области развития цифровой грамотности населения (цифровой куратор)”.

1.3. Цели и задачи практики - требования к результатам освоения рабочей программы практики:

Практика является обязательным разделом образовательной программы. Она представляет собой вид учебной деятельности в форме практической подготовки, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

С целью овладения видом деятельности ВД 4 Консультант в области развития цифровой грамотности населения (цифровой куратор) и соответствующими профессиональными компетенциями обучающийся в ходе освоения программы учебной практики должен:

Иметь практический опыт	Выполнения подготовительных работ по консультированию граждан в области применения информационно-коммуникационных технологий Ознакомительного индивидуального консультирования граждан в области информационно-коммуникационных технологий Организационно-технического обеспечения проведения информационно-просветительских мероприятий, направленных на развитие цифровой грамотности граждан

Уметь	Уточнять и формализовать проблему, с которой столкнулся гражданин, в ходе диалога с ним Организовывать консультирование граждан с ограниченными возможностями с привлечением специалистов Оформлять заявки на предоставление консультационных услуг в соответствии с установленными формами Обрабатывать персональные данные с соблюдением требований, установленных законодательством Российской Федерации Оказывать консультативную помощь, связанную с оперированием персональными данными самими пользователями (и их защитой) при работе с интернет-сервисами Применять различные методы поиска информации в информационно-телекоммуникационной сети «Интернет» Собирать, анализировать и обобщать информацию по вопросам применения информационно-коммуникационных технологий в соответствии с рабочим заданием Использовать информационно-коммуникационные технологии в профессиональной деятельности Составлять информационные модули о теме, сроках и месте проведения консультаций Передавать информацию о консультациях с применением средств информационно-коммуникационных технологий Вносить информацию в базы данных Работать на персональном компьютере, с различными поисковыми системами, электронной почтой на уровне уверенного пользователя Использовать средства сетевых коммуникаций и социальных сервисов, в том числе мобильных Проводить объяснение, сопровождая показом отдельных действий по применению персональных компьютеров, информационно-

	телекоммуникационной сети «Интернет», онлайн-сервисов, мобильных устройств, технических средств автоматизации платежей (в соответствии с запросом гражданина) Консультировать граждан под руководством специалиста, проявлять самостоятельность при решении типовых задач Вести диалог, учитывая возрастные и индивидуальные особенности собеседника Оценивать результативность проведенной консультации с использованием типовых вопросов и заданий Оформлять документацию о предоставлении консультационной услуги в соответствии с установленными формами Отбирать и применять инструменты обеспечения информационной безопасности Собирать, анализировать и обобщать информацию по вопросам развития компетенций в сфере информационно-коммуникационных технологий Подготавливать презентации Оформлять листовки и буклеты по типовым шаблонам Обеспечивать продвижение информации о проведении мероприятия Регистрировать участников мероприятия Осуществлять информационную поддержку и навигацию участников во время мероприятия Контролировать готовность технического обеспечения мероприятия Опрашивать участников мероприятий Составлять и обрабатывать анкеты, проводить анкетирование Анализировать и обрабатывать информацию по заданным отчетам
Знать	Правила деловой переписки и письменного этикета Правила делового общения и речевого этикета

	Сведения об организациях и специалистах, содействующих в коммуникации с людьми с ограниченными возможностями Требования к оформлению документации Принципы и механизмы работы поисковых систем, функциональные возможности популярных сервисов поиска Критерии отбора и методы структурирования информации Средства информационно-коммуникационных технологий для передачи информации Прикладные программы ведения баз данных Законодательство Российской Федерации в области интеллектуальной собственности, правила использования информационных материалов в информационно-телекоммуникационной сети «Интернет» Законодательство Российской Федерации о персональных данных Нормы русского языка Виды и основные пользовательские характеристики мобильных устройств Основные функции операционных и файловых систем Основные программы, входящие в пакет типовых приложений в составе операционной системы Методы обработки текстовой, численной и графической информации Базовые принципы организации и функционирования компьютерных сетей Принципы построения и функционирования баз данных и особенности работы с ними Программы-браузеры для работы в информационно-телекоммуникационной сети «Интернет», программы электронной почты Основные онлайн-сервисы по оказанию электронных услуг, порталы государственных и муниципальных услуг, в том числе услуг, предоставляемых с использованием электронных

	социальных карт, электронных платежей, электронных очередей, электронной приемной Основные поисковые системы, функциональные возможности популярных сервисов поиска Требования информационной безопасности Правила деловой переписки и письменного этикета Правила оформления информационно-презентационных материалов Программное обеспечение для создания презентаций Порядок организации и проведения групповых и массовых мероприятий Наиболее востребованные информационно-коммуникационные технологии Порядок работы с оргтехникой и правила технической безопасности

Планируемые личностные результаты освоения рабочей программы производственной практики:

Код	**Личностные результаты**
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 17	Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; Предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве
ЛР 18	Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей информации

Количество часов на освоение рабочей программы учебной практики: 216 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Результатом освоения рабочей программы учебной практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках профессионального модуля ПМ.04 Выполнение работ по должности служащего “Консультант в области развития цифровой грамотности населения (цифровой куратор)” по основному виду деятельности - ВД 4 Консультант в области развития цифровой грамотности населения (цифровой куратор) для последующего освоения ими профессиональных компетенций (ПК).

Код	Наименование результата обучения
ДПК 4.1	Выполнение подготовительных работ по консультированию граждан в области применения информационно-коммуникационных технологий
ДПК 4.2	Ознакомительное индивидуальное консультирование граждан в области информационно-коммуникационных технологий
ДПК 4.3	Организационно-техническое обеспечение проведения информационно-просветительских мероприятий, направленных на развитие цифровой грамотности граждан

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

Наименование разделов и тем / виды работ	**Содержание учебного материала / содержание работ**	**Объем часов, в том числе в форме практической подготовки**	**Коды компетенций, личностных результатов, формированию которых способствует элемент программы**
1	**2**	**3**	4
Выполнение работ по должности служащего “Консультант в области развития цифровой грамотности населения (цифровой куратор)”	Практические занятия 1. Ведение непосредственного приема обращений граждан. 2. Электронная коммуникация по обращениям граждан. 3. Поиск и обработка информации, необходимой для проведения консультаций в соответствии с рабочим заданием. 4. Визуальное и дистанционное размещение информации и проведение консультаций. 5. Ведение базы данных граждан, обратившихся за консультацией. 6. Объяснение и демонстрация алгоритма применения информационно-коммуникационных технологий. 7. Информирование о наиболее типичных угрозах при работе в сети, с использованием средств коммуникации. 8. Информирование об основных методах противодействия информационным угрозам. 9. Ответы на вопросы граждан, связанные с цифровой тематикой. 10. Проверка усвоения гражданином продемонстрированного алгоритма действий.	**214**	ОК 01-0К 10, ДПК 4.1 – ДПК 4.3, ЛР 13, ЛР 17, ЛР 18

	11. Передача вводной информации по моделям устройств и их возможностям. 12. Передача вводной информации о цифровых сервисах, доступных через информационно-телекоммуникационную сеть "Интернет". 13. Ведение базы данных по ознакомительным первичным консультациям. 14. Составление отчетной документации о предоставлении ознакомительных консультаций. 15. Подготовка презентационных материалов для проведения просветительских мероприятий в соответствии с рабочим заданием. 16. Подготовка оборудования для проведения информационно-просветительских мероприятий. 17. Организация групповых и массовых мероприятий по развитию цифровой грамотности. 18. Выполнение технических работ для проведения групповых и массовых мероприятий по развитию цифровой грамотности. 19. Проведение опросов и анкетирования по результатам мероприятий, направленных на развитие цифровой грамотности. Подготовка сводной отчетной информации		
	Дифференцированный зачет	**2**	
	Всего:	**216**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

4.1. Требования к минимальному материально-техническому обеспечению реализации рабочей программы практики:

Учебная практика проводится в учебной организации.

Материально-техническая база соответствует действующим санитарным и противопожарным нормам.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение реализации рабочей программы учебной практики:

Основные источники:

4.2.1 Основные печатные источники:

1. Угринович, Н. Д., Информатика : учебник / Н. Д. Угринович. — Москва : КноРус, 2022. — 377 с. — ISBN 978-5-406-13967-7. — URL: https://book.ru/book/958100 (дата обращения: 10.12.2022). — Текст : электронный.

4.2.2. Дополнительные источники:

1. Катунин, Г. П. Технологии создания и обработки цифровой мультимедийной информации: учебник для СПО / Г. П. Катунин. — Саратов: Профобразование, 2021. — 793 с. — ISBN 978-5-4488-1308-5. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/108831

2. Майстренко, А. В. Мультимедийные средства обработки информации: учебное пособие для СПО / А. В. Майстренко, Н. В. Майстренко. — Саратов: Профобразование, 2020. — 81 с. — ISBN 978-5-4488-0734-3. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL:https://profspo.ru/books/90169

3. Стасышин, В. М. Разработка информационных систем и баз данных: учебное пособие для СПО / В. М. Стасышин. — Саратов: Профобразование, 2020. — 100 с. — ISBN 978-5-4488-0527-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/87389.html

4. Технологии создания и публикации цифровой мультимедийной информации: практикум для СПО / Л. Н. Титова, Е. П. Жилко, Э. И. Дяминова, Р. Р. Рамазанова. — Саратов: Профобразование, 2021. — 131 с. — ISBN 978-5-4488-1305-4. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/108656

5. Фролов, А. Б. Основы веб-дизайна. Разработка, создание и сопровождение веб-сайтов: учебное пособие для СПО / А. Б. Фролов, И. А.

Нагаева, И. А. Кузнецов. — Саратов: Профобразование, 2020. — 244 c. — ISBN 978-5-4488-0861-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/96765.html

6. Янцев, В. В. JavaScript и PHP. Content management system / В. В. Янцев. — Санкт-Петербург : Лань, 2022. — 192 с. — ISBN 978-5-507-44845-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/266651

7. Букунов, С. В. Разработка приложений с графическим пользовательским интерфейсом на языке Python / С. В. Букунов, О. В. Букунова. — Санкт-Петербург : Лань, 2023. — 90 с. — ISBN 978-5-507-45192-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/292853

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Контроль и оценка результатов освоения рабочей программы практики осуществляется руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий, выполнения практических проверочных работ.

В результате освоения практики в рамках профессионального модуля обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ДПК 4.1 Выполнение подготовительных работ по консультированию граждан в области применения информационно-коммуникационных технологий	Готовность к ведению непосредственного приема обращений граждан Готовность к электронная коммуникация по обращениям граждан Осуществлён поиск и обработка информации, необходимой для проведения консультаций в соответствии с рабочим заданием Реализовано визуальное и дистанционное размещение информации и проведение консультаций Осуществлено ведение базы данных граждан, обратившихся за консультацией	экспертное наблюдение выполнения практических работ; оценка процесса и результатов выполнения видов работ на практике
ДПК 4.2 Ознакомительное индивидуальное консультирование граждан в области информационно-коммуникационных технологий	Выполнено объяснение и демонстрация алгоритма применения информационно-коммуникационных технологий Выполнено информирование о наиболее типичных угрозах при работе в сети, с	экспертное наблюдение выполнения практических работ; оценка процесса и результатов выполнения видов работ на практике

	использованием средств коммуникации Выполнено информирование об основных методах противодействия информационным угрозам Даны ответы на вопросы граждан, связанные с цифровой тематикой Осуществлена проверка усвоения гражданином продемонстрированного алгоритма действий Осуществлена передача вводной информации по моделям устройств и их возможностям Осуществлена передача вводной информации о цифровых сервисах, доступных через информационно-телекоммуникационную сеть «Интернет» Реализовано ведение базы данных по ознакомительным первичным консультациям Составлена отчетная документация о предоставлении ознакомительных консультаций	
ДПК 4.3 Организационно-техническое обеспечение проведения информационно-просветительских мероприятий, направленных на развитие цифровой грамотности граждан	Подготовлены презентационные материалы для проведения информационно-просветительских мероприятий в соответствии с рабочим заданием Подготовлено оборудование для проведения информационно-просветительских мероприятий Продемонстрирована готовность организации групповых и массовых	экспертное наблюдение выполнения практических работ; оценка процесса и результатов выполнения видов работ на практике

	мероприятий по развитию цифровой грамотности Выполнены технические работы для проведения групповых и массовых мероприятий по развитию цифровой грамотности Продемонстрирована готовность проведения опросов и анкетирования по результатам мероприятий, направленных на развитие цифровой грамотности Подготовлена сводная отчетная информация	

Рабочая программа производственной практики по профессиональному модулю ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553 и с учетом профессиональных стандартов:

- «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44449)
- «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный N 44464)
- «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный N 43857)
- «Специалист по технической защите информации», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44443)
- «Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 29 декабря 2015 г. N 1179н

Организация-разработчик: Автономная некоммерческая организация среднего профессионального образования «Колледж экономики, страхового дела и информационных технологий КЭСИ» (АНО ПО «КЭСИ»)

•

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ 3

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 6

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ 7

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ 10

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 16

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

1.1. Область применения рабочей программы

Рабочая программа производственной практики по профессиональному модулю ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида деятельности (ВД): ВД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующих общих и профессиональных компетенций (ПК):

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. 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.

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.

1.2. Место практики в структуре образовательной программы

Производственная практика проводится образовательным учреждением при освоении студентами профессиональных компетенций в рамках профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

1.3. Цели и задачи практики - требования к результатам освоения рабочей программы практики:

Практика является обязательным разделом образовательной программы. Она представляет собой вид учебной деятельности в форме практической подготовки, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

С целью овладения видом деятельности ВД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующими профессиональными компетенциями обучающийся в ходе освоения программы учебной практики должен:

Иметь практический опыт	– эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности; – администрировании автоматизированных систем в защищенном исполнении; – установке компонентов систем защиты информации автоматизированных информационных систем.

Уметь	– обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.
Знать	– состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных; – принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.

Планируемые личностные результаты освоения рабочей программы учебной практики

ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм

Количество часов на освоение рабочей программы учебной практики: 72 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Результатом освоения рабочей программы производственной практики является сформированность у обучающихся практических профессиональных умений в рамках профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении по основному виду деятельности - ВД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении для последующего освоения ими профессиональных компетенций (ПК).

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

Наименование разделов и тем / виды работ	**Содержание учебного материала / содержание работ**	**Объем часов, в том числе в форме практической подготовки**	**Коды компетенций, личностных результатов, формированию которых способствует элемент программы**
1	**2**	**3**	4
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Практические занятия 1. Разработка технического задания на сопровождение информационной системы в соответствии с предметной областью. 2. Формирование предложения о расширении функциональности информационной системы. 3. Исправление ошибок в программном коде информационной системы в процессе эксплуатации. 4. Инсталляция, настройка и сопровождение информационной системы. 5. Разработка обучающей документации информационной системы. 6. Оценка качества информационной системы на соответствие техническим требованиям. 7. Оценка надежности функционирования информационной системы на соответствие техническим требованиям. 8. Выполнение регламента по обновлению, техническому сопровождению, восстановлению данных информационной системы. 9. Организация доступа пользователей к информационной системе. 10. Определение диапазона IP - адресов подсети. 11. Назначение имён. Установка домена. 12. Подключение дополнительного сервера к домену. 13. Создание зеркальных массивов. 14. Настройка DNCP на основном и дополнительном КД. 15. Создание failover. Настройка свидетельств КД.	**70**	ОК 01-0К 10, ПК 1.1 – ПК 1.4, ЛР 13, ЛР 14

16. Настройка зон просмотра DNS. 17. Загрузка зон прямого и обратного просмотра. 18. Создание групповых политик домена. 19. Настройка стартовых страниц в браузере. 20. Создание подразделений и доменных групп. 21. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 22. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения. 23. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам. 24. Применение нормативно-правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. 25. Установка технических средств защиты информации. 26. Монтаж технических средств защиты информации. 27. Настройка технических средств защиты информации. 28. Техническое обслуживание технических средств защиты информации. 29. Применение основных типов технических средств защиты информации. 30. Применение основных типов программных средств защиты информации. 31. Выявление технических каналов утечки информации. 32. Участие в мониторинге эффективности технических средств защиты информации. 33. Диагностика технических средств защиты информации. 34. Устранение отказов и неисправностей технических средств защиты информации. 35. Восстановление работоспособности технических средств защиты информации. 36. Проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которых установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации. 37. Проведение измерений параметров фоновых шумов, создаваемых техническими средствами защиты информации.	

	38. Проведение измерений параметров физических полей, создаваемых техническими средствами защиты информации. 39. Выявление технических каналов утечки информации. 40. Установка инженерно-технических средств физической защиты. 41. Монтаж и настройка инженерно-технических средств физической защиты. 42. Техническое обслуживание инженерно-технических средств физической защиты. 43. Диагностика, устранение отказов и неисправностей инженерно-технических средств физической защиты. 44. Восстановление работоспособности инженерно-технических средств физической защиты. 45. Разработка обучающей документации информационной системы.		
	Дифференцированный зачет	**2**	
	Всего:	**72**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

4.1. Требования к минимальному материально-техническому обеспечению реализации рабочей программы практики:

Производственная практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся на основе договоров, заключаемых между колледжем и профильными организациями. Материально-техническая база организаций должна соответствовать действующим санитарным и противопожарным нормам.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение реализации рабочей программы производственной практики:

Основные источники:

4.2.1 Основные печатные источники:

Макаренко, С.И. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Часть 2. Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях : Учебное пособие / С.И. Макаренко, А.А. Ковальский, С.А. Краснов — Санкт-Петербург : Наукоемкие технологии, 2022. — 358 с. — ISBN 978-5-6044429-8-2. — URL: https://book.ru/book/942928 (дата обращения: 03.12.2022). — Текст : электронный.

Литвинская, О. С., Основы теории передачи информации : учебное пособие / О. С. Литвинская. — Москва : КноРус, 2022. — 194 с. — ISBN 978-5-406-11824-5. — URL: https://book.ru/book/949911 (дата обращения: 03.10.2022). — Текст : электронный.

Кумскова, И. А., Базы данных : учебник / И. А. Кумскова. — Москва : КноРус, 2022. — 400 с. — ISBN 978-5-406-15045-0. — URL: https://book.ru/book/958783 (дата обращения: 04.10.2022). — Текст : электронный.

Ткаченко, С. Н., Основы проектирования баз данных : учебник / С. Н. Ткаченко. — Москва : КноРус, 2022. — 176 с. — ISBN 978-5-406-14991-1. — URL: https://book.ru/book/958706 (дата обращения: 03.10.2022). — Текст : электронный.

Шитов, В. Н., Инженерно-техническая поддержка сопровождения информационных систем : учебник / В. Н. Шитов. — Москва : КноРус, 2022. — 280 с. — ISBN 978-5-406-12650-9. — URL: https://book.ru/book/952137 (дата обращения: 03.10.2022). — Текст : электронный.

Назаров, С. В. Операционные системы : учебное пособие / С. В. Назаров. – Москва : КНОРУС, 2022. – 372 с. : ил. – ISBN 978-5-406-09582-9. – Текст : электронный.

4.2.2. Дополнительные источники

1. Угринович, Н. Д. Информатика : учебник / Н. Д. Угринович. – Москва : КНОРУС, 2022. – 378 с. : ил. – ISBN 978-5-406-09590-4. – Текст : электронный.

2. Угринович, Н. Д. Информатика. Практикум : учебное пособие / Н. Д. Угринович. – Москва : КНОРУС, 2022. – 264 с. : ил. – ISBN 978-5-406-09794-6. – Текст : электронный.

3.2.3. Электронные ресурсы

1. Хабр : сайт. – Москва. – URL: https://habr.com/ru/feed/ (дата обращения: 30.08.2022). – Текст : электронный.

2. LINUX.ORG.RU : сайт. – Москва. – URL: https://www.linux.org.ru/ (дата обращения: 30.08.2022). – Текст : электронный.

4.2.3. Дополнительные печатные источники:

1. Федеральный закон от 29 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 29 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

4. Федеральный закон от 29 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

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

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

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

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

9. 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».

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

11. 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.

12. Меры защиты информации в государственных информационных

системах. Утверждены ФСТЭК России 11 февраля 2014 г.

13. Административный регламент федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 г. N 133

14. Административный регламент Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 N 133

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

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

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

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

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

20. 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.

21. 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».

22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении

Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

23. 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

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

25. ГОСТ Р 34.10-2012. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

26. ГОСТ Р 34-11-2012. "Информационная технология. Криптографическая защита информации. Функция хэширования"

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

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

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

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

31. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

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

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

34. 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.

35. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных

силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

36. 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.

37. 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.

38. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

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

40. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

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

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

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

44. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. Криптографическая защита информации в объектах информационной инфраструктуры. М.: Издательский центр «Академия», 2020.

45. Аверченков В. И., Рытов М. Ю., Шпичак С. А. Криптографические методы защиты информации. – 2-е издание, стереотипное. М.: Общество с ограниченной ответственностью "ФЛИНТА", 2017.

46. Антонов В. А., Абдрахимова Д. И., Новик М. Г. Теоретико-числовые методы в криптографии : Учебное пособие. – Челябинск : Издательский центр ЮУрГУ, 2018. – 51 с.

47. Баричев С.Г., Серов Р.Е., Гончаров В.В. Основы современной криптографии: учеб. пособие. М.: Горячая линия – Телеком, 2018.

48. Карпухин Е. О. Методы скрытой передачи информации: Учебное пособие. – М.: Горячая линия-Телеком, 2020.

49. Коржик В. И., Яковлев В. А. Основы криптографии : Учебное

пособие. СПб: Интермедия, 2017.

50. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации: учебное пособие. — 2-е изд., стер. М. : Горячая линия-Телеком, 2017.

4.2.4. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru

5. Справочно-правовая система «Гарант» » www.garant.ru

6. Федеральный портал «Российское образование www.edu.ru

7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

8. Российский биометрический портал www.biometrics.ru

9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp//:www.ict.edu.ru

10. Сайт Научной электронной библиотеки www.elibrary.ru

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Контроль и оценка результатов освоения рабочей программы практики осуществляется руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий, выполнения практических проверочных работ.

В результате освоения практики в рамках профессионального модуля обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1 Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрация 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.	Выполнение администрирования программных и программно-аппаратных компоненты автоматизированной (информационной) системы	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.	Демонстрация настройки 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

ПК 1.4 Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Демонстрация проверки технического состояния, выполнение технического обслуживания и ремонта, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	экспертное наблюдение выполнения практических работ; оценка процесса и результатов выполнения видов работ на практике

Рабочая программа производственной практики по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553 и с учетом профессиональных стандартов:

- «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44449)
- «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный N 44464)
- «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный N 43857)
- «Специалист по технической защите информации», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44443)
- «Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 29 декабря 2015 г. N 1179н

Организация-разработчик: Автономная некоммерческая организация среднего профессионального образования «Колледж экономики, страхового дела и информационных технологий КЭСИ» (АНО ПО «КЭСИ»)

•

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ 3

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 7

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ 8

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ 11

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 17

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

1.1. Область применения рабочей программы

Рабочая программа производственной практики по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно - аппаратными средствами является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида деятельности (ВД): ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующих общих и профессиональных компетенций (ПК):

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. 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.

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.

1.2. Место практики в структуре образовательной программы

Производственная практика проводится образовательным учреждением на базе профильных предприятий и организаций при освоении студентами профессиональных компетенций в рамках профессионального модуля ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

1.3. Цели и задачи практики - требования к результатам освоения рабочей программы практики:

Практика является обязательным разделом образовательной программы. Она представляет собой вид учебной деятельности в форме практической подготовки, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

С целью овладения видом деятельности ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующими профессиональными компетенциями обучающийся в ходе освоения программы производственной практики должен:

иметь практический опыт:

– установке и настройке программных средств защиты информации;

– тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных

средств защиты информации;

– учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

уметь:

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

– использовать типовые программные криптографические средства, в том числе электронную подпись;

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

– 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.

знать:

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

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

Планируемые личностные результаты освоения рабочей программы производственной практики

ЛР 1	Осознающий себя гражданином и защитником великой страны
ЛР 2	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций

Количество часов на освоение рабочей программы производственной практики: 144 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Результатом освоения рабочей программы производственной практики является сформированность у обучающихся практических профессиональных умений в рамках профессионального модуля ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами по основному виду деятельности - Защита информации в автоматизированных системах программными и программно-аппаратными средствами для последующего освоения ими профессиональных компетенций (ПК).

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

Наименование разделов и тем / виды работ	**Содержание учебного материала / содержание работ**	**Объем часов, в том числе в форме практической подготовки**	**Коды компетенций, личностных результатов, формированию которых способствует элемент программы**
1	**2**	**3**	4
Тема 1.Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Практические занятия	**142**	ОК 01-0К 10, ПК 2.1 – ПК 2.6, ЛР 1, ЛР 2
	Инструктаж по технике безопасности. Разработка групповой политики безопасности. Конфигурирование автоматизированной системы. Текущий контроль, контроль целостности подсистем ОС. Настройка аппаратных комплексов и подсистем защиты информации операционных систем. Установка обновления программного обеспечения. Установка виртуальных ОС Установка ПО на виртуальных машинах. Настройка сетевых операционных систем. Конфигурирование КС. Выполнение тестирование коммутации КС. Тестирование аппаратных компонентов ЗИ Проведение диагностики ПАСЗИ. Использование специализированного ПО для хранения конфиденциальной информации. Использование специализированного ПО для передачи конфиденциальной информации. Использование специализированного ПО для обработки конфиденциальной	**142**	

	информации. Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем. Применение программных комплексов по уничтожению остаточной информации. Применение аппаратных средств для уничтожения носителей информации. Организация учета носителей конфиденциальной информации Составления регламентов обслуживания ИС. Определение работоспособности ПАСЗИ. Выявление и устранение последствий компьютерных атак ПАСЗИ. Выявление и устранение событий ИС средствами ПАСЗИ. Тестирование параметров сетевых протоколов. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. Организация работ с удаленными хранилищами данных и базами данных. Выполнение монтажа компьютерных сетей. установление и настройка параметров современных сетевых протоколов. Работа в операционных системах с соблюдением действующих требований по защите информации Установка обновления программного обеспечения. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных. Использование программных средств для архивирования информации. Проведение аудита защищенности автоматизированной системы. Настройка сетевых операционных систем. Конфигурирование КС. Выполнение тестирование коммутации КС. Тестирование аппаратных компонентов ЗИ Проведение диагностики ПАСЗИ. Использование специализированного ПО для хранения конфиденциальной информации. Использование специализированного ПО для передачи	

	конфиденциальной информации. Использование специализированного ПО для обработки конфиденциальной информации. 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.		
	Дифференцированный зачет	**2**	
	Всего:	**144**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

4.1. Требования к минимальному материально-техническому обеспечению реализации рабочей программы практики:

Производственная практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся на основе договоров, заключаемых между колледжем и профильными организациями. Материально-техническая база организаций должна соответствовать действующим санитарным и противопожарным нормам.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение реализации рабочей программы учебной практики:

Основные источники:

4.2.1 Основные печатные источники:

1. Бабаш, А. В., Криптографические методы и средства защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2022. — 222 с. — ISBN 978-5-406-15474-8. — URL: https://book.ru/book/959682 (дата обращения: 08.12.2022). — Текст : электронный.

2. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2022. — 267 с. — ISBN 978-5-406-13756-7. — URL: https://book.ru/book/955528 (дата обращения: 08.10.2022). — Текст : электронный.

3. Шитов, В. Н., Инженерно-техническая поддержка сопровождения информационных систем : учебник / В. Н. Шитов. — Москва : КноРус, 2022. — 280 с. — ISBN 978-5-406-12650-9. — URL: https://book.ru/book/952137 (дата обращения: 06.09.2022). — Текст : электронный.

4.2.2. Дополнительные печатные источники:

1. Федеральный закон от 29 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 29 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

4. Федеральный закон от 29 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

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

6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской

Федерации об административных правонарушениях».

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

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

9. 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».

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

11. 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.

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

13. Административный регламент федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 г. N 133

14. Административный регламент Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 N 133

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

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

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

18. Требования к системам обнаружения вторжений. Утверждены

приказом ФСТЭК России от 6 декабря 2011 г. № 638.

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

20. 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.

21. 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».

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

23. 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

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

25. ГОСТ Р 34.10-2012. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

26. ГОСТ Р 34-11-2012. "Информационная технология. Криптографическая защита информации. Функция хэширования"

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

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

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

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

2000.

31. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

32. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

Номенклатура показателей качества. Ростехрегулирование, 2005.

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

34. 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.

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

36. 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.

37. 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.

38. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

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

40. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

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

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

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

44. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. Криптографическая защита информации в объектах информационной инфраструктуры. М.: Издательский центр «Академия», 2020.

45. Аверченков В. И., Рытов М. Ю., Шпичак С. А. Криптографические методы защиты информации. – 2-е издание, стереотипное. М.: Общество с ограниченной ответственностью "ФЛИНТА", 2017.

46. Антонов В. А., Абдрахимова Д. И., Новик М. Г. Теоретико-числовые методы в криптографии : Учебное пособие. – Челябинск : Издательский центр ЮУрГУ, 2018. – 51 с.

47. Баричев С.Г., Серов Р.Е., Гончаров В.В. Основы современной криптографии: учеб. пособие. М.: Горячая линия – Телеком, 2018.

48. Карпухин Е. О. Методы скрытой передачи информации: Учебное пособие. – М.: Горячая линия-Телеком, 2020.

49. Коржик В. И., Яковлев В. А. Основы криптографии : Учебное пособие. СПб: Интермедия, 2017.

50. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации: учебное пособие. — 2-е изд., стер. М. : Горячая линия-Телеком, 2017.

4.2.3. Периодические издания:

1. Защита информации. Инсайд: Информационно-методический журнал. URL: http://www.inside-zi.ru/

2. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/

3. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

4. Прикладная информатика. Рецензируемый научно-практический журнал. URL: http://www.appliedinformatics.ru/

5. Проблемы информационной безопасности. Компьютерные системы. Ежеквартальный журнал издательства СПбПУ. URL: http://jisp.ru

4.2.4. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru

5. Справочно-правовая система «Гарант» » www.garant.ru

6. Федеральный портал «Российское образование www.edu.ru

7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

8. Российский биометрический портал www.biometrics.ru

9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp//:www.ict.edu.ru

10. Сайт Научной электронной библиотеки www.elibrary.ru

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Контроль и оценка результатов освоения рабочей программы практики осуществляется руководителем практики в процессе наблюдения и оценивания самостоятельного выполнения обучающимися заданий.

В результате освоения практики в рамках профессионального модуля обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта	**Основные показатели оценки результата**	**Формы и методы контроля и 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
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

Рабочая программа производственной практики по профессиональному модулю ПМ.03 Защита информации техническими средствами разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553 и с учетом профессиональных стандартов:

- «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44449)
- «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный N 44464)
- «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный N 43857)
- «Специалист по технической защите информации», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44443)
- «Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 29 декабря 2015 г. N 1179н

Организация-разработчик: Автономная некоммерческая организация среднего профессионального образования «Колледж экономики, страхового дела и информационных технологий КЭСИ» (АНО ПО «КЭСИ»)

•

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ 3

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 7

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ 8

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ 10

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ 16

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

1.1. Область применения рабочей программы

Рабочая программа производственной практики по профессиональному модулю ПМ.03 Защита информации техническими средствами является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида деятельности (ВД): ВД 3 Защита информации техническими средствами и соответствующих общих и профессиональных компетенций (ПК):

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. 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.

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, 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.

1.2. Место практики в структуре образовательной программы

Производственная практика проводится образовательным учреждением на базе профильных предприятий и организаций при освоении студентами профессиональных компетенций в рамках профессионального модуля ПМ.03 Защита информации техническими средствами.

1.3. Цели и задачи практики - требования к результатам освоения рабочей программы практики:

Практика является обязательным разделом образовательной программы. Она представляет собой вид учебной деятельности в форме практической подготовки, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

С целью овладения видом деятельности ВД.3 Защита информации техническими средствами и соответствующими профессиональными компетенциями обучающийся в ходе освоения программы производственной практики должен:

Иметь практический опыт	– выявлении технических каналов утечки информации; – применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации; – проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации

	объектов информатизации по требованиям безопасности информации; – проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
уметь	– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять инженерно-технические средства физической защиты объектов информатизации.
знать	– физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации; – основные способы физической защиты объектов информатизации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

Планируемые личностные результаты освоения рабочей программы производственной практики:

Код	Личностные результаты
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм

Количество часов на освоение рабочей программы производственной практики: 180 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Результатом освоения рабочей программы производственной практики является сформированность у обучающихся практических профессиональных умений в рамках профессионального модуля ПМ 03 Защита информации техническими средствами по основному виду деятельности - ВД 3 Защита информации техническими средствами для последующего освоения ими профессиональных компетенций (ПК).

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, 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.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

Наименование разделов и тем / виды работ	**Содержание учебного материала / содержание работ**	**Объем часов, в том числе в форме практической подготовки**	**Коды компетенций, личностных результатов, формированию которых способствует элемент программы**
1	**2**	**3**	4
Защита информации техническими средствами	Практические занятия	**142**	ОК 01-0К 10, ПК 3.1 – ПК 3.5, ЛР 13, ЛР 14
	Инструктаж по технике безопасности. Оценка защищенности речевой информации на основе анализа многомерных данных Усовершенствование комплекса виброакустической оценки защиты речевой информации "VNK -012GL" Влияние шумоочистки на результат оценки акустической защищенности Разработка модели угроз утечки информации по техническим каналам Несанкционированный доступ к ЭВМ. Аспекты безопасность UEFI. Анализ угроз, уязвимостей компьютерных сетей и средств защиты Системы обнаружения вторжений Встраивание идентификационной метки в аудиосигнал с использованием эффекта маскировки в спектре Применение дискретного вейвлет-преобразования для выявления редактированных участков звуковых сигналов Метод многомерного анализа данных в селективных поисковых системах Применение методов многомерного анализа данных при обработке полиграмм для выявления возможного инсайдера Селективный металлодетектор на микроконтроллере	**178**	

	Методика обработки сигналов металлодетекторов Разработка программно-аппаратного комплекса для двухфакторной аутентификации		
	Дифференцированный зачет	**2**	
	Всего:	**180**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

4.1. Требования к минимальному материально-техническому обеспечению реализации рабочей программы практики:

Производственная практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся на основе договоров, заключаемых между колледжем и профильными организациями. Материально-техническая база организаций должна соответствовать действующим санитарным и противопожарным нормам.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение реализации рабочей программы учебной практики:

Основные источники:

4.2.1 Основные печатные источники:

1. Бабаш, А. В., Криптографические методы и средства защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2022. — 222 с. — ISBN 978-5-406-15474-8. — URL: https://book.ru/book/959682 (дата обращения: 08.12.2022). — Текст : электронный.

2. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2022. — 267 с. — ISBN 978-5-406-13756-7. — URL: https://book.ru/book/955528 (дата обращения: 08.10.2022). — Текст : электронный.

3. Шитов, В. Н., Инженерно-техническая поддержка сопровождения информационных систем : учебник / В. Н. Шитов. — Москва : КноРус, 2022. — 280 с. — ISBN 978-5-406-12650-9. — URL: https://book.ru/book/952137 (дата обращения: 06.09.2022). — Текст : электронный.

4.2.2. Дополнительные печатные источники:

1. Федеральный закон от 29 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 29 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

4. Федеральный закон от 29 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

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

6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской

Федерации об административных правонарушениях».

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

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

9. 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».

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

11. 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.

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

13. Административный регламент федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 г. N 133

14. Административный регламент Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 N 133

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

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

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

18. Требования к системам обнаружения вторжений. Утверждены

приказом ФСТЭК России от 6 декабря 2011 г. № 638.

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

20. 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.

21. 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».

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

23. 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

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

25. ГОСТ Р 34.10-2012. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

26. ГОСТ Р 34-11-2012. "Информационная технология. Криптографическая защита информации. Функция хэширования"

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

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

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

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

2000.

31. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

32. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

Номенклатура показателей качества. Ростехрегулирование, 2005.

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

34. 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.

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

36. 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.

37. 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.

38. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

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

40. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

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

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

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

44. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. Криптографическая защита информации в объектах информационной инфраструктуры. М.: Издательский центр «Академия», 2020.

45. Аверченков В. И., Рытов М. Ю., Шпичак С. А. Криптографические методы защиты информации. – 2-е издание, стереотипное. М.: Общество с ограниченной ответственностью "ФЛИНТА", 2017.

46. Антонов В. А., Абдрахимова Д. И., Новик М. Г. Теоретико-числовые методы в криптографии : Учебное пособие. – Челябинск : Издательский центр ЮУрГУ, 2018. – 51 с.

47. Баричев С.Г., Серов Р.Е., Гончаров В.В. Основы современной криптографии: учеб. пособие. М.: Горячая линия – Телеком, 2018.

48. Карпухин Е. О. Методы скрытой передачи информации: Учебное пособие. – М.: Горячая линия-Телеком, 2020.

49. Коржик В. И., Яковлев В. А. Основы криптографии : Учебное пособие. СПб: Интермедия, 2017.

50. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации: учебное пособие. — 2-е изд., стер. М. : Горячая линия-Телеком, 2017.

4.2.3. Периодические издания:

1. Защита информации. Инсайд: Информационно-методический журнал. URL: http://www.inside-zi.ru/

2. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/

3. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

4. Прикладная информатика. Рецензируемый научно-практический журнал. URL: http://www.appliedinformatics.ru/

5. Проблемы информационной безопасности. Компьютерные системы. Ежеквартальный журнал издательства СПбПУ. URL: http://jisp.ru

4.2.4. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru

5. Справочно-правовая система «Гарант» » www.garant.ru

6. Федеральный портал «Российское образование www.edu.ru

7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

8. Российский биометрический портал www.biometrics.ru

9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp//:www.ict.edu.ru

10. Сайт Научной электронной библиотеки www.elibrary.ru

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Контроль и оценка результатов освоения рабочей программы практики осуществляется руководителем практики в процессе наблюдения и оценивания самостоятельного выполнения обучающимися заданий.

В результате освоения практики в рамках профессионального модуля обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрация умений по установке, монтажу, настройке и техническому обслуживанию технических средств защиты информации	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.	Осуществление 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, создаваемых техническими средствами обработки информации ограниченного доступа.	Демонстрация умений по измерению параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	экспертное наблюдение выполнения практических работ; оценка процесса и результатов выполнения видов работ на практике

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Демонстрация умений по измерению 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.	Организация работ по физической защите объектов информатизации.	экспертное наблюдение выполнения практических работ; оценка процесса и результатов выполнения видов работ на практике

Рабочая программа преддипломной практики разработана на основе Федерального государственного образовательного стандарта для специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 № 1553, и учебного плана образовательной программы специалистов среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Организация-разработчик: Автономная некоммерческая организация среднего профессионального образования «Колледж экономики, страхового дела и информационных технологий КЭСИ» (АНО ПО «КЭСИ»)

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

1.1. Область применения рабочей программы

Рабочая программа производственной (преддипломной) практики является частью образовательной программы специалистов среднего профессионального образования в соответствии с ФГОС по специальности СПО 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» в части освоения основных видов профессиональной деятельности (ВПД):

ВПД 1. «Эксплуатация автоматизированных (информационных) систем в защищѐнном исполнении» и соответствующих профессиональных компетенций:

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.

ВПД 2. «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и соответствующих профессиональных компетенций:

ПК 2.1. Осуществлять установку и настройку отдельных программных, программноаппаратных средств защиты информации.

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

ПК 2.3. Осуществлять тестирование функций отдельных программных и программноаппаратных 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 программноаппаратных средств обнаружения, предупреждения и ликвидации последствии компьютерных атак.

ВПД 3. «Защита информации техническими средствами» и соответствующих профессиональных компетенций:

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств 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 изменение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4. Осуществлять изменение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информации.

1.2. Цели и задачи производственной (преддипломной) практики

В процессе прохождения производственной (преддипломной) практики приобретается и обновляется полученный ранее (в процессе прохождения предыдущих учебных и производственных практик) практический опыт:

- производить установку и настройку компонентов автоматизированных (информационных систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации;
- администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении;
- обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации;
- осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении;
- осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации;
- обеспечивать защиту информации в автоматизированных системах отдельными программами, программно- аппаратными средствами;
- осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации;
- осуществлять обработку, хранение и передачу информации ограниченного доступа;
- уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств;
- осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных программно-аппаратных средств обнаружения, предупреждения и ликвидации последствии компьютерных атак;
- осуществлять установку, монтаж, настройку и техническое обслуживание технических средств информации в соответствии с требованиями эксплуатационной документации;
- осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации;
- осуществлять изменение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа;
- осуществлять изменение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;
- организовывать отдельные работы по физической защите объектов информации;

Приобретаются или подтверждаются ранее приобретенные (в ходе теоретического обучения и прохождения учебных и производственных практик) умения:

- обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;
- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;
- организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;
- настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- 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 программноаппаратных средств обнаружения, предупреждения;
- 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;

Подтверждаются полученные в ходе теоретического обучения знания:

- состав и принципы работы автоматизированных систем, операционных систем и сред;
- принципы разработки алгоритмов программ, основных приемов программирования;
- модели баз данных;
- принципы построения, физические основы работы периферийных устройств;
- теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;
- порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;
- принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;
- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
- типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
- основные понятия криптографии и типовых криптографических методов и средств защиты информации;
- особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
- типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;
- порядок технического обслуживания технических средств защиты информации;
- номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
- физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

- методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;
- номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;
- основные принципы действия и характеристики технических средств физической защиты;
- основные способы физической защиты объектов информатизации;

номенклатуру применяемых средств физической защиты объектов информатизации; требования техники безопасности при работе с вычислительной техникой;

1.3. Количество часов на производственную (преддипломную) практику

Производственная (преддипломная) практика по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» проводится на завершающем этапе подготовки специалистов среднего звена после освоения программ профессиональных модулей, освоения теоретического и практического обучения и сдачи обучающимися всех видов промежуточной аттестации, предусмотренных ФГОС СПО по данной специальности.

Производственная (преддипломная) практика проводится в течение 4 недель, или 144 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Результатом освоения программы производственной (преддипломной) практики является овладение обучающимися видами профессиональной деятельности: эксплуатация автоматизированных (информационных) систем в защищѐнном исполнении; защита информации в автоматизированных системах программными и программно-аппаратными средствами; защита информации техническими средствами; выполнение работ по одной или нескольким профессиям рабочих, должностям служащих, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

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
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программноаппаратных 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 программноаппаратных 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 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, 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
Код	**Наименование результата обучения**

ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня
ОК 09.	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.

3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ (преддипломной) ПРАКТИКИ

Наименование разделов и тем практики	Содержание учебного материала (дидактические единицы)	Объем часов
Формирование требований	1. Обследование объекта и подготовительная работа с экспертами 2. Обоснование необходимости создания или модификации ИС в защищенном исполнении. 3. Формирование требований к пользователям ИС	12
Разработка концепции ИС	1. Изучение объекта с точки зрения функциональной и организационной структуры 2. Изучение объекта с точки зрения организации и содержания документооборота 3. Проведение необходимых научно-исследовательских работ 4. Разработка вариантов концепции ИС 5. Выбор варианта концепции ИС, удовлетворяющего требованиям пользователей	36
Техническое задание	1. Разработка и утверждение плана технического задания на создание или модификацию ИС в защищенном исполнении 2. Детализация разделов плана технического задания на создание или модификацию ИС в защищенном исполнении 3. Утверждение технического задания на создание ИС в защищенном исполнении	12
Эскизный проект	1. Обоснование предварительных проектных решений по отдельным частям ИС. 2. Обоснование предварительных проектных решений по ИС в целом. 3. Разработка предварительных проектных решений по отдельным частям ИС в защищенном исполнении. 4. Разработка предварительных проектных решений по ИС в целом. 5. Разработка документации на ИС в целом и на ее отдельные части.	36
Технический проект	1. Разработка проектных решений по отдельным частям ИС в защищенном исполнении 2. Разработка проектных решений по ИС в целом.	12
Рабочая документация	1. Разработка рабочей документации на внедрение ИС 2. Разработка документации по техническому сопровождению ИС в период эксплуатации. 3. Разработка документации по обучению пользователей работе с ИС 4. Формирование справочной интерактивной поддержки ИС. 5. Создание или адаптация Интернет-ресурса поддержки ИС.	36
Итого		144

4. УСЛОВИЯ ПРОВЕДЕНИЯ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

4.1. Общие требования к организации производственной (преддипломной) практики

На производственную (преддипломную) практику допускаются обучающиеся, полностью выполнившие учебный план и не имеющие задолженности.

Производственная (преддипломная) практика обучающихся по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» имеет *целью* практическую апробацию и закрепление знаний, полученных в процессе теоретического обучения.

На практике обучающиеся должны исследовать организацию, являющуюся базой практики, соотнести полученные теоретические знания с конкретным опытом, получить необходимые практические навыки работы в области прикладной информатики.

Обязательным условием допуска к производственной (преддипломной) практике является освоение учебного материала и учебной практики для получения первичных, профессиональных умений и навыков, производственной практики, освоенных профессиональных и общих компетенций, в рамках профессиональных модулей:

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищѐнном исполнении.

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

ПМ.03 Защита информации техническими средствами.

ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

Для проведения производственной (преддипломной) практики предусматривается следующая документация:

- график практики;
- рабочая программа практики;
- договоры (соглашения) образовательной организации с базовыми организациями и предприятиями;
- приказ о закреплении обучающихся по базам практики и назначении руководителей практикой от образовательной организации и предприятий;
- дневник практики;
- отчеты по практике;
- характеристика обучающегося по освоению профессиональных компетенций в период прохождения практики*;*
- индивидуальное задание по практике*;*

По итогам производственной (преддипломной) практики проводится защита в формедифференцированного зачета на основе отчета, выполненного индивидуального задания и дневника практики.

Отчет должен содержать анализ деятельности организации (предприятия), выводы о приобретенных навыках, освоении профессиональных компетенций и возможности применения теоретических знаний, полученных при обучении (в форме прототипов проектных решений с учетом особенностей содержания деятельности организации, имеющегося программно-аппаратного обеспечения, выбранной технологии и инструментальных средств разработки объекта выпускной квалификационной работы).

4.2. Обязанности руководителя практики от учебного заведения

Преподаватель колледжа, назначенный руководителем практики обучающихся:

- обеспечивает проведение всех организационных мероприятий перед выездом обучающихся на практику (инструктаж, выдачу договора, индивидуального задания);
- устанавливает связь с руководителями практики от организации и совместно с ними составляет рабочую программу проведения практики;
- разрабатывает тематику индивидуальных заданий;
- принимает участие в распределении обучающихся по рабочим местам или перемещении их по видам работ;

- осуществляет контроль за соблюдением сроков практики и ее содержанием в соответствии с утвержденной программой и индивидуальным заданием;
- оказывает обучающимся методическую помощь при выполнении ими индивидуальных заданий и сборе материалов;
- несет ответственность совместно с руководителем практики от организации за создание на базах практики нормальных условий труда обучающихся и за соблюдение ими правил техники безопасности;
- руководит проектно-исследовательской работой обучающихся в соответствии с индивидуальным заданием;
- оценивает результаты выполнения обучающимися программы практики, проверяет отчет о прохождении практики, дает отзыв о работе;
- принимает участие в работе комиссии по защите отчетов.

4.3. Обязанности руководителя практики от организации

В соответствии с заключенным с колледжем договором, руководитель практики от организации:

- организует практику обучающихся в полном соответствии с положением и программой (заданием) практики.
- совместно с руководителем практики от колледжа, при участии обучающихся разрабатывает индивидуальные календарные планы-графики прохождения практики.
- оказывает содействие в сборе, систематизации и анализе первичной информации по индивидуальному заданию.
- оказывает обучающимся содействие в выборе и уточнении тем выпускных квалификационных работ, представляющих практический интерес для предприятия. - обеспечивает обучающихся необходимыми консультациями по всем вопросам, входящим в задание по практике, с привлечением специалистов предприятия.
- контролирует выполнение обучающимися задания на практику и правила внутреннего распорядка.
- по окончании практики дает характеристику о работе обучающихся с оценкой освоения общих и профессиональных компетенций.

4.4. Права и обязанности обучающихся в период практики

При прохождении практики обучающиеся имеют право:

- получать необходимую информацию для выполнения задания;
- пользоваться библиотекой предприятия и с разрешения главных специалистов и руководителей подразделений информационными фондами и техническими архивами предприятия;
- получать компетентную консультацию специалистов предприятия по вопросам, предусмотренным заданием на практику;
- с разрешения руководителя практикой от предприятия и руководителя подразделения пользоваться вычислительной и оргтехникой для обработки информации, связанной с выполнением задания по практике
- пользоваться услугами подразделений непроизводственной инфраструктуры предприятия

(столовой, спортсооружениями и т.п.) В
период практики обучающиеся обязаны:

- полностью и самостоятельно выполнять задания, предусмотренные программой и календарным планом практики;
- осуществлять сбор, систематизацию, обработку и анализ первичной и иллюстративных материалов;
- регулярно вести записи в дневнике практики о характере выполняемой работы и заданий и своевременно представлять его для контроля руководителям практики;
- выполнять существующие на предприятии правила внутреннего распорядка, строго соблюдать правила охраны труда;
- обеспечить необходимое качество и нести равную со штатными работниками ответственность за выполняемую работу по плану подразделения и ее результаты;

- представить руководителю практики отчет о выполнении задания в полном объеме и защитить его.

За невыполнения задания по практике в установленный срок обучающийся получает неудовлетворительную оценку, за что к нему применяются санкции как к неуспевающему, вплоть до отчисления из колледжа.

При нарушении обучающихся трудовой дисциплины и правил внутреннего распорядка предприятия, он может быть отстранен от прохождения практики, о чем сообщается заместителю директора по учебной работе и производственному обучению и по их предложению директор может рассматривать вопрос об отчислении обучающихся из колледжа.

4.5 Информационное обеспечение практики

Стандарты и нормативные акты.

Группа 1: Программный продукт. Базовые документы.

1. Система добровольной сертификации программного обеспечения средств измерений и информационно-измерительных систем и аппаратно-программных комплексов - Правила функционирования.
2. Система добровольной сертификации программного обеспечения средств измерений и информационно-измерительных систем - Порядок применения знака соответствия.
3. Федеральный закон Российской Федерации от 26 июня 2008 года N 102-ФЗ Об обеспечении единства измерений.
4. ГОСТ Р ИСО/МЭК 9126-93 Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению.
5. ГОСТ Р ИСО/МЭК 12119-2000 Информационная технология. Пакеты программ. Требования к качеству и тестирование.
6. ГОСТ Р ИСО 9127-94 Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов.
7. Рекомендация KOOMET R/LM/10:2004 Программное обеспечение средств измерений. Общие технические требования.
8. МИ 2955-2005 ГСИ. Типовая методика аттестации программного обеспечения средств измерений и порядок еѐ проведения.
9. МИ 2174-91 ГСИ. Аттестация алгоритмов и программ обработки данных при измерениях.

Основные положения

Группа 2: Прочие документы. ГОСТы, МИ, рекомендации.

1. ГОСТ Р ИСО/МЭК ТО 12182-2002 Информационная технология. Классификация программных средств.
2. ГОСТ Р ИСО/МЭК 12207-99 Информационная технология. Процессы жизненного цикла программных средств.
3. ГОСТ Р ИСО/МЭК 14764-2002 Информационная технология. Сопровождение программных средств.
4. ГОСТ Р ИСО/МЭК 15026-2002 Информационная технология. Уровни целостности систем и программных средств.
5. ГОСТ Р ИСО/МЭК ТО 15271-2002 Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207. (Процессы жизненного цикла программных средств).
6. ГОСТ Р ИСО/МЭК 15910-2002 Информационная технология. Процесс создания документации пользователя программного средства.
7. ГОСТ 19.001-77 Единая система программной документации. Общие положения.
8. ГОСТ 19.005-85 Единая система программной документации. Р-схемы алгоритмов и программ. Обозначения условные графические и правила выполнения.
9. ГОСТ 19.105-78 ЕСПД. Общие требования к программным документам.
10. ГОСТ 19.301-79 ЕСПД. Программа и методика испытаний. Требования к содержанию и оформлению.

11. ГОСТ 19.505-79 ЕСПД. Руководство оператора. Требования к содержанию и оформлению.
12. ГОСТ 28195-89 Оценка качества программных средств. Общие положения.
13. ГОСТ 28195-99 Оценка качества программных средств. Общие положения.
14. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
15. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
16. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
17. ГОСТ Р ИСО/МЭК 8631-94 Информационная технология. Программные конструктивы и условные обозначения для их представления.
18. ГОСТ Р ИСО/МЭК ТО 9294-93 Информационная технология. Руководство по управлению документированием программного обеспечения.
19. ГОСТ 19.701-90 (ИСО 5807-85) ЕСПД. Схемы алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения.
20. ГОСТ 34.320-96 Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы.
21. МИ 2612-2000 ГСИ. Метрологические критерии оценки соответствия качества объекта сертификации нормативным требованиям.
22. Р 50.1.027-2001 - Информационные технологии поддержки жизненного цикла продукции. Автоматизированный обмен технической информацией. Основные положения и общие требования.
23. Р 50.1.028-2001 Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования.
24. Р 50.1.029-2001 Информационные технологии поддержки жизненного цикла продукции. Интерактивные электронные технические руководства. Общие требования к содержанию, стилю и оформлению.
25. Р 50.1.030-2001 Информационные технологии поддержки жизненного цикла продукции. Интерактивные электронные технические руководства. Требования к логической структуре базы данных.
26. Р 50.1.031-2001 Информационные технологии поддержки жизненного цикла продукции. Терминологический словарь. Часть 1. Стадии жизненного цикла продукции. Часть 2. Терминология, относящаяся к применению серии стандартов ГОСТ Р ИСО 10303.

Основная литература:

1. 1. Бабаш, А. В., Криптографические методы и средства защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2022. — 222 с. — ISBN 978-5-406-15474-8. — URL: https://book.ru/book/959682 (дата обращения: 08.12.2022). — Текст : электронный.
2. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2022. — 267 с. — ISBN 978-5-406-13756-7. — URL: https://book.ru/book/955528 (дата обращения: 08.10.2022). — Текст : электронный.
3. Шитов, В. Н., Инженерно-техническая поддержка сопровождения информационных систем : учебник / В. Н. Шитов. — Москва : КноРус, 2022. — 280 с. — ISBN 978-5-406-12650-9. — URL: https://book.ru/book/952137 (дата обращения: 06.09.2022). — Текст : электронный.

5.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОИЗВОДСТЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Контроль и оценка результатов прохождения преддипломной практики осуществляется руководителем ВПР, руководителем отдела практик в процессе выполнения обучающимися работ на предприятии, а также сдачи обучающимся отчета по практике.

Формой отчетности обучающимся по преддипломной практике является письменный ***отчет о выполнении работ и приложений*** к отчету, свидетельствующих о закреплении знаний, умений, приобретении практического опыта, формировании общих и профессиональных компетенций, освоении профессиональных модулей.

Обучающийся в течение первой недели после окончания практики сдает руководителю ВКР на проверку отчет по преддипломной практике и защищает отчет по практике в установленные сроки. По результатам защиты обучающимся отчетов выставляется дифференцированный зачет по практике.

Отчет о прохождении преддипломной практики составляется по результатам самостоятельной работы обучающимся по реализации практической части выпускной квалификационной работы и содержательно включает в себя предварительный вариант разрабатываемых проектных решений с учетом особенностей деятельности организации и решаемых задач.

Структурно отчет соответствует практической части выпускной квалификационной работы и включает в себя следующие компоненты (применительно к разработке интернет-ресурса):

1. Выбор и установка инструментальных средств разработки интернет-ресурса. Здесь осуществляются выбор и, при необходимости, установка и настройка инструментальных средств, предполагаемых к использованию при разработке интернет-ресурса.
2. Разработка макета интернет-ресурса. Здесь выполняется создание макета интернет-ресурса в соответствии с его структурой (совокупность отдельных блоков или страниц с их связями, типы и порядок взаимодействия с пользователем, возможные шаблоны и т.п.).
3. Разработка дизайна интернет-ресурса. Здесь для интернет-ресурса в целом и его отдельных компонентов разрабатываются решения по их представлению на экране воспроизводящего устройства (порядок размещения на экране, цветовое и шрифтовое оформление, порядок воспроизведения и оформление мультимедийных компонентов, использование тех или иных спецэффектов, адаптация под различные типы экранов воспроизводящих устройств и т.п.)
4. HTML-разметка компонентов интернет-ресурса. Здесь выполняется HTML-разметка необходимых компонентов разрабатываемого ресурса.
5. Веб-программирование компонентов интернет-ресурса. Здесь выполняется вебпрограммирование необходимых компонентов интернет-ресурса.
6. Тестирование компонентов интернет-ресурса. Здесь осуществляется тестирование созданных в пп. 4 и 5 компонентов интернет-ресурса.
7. Отладка компонентов интернет-ресурса. Здесь по результатам выполнения п. 6 осуществляется отладка тех компонентов интернет-ресурса, в которых обнаружены ошибки.
8. Оформление разработанных проектных решений. Здесь совокупность отлаженных компонентов интернет-ресурса в готовом для эксплуатации виде устанавливается на локальном устройстве с веб-сервером, разрабатывается и оформляется техническая и эксплуатационная документация

Результаты (освоенные профессиональные и общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и 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	Наличие вотчете и полнота материалов анализа данных системному и прикладному программному обеспечению, собранных в процессе практики
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	- Проявлять умения и практического опыта администрирования программных и программно- аппаратных компонентов автоматизированной	Наличие в отчете и полнота материалов анализа данных системному и прикладному программному обеспечению, собранных в процессе практики
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	- Проводить перечень работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Наличие в отчете и полнота материалов анализа данных системному и прикладному программному обеспечению, собранных в процессе практики
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	Наличие в отчете и полнота материалов анализа данных системному и прикладному программному обеспечению, собранных в процессе практики

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	- -обеспечение бесперебойного функционирования вычислительной сети в соответствии с техническими условиями и нормативами обслуживания; - проведение необходимых тестовых проверок и профилактических осмотров; - осуществление мониторинга использования вычислительной сети; - фиксирование и анализ сбоев в работе серверного и сетевого оборудования; - обеспечение своевременного выполнения профилактических работ; - своевременное выполнение мелкого ремонта оборудования; - фиксирование необходимости - внеочередного обслуживания программнотехнических средств; - соблюдение нормы затрат материальных ресурсов и времени; - ведение технической и отчетной документации	Наличие в отчете и полнота материалов анализа данных.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программами, программноаппаратными средствами..	- администрирование размещѐнных сетевых ресурсов; - поддержание актуальности сетевых ресурсов; - организация доступа к локальным и глобальным сетям, в том числе, в сети Интернет; - обеспечение обмена информацией с - другими организациями с использованием электронной почты; - контролирование использования сети Интернет и электронной почты; - сопровождение почтовой системы; - применение новых технологий системного администрирования	Наличие в отчете и полнота материалов анализа данных.
ПК 2.3 Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	- обеспечение наличия программно-технических средств сбора данных для анализа показателей использования и функционирования компьютерной сети; - осуществление мониторинга производительности сервера; - протоколирование системных и сетевых событий; - протоколирование события доступа к ресурсам; - применение нормативно-технической документации в области информационных технологий	Наличие в отчете и полнота материалов анализа данных.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа..	- совместное планирование; - развитие программно-технической базы организации; - обоснование предложения по реализации стратегии в области - информационных технологий; - определение влияния системного администрирования на процессы других подразделений	Наличие в отчете и полнота материалов анализа данных.
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программноаппаратных средств	- Демонстрировать умения и практические навыки уничтожать информацию и носители информации с использованием программных и программноаппаратных средств	Наличие в отчете и полнота материалов анализа данных системному и прикладному программному обеспечению, собранных в процессе практики
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	- Демонстрировать умения и практические навыки 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	Наличие в отчете требований к информационному ресурсу и описания конфигурации прикладного ПО
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 и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Наличие в отчете и полнота материалов анализа данных системному и прикладному программному обеспечению, собранных в процессе практики
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	Наличие в отчете и полнота материалов анализа данных системному и прикладному программному обеспечению, собранных в процессе практики

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, 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	Наличие в отчете и полнота материалов анализа данных системному и прикладному программному обеспечению, собранных в процессе практики
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	Наличие в отчете материалов по работе с клиентами.
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	Наличие в отчете и полнота материалов анализа данных системному и прикладному программному обеспечению

Результаты (освоенные профессиональные и 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 образовательной программы Экспертное наблюдение и оценка при выполнении

ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- - использование различных источников, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач	работ по производственной (преддипломной) практике Дифференцированный зачет
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,	
Результаты (освоенные профессиональные и общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
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 информационнокоммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- - эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	
ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.	- - эффективность использования знаний по финансовой грамотности, планирование предпринимательской деятельности в профессиональной сфере	

Процедура аттестации и система оценивания успеваемости и достижений обучающихся

Итогом преддипломной практики является оценка (дифференцированный зачет – «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»), которая выставляется руководителем практики от учебного заведения на основании наблюдений за самостоятельной работой практиканта и выполненного им индивидуального задания (предварительным вариантом практической части дипломного проекта).