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

РАБОЧАЯ ПРОГРАММА
ПП.02.01 ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

квалификация

техник по защите информации

Белгород 2020 г.

Рабочая программа производственной практики (по профилю специальности) разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности **10.02.04 Обеспечение информационной безопасности телекоммуникационных систем**, профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях» утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 03 ноября 2016 г. N 608н

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 ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Рабочая программа производственной 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 производственной 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 производственной практики – требования к результатам освоения производственной практики:

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения производственной 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;

уметь:

– выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;

– определять рациональные методы и средства защиты на объектах и оценивать их эффективность;

– производить установку и настройку типовых программно-аппаратных средств защиты информации;

– пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;

знать:

– типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;

– основные протоколы идентификации и аутентификации в телекоммуникационных системах;

– состав и возможности типовых конфигураций программно-аппаратных средств защиты информации;

– особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;

– основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;
основные понятия криптографии и типовые криптографические методы защиты информации.

1.3. Количество часов на освоение рабочей программы производственной практики:

на производственную практику отводится 216 часов (6 недель).

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Результатом освоения производственной 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 ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

3.1. Тематический план производственной практики (по профилю специальности))

Коды формируемых компетенций	**Наименование профессионального модуля**	**Объём времени, отведённый на производственную 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	216 часов, 6 недель

3.2. Содержание производственной практики (по профилю специальности)

Наименование тем производственной практики	Содержание производственной 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			**216**	
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			**132**	
Тема 1.1. Обеспечение безопасности операционных систем	**Содержание**		**18**	
	1	Инструктаж по технике безопасности. Определение целей и задач практики. Требования к оформлению отчетной документации	6	**2**
	2	Средства идентификации, аутентификации операционных систем	12	**3**
Тема 1.2. Технологии разграничения доступа	**Содержание**		**54**	
	1	Ознакомление с предприятием	6	**3**
	2	Изучение правил внутреннего распорядка предприятия	6	**3**
	3	Определение статуса, структуры и системы управления функциональных подразделений и служб предприятия. Изучение положения об их деятельности и правовом статусе	6	**3**
	4	Ознакомление с перечнем и конфигурацией средств вычислительной техники	6	**3**
	5	Ознакомление с перечнем и назначением программных средств, установленных на персональных компьютерах предприятия	6	**3**
	6	Изучение должностных инструкций инженерно-технических работников среднего звена в соответствии с подразделением предприятия	6	**3**
	7	Участие в организации работ по защите персональных компьютеров на предприятии	18	**3**
Тема 1.3. Обеспечение	**Содержание**		**36**	**3**

информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	**1**	Ознакомление с архитектурой сети	6	
	2	Анализ интересов клиента, выбор вариантов решений	6	**3**
	3	Участие в организации работ по защите локальных сетей на предприятии	24	**3**
Тема 1.4. Технологии обнаружения вторжений	**Содержание**		**18**	
	1	Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети	12	**3**
	2	Администрирование систем безопасности проводной защищенной локальной сети	6	**3**
Тема 1.5. Методы управления средствами защиты	**Содержание**		**6**	
	1	Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей.	6	**3**
МДК 02.02. Криптографическая защита информации			**84**	
Тема 2.1. Основы криптографических методов защиты информации	**Содержание**		**12**	
	1	Выбор программных средств шифрования в соответствии с решаемой задачей	12	**3**
Тема 2.2. Современные стандарты шифрования	**Содержание**		**30**	
	1	Подключение, установка драйверов, настройка программных средств абонентского шифрования	12	**3**
	2	Администрирование внедренных средств	18	**3**
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	**Содержание**		**42**	**3**
	1	Настройка средств электронной подписи	12	
	2	Администрирование средств электронной подписи	12	**3**
	3	Администрирование средств PKI	12	**3**
	4	Зачетное занятие	6	**3**
Всего:			**216**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

4.1. Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы производственной практики предполагает проведение производственной практики на предприятиях/организациях на основе прямых договоров, заключаемых между учебным заведением и предприятием/организацией, куда направляются обучающиеся.

Оборудование и технические средства на рабочем месте должны соответствовать содержанию деятельности и давать возможность обучающемуся овладеть профессиональными компетенциями по всем осваиваемым видам деятельности, предусмотренным программой с использованием современных технологий, материалов и оборудования.

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.

Базами практик должны быть предприятия\организации, оснащенные современным оборудованием, наличием квалифицированного персонала, близким, по возможности, территориальным расположением, отвечающих следующим требованиям:

– наличие сфер деятельности, предусмотренных программой производственной практики;

– обеспеченность квалифицированными кадрами для руководства производственной практикой.

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

Реализация образовательной программы обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового договора, в том числе из числа руководителей и работников организаций, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии и имеющих стаж работы в данной профессиональной области не менее 3 лет.

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 ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Формой отчетности обучающегося по производственной 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 производственная 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 MicrosoftWord, распечатан на одной стороне белой бумаги формата А4 (210х297 мм). Цвет шрифта - черный, межстрочный интервал - полуторный, гарнитура - TimesNewRoman, размер шрифта - 14 кегль.

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

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.	