Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное
профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

РАБОЧАЯ ПРОГРАММА
УП.02.01 УЧЕБНОЙ ПРАКТИКИ

по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

квалификация

техник по защите информации

Белгород 2020 г.

Рабочая программа учебной практики разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности **10.02.04 Обеспечение информационной безопасности телекоммуникационных систем**, и примерной основной образовательной программы Федерального учебно-методического объединения в системе СПО по укрупненным группам профессий, специальностей 10.00.00 «Информационная безопасность» квалификация **техник по защите информации** (Организация разработчик: **Федеральное учебно-методическое объединение в системе среднего профессионального образования по укрупненной группе специальностей 10.00.00 «Информационная безопасность», 2017 год).**

Рассмотрено цикловой комиссией Протокол заседания № 1 от «31» августа 2020г. Председатель цикловой комиссии _____/Чобану Л.А./	Согласовано Зам.директора по УМР _____/Бакалова Е.Е. «31» августа 2020 г.	Утверждаю Зам.директора по УР _____ /Выручаева Н.В. «31» августа 2020 г.
Рассмотрено цикловой комиссией Протокол заседания № 1 от «___» августа 2021 г. Председатель цикловой комиссии _____/_____		
Рассмотрено цикловой комиссией Протокол заседания № 1 от «___» августа 2022 г Председатель цикловой комиссии _____/_____		
Рассмотрено цикловой комиссией Протокол заседания № 1 от «___» августа 2023 г Председатель цикловой комиссии _____/_____		

Организация-разработчик: ОГАПОУ «Белгородский индустриальный колледж»
Составитель:
преподаватель ОГАПОУ «Белгородский индустриальный колледж» Внукова Н.В.
Экспертиза:
(*внутренний рецензент*) ОГАПОУ «Белгородский индустриальный колледж», преподаватель ОГАПОУ «Белгородский индустриальный колледж» Солдатенко М.Н.
(*внешний рецензент*) Генеральный директор ООО «Фортуна» Мочалов В.И.

СОДЕРЖАНИЕ

стр.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Рабочая программа учебной практики (далее рабочая программа) – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в части освоения основного вида профессиональной деятельности (ВПД):

ВД 1 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

и соответствующих профессиональных компетенций (ПК):

ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.

ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.

ПК 2.3. Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Рабочая программа учебной практики может быть использована в

– в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки);

– в профессиональной подготовке по профессиям рабочих: техник по защите информации.

Опыт работы не требуется.

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

Основной целью учебной практики является углубление и закрепление теоретических знаний, полученных в процессе обучения; приобретение необходимых профессиональных навыков работы в соответствующих учреждениях в рамках профессионального модуля.

Задачами учебной практики являются:

– формирование у обучающихся знаний, умений и навыков, профессиональных компетенций, профессионально значимых личностных качеств;

– развитие профессионального интереса;

– формирование целостного отношения к профессиональной деятельности, готовности к выполнению профессиональных задач в соответствии с нормами морали, профессиональной этики и служебного этикета;

– адаптация обучающихся к профессиональной деятельности.

С целью овладения указанным видом профессиональной деятельности ВД 1 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты и соответствующими профессиональными компетенциями обучающийся в ходе освоения учебной практики должен:

иметь практический опыт:

– определения необходимых средств криптографической защиты информации;

– использования программно-аппаратных криптографических средств защиты информации;

– установки, настройки специализированного оборудования криптографической защиты информации;

– применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;

– шифрования информации.

1.3. Количество часов на освоение рабочей программы учебной практики:

на учебную практику отводится 72 часа (2 недели).

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения учебной практики является овладение обучающимися видом профессиональной деятельности (ВПД) ВД 1 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 2.1.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3.	Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.
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 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

3.1. Тематический план учебной практики

Коды формируемых компетенций	**Наименование профессионального модуля**	**Объём времени, отведённый на учебную практику (в часах, неделях)**
ПК 2.1, ПК 2.2, ПК 2.3 **ОК 01, ОК 02, ОК 03, ОК 04, ОК 09, ОК 10**	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	**72 часа (2 недели)**

3.2. Содержание учебной практики

Наименование тем учебной практики	Содержание учебной практики		Объем часов	Уровень освоения
1	2		3	4
Раздел ПМ 02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты			**72**	
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			**42**	
Тема 1.1. Обеспечение безопасности операционных систем	Содержание		**6**	
	1	Инструктаж по технике безопасности. Определение целей и задач практики. Требования к оформлению отчетной документации	2	**2**
	2	Средства идентификации аутентификации операционных систем	4	**3**
Тема 1.2. Технологии разграничения доступа	Содержание		**18**	
	1	Администрирование межсетевого экрана	6	**3**
	2	Ознакомление, подключение, настройка системы резервного копирования	6	**3**
	3	Администрирование системы резервного копирования	6	**3**
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	Содержание		**6**	
	1	Подключение, установка драйверов, настройка программных средств шифрования (Криптон или др.)	6	**3**
Тема 1.4. Технологии обнаружения вторжений	Содержание		**6**	
	1	Ознакомление, подключение, настройка системы антивирусной защиты	2	**3**
	2	Администрирование системы антивирусной защиты	4	**3**
Тема 1.5. Методы управления средствами защиты	Содержание		**6**	
	1	Аудит безопасности информационной системы	6	**3**
МДК 02.02. Криптографическая защита информации			**30**	
	Содержание		**6**	**3**

Тема 2.1. Основы криптографических методов защиты информации	**1**	Составление алгоритма шифра	6	
Тема 2.2. Современные стандарты шифрования	Содержание		**6**	**3**
	1	Администрирование программных средств шифрования	6	
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	Содержание		**18**	**3**
	1	Составление алгоритма хеш-функции	2	
	2	Подключение, установка драйверов, настройка аппаратных средств шифрования	4	
	3	Администрирование аппаратных средств шифрования	6	
	4	Зачетное занятие	6	
Всего:			**72**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы учебной практики предполагает проведение учебной практики в мастерских профессиональной образовательной организации и требует наличия оборудования, инструментов, расходных материалов, обеспечивающих выполнение всех видов работ, определенных содержанием программ профессиональных модулей в соответствии с выбранной траекторией, в том числе оборудования и инструментов, используемых при проведении чемпионатов WorldSkills и указанных в инфраструктурных листах конкурсной документации WorldSkills по компетенции «Кибербезопасность» (или их аналогов).

Оборудование и технические средства на рабочем месте:

- автоматизированные рабочие места на 12-15 обучающихся (процессор не ниже Core i3, оперативная память объемом не менее 8 Гб) или аналоги;
- автоматизированное рабочее место преподавателя (процессор не ниже Core i3, оперативная память объемом не менее 8 Гб) или аналоги;
- сервер в лаборатории (8-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 16 Гб, жесткие диски общим объемом не менее 1 Тб, программное обеспечение: WindowsServer 2012 или более новая версия) или выделение аналогичного по характеристикам виртуального сервера из общей фермы серверов;
- проектор и экран;
- маркерная доска;
- программное обеспечение общего и профессионального назначения.

4.2. Требования к документации, необходимой для проведения практики

По итогам прохождения учебной практики предоставляется:

- отчет о практике;
- дневник учебной практики;
- утвержденный отзыв-характеристика о работе обучающегося.

4.3. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

3.2.1. Печатные издания

1. Бубнов, А.А. Основы информационной безопасности [Текст]: учеб. пособие для студентов учреждений среднего проф. образования / А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинкин. - 3-е изд., стер. - М.: Академия, 2017. - 256 с. - (Профессиональное образование. Информационная безопасность).

2. Защита информационных технологий. Справочник: справочник / Ю.И. Коваленко. - М.: Русайнс, 2016. - 321 с. - http://www.book.ru/book/ 921524

3. Информационная безопасность.: учебник / Мельников В.П. под ред., Куприянов А.И. — Москва: КноРус, 2019. — 267 с. — (СПО).

4. Информационная безопасность: учебник / Мельников В.П. под ред., Куприянов А.И. — Москва: КноРус, 2019. — 267 с. — (СПО). — URL: https://book.ru/book/932059 (дата обращения: 01.11.2019). — Текст: электронный.

5. Новикова Е. Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи [Текст]: учебник для использования в образовательном процессе образовательных организаций, реализующих программы среднего профессионального образования по специальности "Инфокоммуникационные сети и системы связи" / Е. Л. Новикова. - Москва: Академия, 2018. – 192 с.

6. Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

7. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябовд.Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2016. – 363 с.

8. Томаси У. Электронные системы связи.- М.: Техносфера, 2016. -1360с.

3.2.2. Электронные издания (электронные ресурсы)

Интернет-ресурсы:

1. Бабаш, А.В. Криптографические методы защиты информации: учебник / Бабаш А.В., Баранова Е.К. — Москва: КноРус, 2019. — 189 с. — URL: https://book.ru/book/933943 (дата обращения: 01.11.2019). — Текст: электронный.

2. Баранова, Е.К. Криптографические методы защиты информации. Лабораторный практикум +CD: учебное пособие / Баранова Е.К., Бабаш А.В. — Москва: КноРус, 2017. — 196 с. — URL: https://book.ru/book/920017 (дата обращения: 01.11.2019). — Текст: электронный

3. Голиков А.М. Кодирование в телекоммуникационных системах [Электронный ресурс]: учебное пособие Курс лекций, компьютерный практикум, задание на самостоятельную работу / А.М. Голиков. - Электрон. текстовые данные. - Томск: Томский государственный университет систем

управления и радиоэлектроники, 2016. - 338 с.- Режим доступа: http://www.iprbookshop.ru/72111.html

4. Горбенко А.О. Основы информационной безопасности (введение в профессию) [Электронный ресурс]: учебное пособие / А.О. Горбенко. - Электрон. текстовые данные. — СПб.: Интермедия, 2017. - 335 с. - Режим доступа: http://www.iprbookshop.ru/66797.html

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

6. Креопалов, В. В. Технические средства и методы защиты информации: учебное пособие / В. В. Креопалов. — М.: Евразийский открытый институт, 2011. — 278 с. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/10871.html (дата обращения: 01.11.2019). — Режим доступа: для авторизир. пользователей

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

8. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи: учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов: Ай Пи Эр Медиа, 2019. — 227 с. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/80290.html (дата обращения: 05.11.2019). — Режим доступа: для авторизир. пользователей

3.2.3. Дополнительные источники

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

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

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

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

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

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

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

8. 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».

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

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

11. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

12. 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.

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

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

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

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

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

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

19. Требования к системам обнаружения вторжений. Утверждены

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

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

21. 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.

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 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

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

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

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

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

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

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

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

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

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

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

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

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

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

38. 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.

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

40. 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.

41. 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.

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

43. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам.

Утвержден Гостехкомиссией России, 2002.

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

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

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

4.4. Кадровое обеспечение образовательного процесса

Практика осуществляется руководителем практики, который:
- согласовывает программу практики;
- контролирует процесс проведение практики;
- осуществляет планирование всех видов и этапов практики.

4.5. Требования к руководителям практики

Руководство учебной практикой осуществляют преподаватели колледжа, а также работники предприятий, закрепленные за обучающимися. Колледж выделяет в каждую фирму (организацию) преподавателя руководителя практики. В его обязанности входит периодическое посещение фирмы (отдела), контроль выполнения задания на практику, уточнение (корректировка) задания в зависимости от конкретных условий при обязательном согласовании этих вопросов с руководителем практики от предприятия. По результатам контроля преподаватель делает записи в журнале.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Формой отчетности обучающегося по учебной 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 рабочей программы; заполненный дневник и характеристика. По итогам работы в период практики студенту выдается характеристика, которая утверждается руководителем предприятия и скрепляется печатью предприятия. Обучающийся после прохождения практики защищает отчет по практике. Защита отчетов организуется в колледже. Студент докладывает результаты выполнения индивидуального задания, отвечает на вопросы руководителя практики от колледжа. По результатам защиты обучающимися отчетов выставляется дифференцированный зачет по практике.

На защиту представляется:

- отчет о практике;
- дневник учебной практики;
- утвержденный отзыв-характеристика о работе студента.

Письменный отчет о выполнении работ включает в себя следующие разделы:

- титульный лист;
- содержание;
- введение;
- основная часть (индивидуальное задание);
- характеристика места прохождения практики;
- правила охраны труда на рабочем месте;
- заключение.

Текст отчета должен быть подготовлен с использованием компьютера в Microsoft Word, распечатан на одной стороне белой бумаги формата А4 (210х297 мм). Цвет шрифта - черный, межстрочный интервал - полуторный, гарнитура - Times New Roman, размер шрифта - 14 кегль.

Работа над отчетом по практике должна позволить руководителю оценить уровень развития общих профессиональных компетенций студента.

При определении оценки учитывается:

- степень и качество отработки студентом программы практики и индивидуального задания;
- результаты исполнения служебных обязанностей;
- содержание и качество оформления отчетных документов.

Общая оценка студенту-практиканту определяется исходя из частных оценок:

- оценки, полученной на предприятии (в организации, фирме);
- оценки, полученной за ответы в ходе защиты.

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.	-установка, настройка, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей	Наблюдение и оценка при выполнении работ на учебной практике Защита отчетов по учебной практике
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.	- обеспечение бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях	
ПК 2.3. Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.	- защита информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.	

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

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки

ОК 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	Экспертное наблюдение за выполнением работ
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и 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.	- взаимодействовать с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	