МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»**
Северо-Кавказский филиал

СОГЛАСОВАНО

Генеральный директор ООО «Промышленные системы автоматического управления»

_____ В.Г. Потемкин

«__» _____ 2021 г.

УТВЕРЖДАЮ:
Директор СКФ БГТУ
им. В.Г. Шухова

_____ В.Л. Курбатов

«24» февраля 2021 г.

РАБОЧАЯ ПРОГРАММА
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
ПМ.03 Защита информации техническими средствами
ПМ.04 Выполнение работ по профессии «Оператор электронно-вычислительных и вычислительных машин»

основной профессиональной образовательной программы – программы подготовки специалистов среднего звена

Специальность
10.02.05 Обеспечение информационной безопасности автоматизированных систем
(базовой подготовки)
Квалификация выпускника
Техник по защите информации
Срок обучения
3 года 10 месяцев

Минеральные Воды, 2021 г.

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного Приказом Министерства образования и науки РФ № 1553 от 09.12.2016 г.,
- Плана учебного процесса БГТУ им. В.Г. Шухова по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного в 2021 г.

Организация разработчик: СКФ ФГБОУ ВО «БГТУ им. В.Г. Шухова», Северо-Кавказский филиал

Составитель: старший преподаватель  О.А. Митюгова

ученая степень и звание подпись инициалы, фамилия

Рабочая программа обсуждена и рекомендована на заседании кафедры Экономических и естественно-научных дисциплин

название кафедры

«_24_» _февраля_ 2021 г., протокол №_7__

Заведующий кафедрой: к.пед.н.  И.В. Черкасова

ученая степень и звание подпись инициалы, фамилия

Согласовано с работодателями:

ФИО	***Должность, место работы***
Потемкин Владимир Григорьевич	Директор ООО «Промышленные системы автоматического управления»

СОДЕРЖАНИЕ

1. ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
1.1Паспорт рабочей программы учебной практики 4
1.2Результаты освоения рабочей программы учебной практики 6
1.3Тематический план и содержание учебной практики 7
1.4Условия реализации рабочей программы учебной практики 10
1.5Контроль и оценка результатов освоения программы учебной практики 14
2. ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
2.1Паспорт рабочей программы учебной практики 17
2.2Результаты освоения рабочей программы учебной практики 18
2.3Тематический план и содержание учебной практики 22
2.4Условия реализации рабочей программы учебной практики 30
2.5Контроль и оценка результатов освоения программы учебной практики 34
3 ПМ.03 Защита информации техническими средствами
3.1Паспорт рабочей программы учебной практики 37
3.2Результаты освоения рабочей программы учебной практики 41
3.3Тематический план и содержание учебной практики 47
3.4Условия реализации рабочей программы учебной практики 50
3.5Контроль и оценка результатов освоения программы учебной практики 54
4 ПМ.04 Выполнение работ по профессии «Оператор электронно-вычислительных и вычислительных машин»
4.1Паспорт рабочей программы учебной практики 56
4.2Результаты освоения рабочей программы учебной практики 58
4.3Тематический план и содержание учебной практики 61
4.4Условия реализации рабочей программы учебной практики 64
4.5Контроль и оценка результатов освоения программы учебной практики 67

ПМ 01:ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

1.1, Область применения программы

Рабочая программа производственной практики (по профилю специальности) является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности10.02.05 «Обеспечение информационной безопасности автоматизированных систем»в части освоения квалификации «Техник по защите информации» и основного вида ПМ 01:Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

Рабочая программа производственной практики (по профилю специальности) может быть использована в дополнительном профессиональном образовании, повышении квалификации и переподготовки кадров по специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

1.2. Цели и задачи производственной практики (но профилю специальности):

формирование у обучающихся практических умений (приобретение практического опыта) в рамках освоения профессиональных модулей по основным видам деятельности.

1.3. Требования к результатам освоения производственной практики (по профилю специальности):

В результате прохождения производственной практики (по профилю специальности) но видам деятельности обучающийся должен:

Виды деятельности	Требования к умениям (практическому опыту)
1	2
01Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	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

1.4. Количество часов на освоение рабочей программы производственной практики (по профилю специальности):

Всего –144часов

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Результатом освоения рабочей программы производственной практики (по профилю специальности) является освоение обучающимися профессиональных и общих компетенций в рамках модуля по основным видам деятельности, сформированность у обучающихся практических профессиональных умений в рамках освоения профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении по специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по основным видам профессиональной деятельности:

01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении, необходимых для последующего освоения ими следующих профессиональных и общих компетенций:

Код компетенции	Наименование результата освоения практики
2	2
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
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. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРОГРАММЫПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

3.1. Тематический план производственной практики (по профилю специальности)

Виды работ	Наименование тем производственной практики	Коды осваиваемых компетенций	Количество часов по темам	Уровни освоения
1	2	3	4	5
Проведение инструктажа по технике безопасности.	Тема 1. Инструктаж по технике безопасности. Ознакомление с технической документацией	ОК 01-10 ПК 1.1-1.4	6	2
Ознакомление с планом проведения производственной практики.		ОК 01-10 ПК 1.1-1.4	6	2
Получение заданий.Оформление технической документации, правила оформления документов		ОК 01-10 ПК 1.1-1.4	6	2
Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации		ОК 01-10 ПК 1.1-1.4	6	2
Обслуживание средств защиты информации прикладного и системного программного обеспечения	Тема № 2. Обслуживание средств защиты информации прикладного и системного программного обеспечения	ОК 01-10 ПК 1.1-1.4	6	3
Настройка программного обеспечения с соблюдением требований по защите		ОК 01-10 ПК 1.1-1.4	6	3

информации				
Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам		ОК 01-10 ПК 1.1-1.4	6	3
Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением		ОК 01-10 ПК 1.1-1.4	6	3
Настройка встроенных средств защиты информации программного обеспечения		ОК 01-10 ПК 1.1-1.4	6	3
Проверка функционирования встроенных средств защиты информации программного обеспечения	Тема 3. Обслуживание средств защиты информации в компьютерных системах и сетях	ОК 01-10 ПК 1.1-1.4	6	3
Своевременное обнаружение признаков наличия вредоносного программного обеспечения		ОК 01-10 ПК 1.1-1.4	6	3
Обслуживание средств защиты информации в компьютерных системах и сетях		ОК 01-10 ПК 1.1-1.4	6	3
Обслуживание систем защиты информации в автоматизированных системах		ОК 01-10 ПК 1.1-1.4	6	3
Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем		ОК 01-10 ПК 1.1-1.4	6	3
Проверка работоспособности системы защиты информации автоматизированной системы	Тема 4. Проверка работоспособности системы защиты информации автоматизированной системы	ОК 01-10 ПК 1.1-1.4	6	3
Проверка		ОК 01-10	6	2

работоспособности системы защиты информации автоматизированной системы		ПК 1.1-1.4		
Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	Тема 5.Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	ОК 01-10 ПК 1.1-1.4	6	2
Контроль стабильности характеристик системы защиты информации автоматизированной системы		ОК 01-10 ПК 1.1-1.4	6	2
Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем		ОК 01-10 ПК 1.1-1.4	6	2
Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	Тема 6.Ведение технической документации и использование инструментальных средств для автоматизации оформления документации	ОК 01-10 ПК 1.1-1.4	6	2
Использовать инструментальные средства для автоматизации оформления документации		ОК 01-10 ПК 1.1-1.4	6	2
Оформление отчета по практике		ОК 01-10 ПК 1.1-1.4	6	2
Оформление отчета по практике			6	
Оформление отчета по практике			6	
	Промежуточная аттестация проводится в форме дифференцированного зачета			
Всего			144	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

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

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

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

4.1. Требований к минимальному материально-техническому обеспечению

Реализация рабочей программы производственной практики (по профилю специальности) предполагает наличие рабочих мест организациях на основе заключенных прямых договоров.

4.2. Оснащение

Реализация рабочей программы производственной практики предполагает наличие рабочих мест в организациях, направление деятельности которых соответствует профилю подготовки обучающихся где проводится производственная практика.

4.3. Общие требования к организации производственной практики (по профилю специальности)

Производственная практика (по профилю специальности) проводится руководителем практики от образовательного учреждения и руководителем практики от организации.

4.4. Кадровое обеспечение образовательного процесса

Требования к руководителям практики от структурного подразделения техникума - наличие высшего профессионального образования по специальности и трудового стажа по специальности не менее трех лет соответствующего профилю производственной практики.

Требования к руководителям практики от организации - наличие высшего профессионального образования, соответствующего профилю производственной практики.

4.5. Перечень учебных изданий, Интернет - ресурсов, дополнительной литературы

4.5.1. Обязательная литература

1. Гостев, И. М. Операционные системы : учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Профессиональное образование).
2. Журавлева, Т. Ю. Практикум по дисциплине «Операционные системы» : автоматизированный практикум / Т. Ю. Журавлева. — Саратов : Вузовское образование, 2014. — 40 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/20692.html (дата обращения: 12.02.2021). — Режим доступа: для авторизир. Пользователей
3. Мамойленко, С. Н. Операционные системы. Часть 1. Операционная система Linux : учебное пособие / С. Н. Мамойленко, О. В. Молдованова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2012. — 128 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/40540.html (дата обращения: 12.02.2021). — Режим доступа: для авторизир. Пользователей
4. Стружкин, Н. П. Базы данных: проектирование. Практикум : учебное пособие для среднего профессионального образования / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2020. — 291 с.
5. Берикашвили, В. Ш. Основы радиоэлектроники: системы передачи информации : учебное пособие для среднего профессионального образования / В. Ш.

Берикашвили. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 105 с.

6. Кравченко В.Б. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении : учеб. Пособие для студ. Учреждений сред. Проф. Образования / В.Б. Кравченко, П.В. Зиновьев, И.Н. Селютин. - Москва : "Академия", 2018. - 204 с.

4.5.2. Дополнительные источники:

1. Филиппов, М. В. Операционные системы : учебно-методическое пособие / М. В. Филиппов, Д. В. Завьялов. — Волгоград : Волгоградский институт бизнеса, 2014. — 163 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/56020.html (дата обращения: 12.02.2021). — Режим доступа: для авторизир. Пользователей
2. Куль, Т. П. Операционные системы : учебное пособие / Т. П. Куль. — Минск : Республиканский институт профессионального образования (РИПО), 2019. — 311 c. — ISBN 978-985-503-940-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/93431.html (дата обращения: 12.02.2021). — Режим доступа: для авторизир. пользователей

4.5.3. Периодические издания:

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

3.2.4. Электронные источники:

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

3.2.3. Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

2. Журналы Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

3.2.4. Электронные источники:

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

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

Контроль и оценка результатов освоения производственной практики (по профилю специальности) осуществляется руководителем практики в процессе проведения практики. В результате освоения производственной практики (по профилю специальности) обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты обучения (освоенные умения в рамках ВД)	Основные показатели оценки результатов	Формы и методы контроля и оценки результатов обучения
ПК 1.1.Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной	Производит установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Дифференцированный зачет в форме защиты отчета по производственной практики (по профилю специальности)

документации.		
ПК 1.2Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Администрирует 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.	Обеспечивает 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.	Осуществляет проверку технического состояния, техническое обслуживание и текущий ремонт, устраняет отказы и восстанавливает работоспособность автоматизированных (информационных) систем в защищенном исполнении.	

Студент должен подготовить всю необходимую отчетную документацию:

1. Отчет о проделанной работе по производственной практике(по профилю специальности), то есть письменное изложение всех произведенных работ и заполненных документов по каждой теме в отдельности, подтверждающих выполнения программы производственной практики.
2. Заполненный дневник производственной практике(по профилю специальности) с оценками руководителя практики от организации.
3. Отзыв-характеристика руководителя практики о студенте. Отзыв - характеристика подписывается руководителем практики и скрепляется печатью организации,
4. Аттестационный лист по производственной практике с указанием освоенных профессиональных компетенций, подписанный руководителем практики от организации.

ПМ.02. ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

1.1 Область применения программы

Рабочая программа производственной практики (по профилю специальности) является частью основной профессиональной образовательной программы в соответствиис ФГОС СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»в части освоения квалификации «Техник по защите информации» и основного вида ПМ.02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами**.** Рабочая программа производственной практики (по профилю специальности) может быть использована в дополнительном профессиональном образовании, повышении квалификации и переподготовки кадров по специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

1.3. Цели и задачи производственной практики (но профилю специальности):

формирование у обучающихся практических умений (приобретение практического опыта) в рамках освоения профессиональных модулей по основным видам деятельности.

1.3. Требования к результатам освоения производственной практики (по профилю специальности):

В результате прохождения производственной практики (по профилю специальности) но видам деятельности обучающийся должен:

Виды деятельности	Требования к умениям (практическому опыту)
1	2
02*Защита информации в автоматизированных системах программными и программно-аппаратными средствами*	*иметь практический опыт:* установки, настройки программных средств защиты информации в автоматизированной системе; обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе; *уметь:* устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

	устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; применять средства гарантированного уничтожения информации; 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

1.4. Количество часов на освоение рабочей программы производственной практики (по профилю специальности):
Всего –108часов

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Результатом освоения рабочей программы производственной практики (по профилю специальности) является освоение обучающимися профессиональных и общих компетенций в рамках модуля по основным видам деятельности, сформированность у обучающихся практических профессиональных умений в рамках освоения профессиональногомодуля ПМ.02. Защита информации в автоматизированных системах программными и программно-аппаратными средствамипо специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по основным видам профессиональной деятельности:
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами, необходимых для последующего освоения ими следующих профессиональных и общих компетенций:

Код компетенции	Наименование результата освоения практики
2	2
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации,

	необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
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.

3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

3.1. Тематический план производственной практики (по профилю специальности)

Виды работ	Наименование тем производственной практики	Коды осваиваемых компетенций	Количество часов по темам	Уровни освоения
1	2	3	4	5
Проведение инструктажа по технике безопасности. Ознакомление с планом проведения производственной практики.	Тема 1. Инструктаж по технике безопасности. Анализ принципов построения систем информационной защиты производственных подразделений	ОК 01-10 ПК 2.1-2.6	6	1-2
Разработка и анализ требований к системе защиты информации.		ОК 01-10 ПК 2.1-2.6	6	2

Анализ принципов построения систем информационной защиты производственных подразделений		ОК 01-10 ПК 2.1-2.6	6	2
Анализ принципов построения систем информационной защиты производственных подразделений		ОК 01-10 ПК 2.1-2.6	6	2
Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы	Тема 2.Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы	ОК 01-10 ПК 2.1-2.6	6	2
Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.		ОК 01-10 ПК 2.1-2.6	6	2-3
Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; – Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности		ОК 01-10 ПК 2.1-2.6	6	2-3
Участие в диагностировании,		ОК 01-10 ПК 2.1-2.6	6	2-3

устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности				
Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	Тема 3.Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	ОК 01-10 ПК 2.1-2.6	6	2-3
Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении		ОК 01-10 ПК 2.1-2.6	6	2-3
Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации		ОК 01-10 ПК 2.1-2.6	6	2-3
Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации		ОК 01-10 ПК 2.1-2.6	6	2-3
Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики	Тема 4.Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами	ОК 01-10 ПК 2.1-2.6	6	2-3
Применение нормативных правовых актов, нормативных		ОК 01-10 ПК 2.1-2.6	6	3

методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики				
Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики		ОК 01-10 ПК 2.1-2.6	6	2
Оформление отчета по практике		ОК 01-10 ПК 2.1-2.6	6	2-3
Оформление отчета по практике		ОК 01-10 ПК 2.1-2.6	6	2-3
Промежуточная аттестация проводится в форме дифференцированного зачета				
Всего			108	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3- продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

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

4.1. Требований к минимальному материально-техническому обеспечению

Реализация рабочей программы производственной практики (по профилю специальности) предполагает наличие рабочих мест организациях на основе заключенных прямых договоров.

4.2. Оснащение

Реализация рабочей программы производственной практики предполагает наличие рабочих мест в организациях, направление деятельности которых соответствует профилю подготовки обучающихся где проводится производственная практика.

4.3. Общие требования к организации производственной практики (по профилю специальности)

Производственная практика (по профилю специальности) проводится руководителем практики от образовательного учреждения и руководителем практики от организации.

4.4. Кадровое обеспечение образовательного процесса

Требования к руководителям практики от структурного подразделения техникума - наличие высшего профессионального образования по специальности и трудового стажа по специальности не менее трех лет соответствующего профилю производственной практики.

Требования к руководителям практики от организации - наличие высшего профессионального образования, соответствующего профилю производственной практики.

4.5. Перечень учебных изданий, Интернет - ресурсов, дополнительной литературы

4.2.1. Основная литература

1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548 (дата обращения: 16.02.2021).
2. Бутакова, Н. Г. Криптографические методы и средства защиты информации : учебное пособие / Н. Г. Бутакова, Н. В. Федоров. — Санкт-Петербург : Интермедия, 2020. — 380 с. — ISBN 978-5-4383-0210-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161347 (дата обращения: 16.02.2021). — Режим доступа: для авториз. пользователей.
3. *Внуков, А. А.* Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467356 (дата обращения: 16.02.2021).

4.2.2. Дополнительные источники:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451933 (дата обращения: 16.02.2021).

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

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

4. Федеральный закон от 27 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 ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

14. 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.

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 13335-3-2007 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 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

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

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

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

40. 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.

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

42. 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.

43. 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.

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

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

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

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

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

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

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

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

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

4.2.3. Периодические издания:

1. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
2. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.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 ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Контроль и оценка результатов освоения производственной практики (по профилю специальности) осуществляется руководителем практики в процессе проведения практики. В результате освоения производственной практики (по профилю специальности) обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты обучения (освоенные умения в рамках ВД)	Основные показатели оценки результатов	Формы и методы контроля и оценки результатов обучения
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрирует умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	Дифференцированный зачет в форме защиты отчета по производственной практики (по профилю специальности)
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрирует умениями практические навыки в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	
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	
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявляетпрактические навыки и умения в обработке, хранении и передаче информации ограниченного доступа	
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	
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных)	Проявляет умения и практические навыки в защите автоматизированных (информационных) систем с использованием программных и	

системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	

Студент должен подготовить всю необходимую отчетную документацию:

1. Отчет о проделанной работе по производственной практике(по профилю специальности), то есть письменное изложение всех произведенных работ и заполненных документов по каждой теме в отдельности, подтверждающих выполнения программы производственной практики.
2. Заполненный дневник производственной практике(по профилю специальности) с оценками руководителя практики от организации.
3. Отзыв-характеристика руководителя практики о студенте. Отзыв - характеристика подписывается руководителем практики и скрепляется печатью организации,
4. Аттестационный лист по производственной практике с указанием освоенных профессиональных компетенций, подписанный руководителем практики от организации.

ПМ.03: ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1Область применения программы

Рабочая программа производственной практики (по профилю специальности) ПП.03 является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» в части освоения квалификации «Техник по защите информации» и основного вида ПМ.03: Защита информации техническими средствами.

Рабочая программа производственной практики (по профилю специальности) может быть использована в дополнительном профессиональном образовании, повышении квалификации и переподготовки кадров по специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

1.2. Цели и задачи учебной практики:

формирование у обучающихся практических умений (приобретение практического опыта) в рамках освоения профессиональных модулей по основным видам деятельности.

1.3. Требования к результатам освоения учебной практики:

В результате прохождения производственной практики (по профилю специальности) по видам деятельности обучающийся должен:

Виды деятельности	Требования к умениям (практическому опыту)
1	2
03 Защита информации техническими средствами	иметь практический опытв: установке, монтажа и настройки технических средств защиты информации; техническом обслуживании технических средств защиты информации; применения основных типов технических средств защиты информации; 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

1.4. Количество часов на освоение рабочей программы производственной практики (по профилю специальности):
Всего –108часов

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения рабочей программы производственной практики (по профилю специальности) является освоение обучающимися профессиональных и общих компетенций в рамках модуля по основным видам деятельности, сформированность у обучающихся практических профессиональных умений в рамках освоения профессионального модуля ПМ.03 Защита информации техническими средствами по специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по основным видам профессиональной деятельности: *Защита информации техническими средствами*, необходимых для последующего освоения ими следующих профессиональных и общих компетенций:

Код компетенции	Наименование результата освоения практики
2	2
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и

	иностранном языках.
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. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРОГРАММЫПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

3.1. Тематический план производственной практики (по профилю специальности)

Виды работ	Наименование тем производственной практики	Коды осваиваемых компетенций	Количество часов по темам	Уровни освоения
1	2	3	4	5
Проведение инструктажа по технике безопасности. Ознакомление с планом проведения производственной практики.	Тема 1. Инструктаж по технике безопасности.	ОК 01-10 ПК 3.1-3.5	6	2
Анализ объектов информатизации предприятий, учреждении. организаций	Тема 2.Анализ объектов информатизации и обеспечения ресурсамиинженерно-технической защиты информации	ОК 01-10 ПК 3.1-3.5	6	2
Анализ ресурсов обеспечения инженерно-технической защиты информации		ОК 01-10 ПК 3.1-3.5	6	2
Изучение основных этапов про-ектирования системы защиты информации техническими средствами	Тема 3.Проектирование системы защиты информации техническими средствами	ОК 01-10 ПК 3.1-3.5	6	2
Оценка эффективности защиты информации		ОК 01-10 ПК 3.1-3.5	6	2
Планирование н		ОК 01-10	6	2-3

проектирование внутренних нормативных документов по введению средств защиты информации в эксплуатацию		ПК 3.1-3.5		
Планирование н проектирование внутренних нормативных документов по введению средств защиты информации в эксплуатацию		ОК 01-10 ПК 3.1-3.5	6	2-3
Оформление технической и технологической документации		ОК 01-10 ПК 3.1-3.5	6	2-3
Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации	Тема 4.Применение и эксплуатация технических средств защиты информации Тема 4.Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами	ОК 01-10 ПК 3.1-3.5	6	2-3
Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации		ОК 01-10 ПК 3.1-3.5	6	2-3
Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения		ОК 01-10 ПК 3.1-3.5	6	2-3
Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения		ОК 01-10 ПК 3.1-3.5	6	2-3
Участие в монтаже, обслуживании и эксплуатации средств защиты информации от		ОК 01-10 ПК 3.1-3.5	6	2-3

несанкционированного съёма и утечки по техническим каналам				
Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами		ОК 01-10 ПК 3.1-3.5	6	3
Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами		ОК 01-10 ПК 3.1-3.5	6	2
Оформление отчета по практике		ОК 01-10 ПК 3.1-3.5	6	2-3
Оформление отчета по практике		ОК 01-10 ПК 3.1-3.5	6	2-3
Промежуточная аттестация проводится в форме дифференцированного зачета				
Всего			108	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3- продуктивный (планированиеи самостоятельное выполнение деятельности, решение проблемных задач).

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

4.1. Требований к минимальному материально-техническому обеспечению

Реализация рабочей программы производственной практики (по профилю специальности) предполагает наличие рабочих мест организациях на основе заключенных прямых договоров.

4.2. Оснащение

Реализация рабочей программы производственной практики предполагает наличие рабочих мест в организациях, направление деятельности которых соответствует профилю подготовки обучающихся где проводится производственная практика.

4.3. Общие требования к организации производственной практики (по профилю специальности)

Производственная практика (по профилю специальности) проводится руководителем практики от образовательного учреждения и руководителем практики от организации.

4.4. Кадровое обеспечение образовательного процесса

Требования к руководителям практики от структурного подразделения техникума - наличие высшего профессионального образования по специальности и трудового стажа по специальности не менее трех лет соответствующего профилю производственной практики.

Требования к руководителям практики от организации - наличие высшего профессионального образования, соответствующего профилю производственной практики.

4.5. Перечень учебных изданий, Интернет - ресурсов, дополнительной литературы

4.5.1. Обязательная литература

1. Внуков А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование)
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru/bcode/456792 (дата обращения: 11.02.2021).
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548 (дата обращения: 16.02.2021).
4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451933 (дата обращения: 16.02.2021).

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

14. 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.

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

22. 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

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

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

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

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

27. 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

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

29. 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

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

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

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

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

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

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

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.

4.5.3 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. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru

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

Контроль и оценка результатов освоения производственнойпрактики осуществляется руководителем практики в процессе проведения практики. В результате освоения учебной практики обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты обучения (освоенные умения в рамках ВД)	Основные показатели оценки результатов	Формы и методы контроля и оценки результатов обучения
ПК 3.1.Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Демонстрирует умения и практические навыки в установке, монтаже, настройке и техническомобслуживании технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Дифференцированный зачет
ПК 3.2.Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями	Демонстрирует умениями практические навыки в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	

эксплуатационной документации.		
ПК 3.3.Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	Выполнение перечня работ по измерению 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.	Проявляетпрактические навыки и умения в измерении параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	
ПК 3.5.Организовывать отдельные работы по физической защите объектов информатизации.	Демонстрирует умениями практические навыки в организации отдельных работ по физической защите объектов информатизации	

ПМ.04: ВЫПОЛНЕНИЕ РАБОТ ПО ПРОФЕССИИ «ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН»

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

1.1Область применения программы

Рабочая программа производственной практики (по профилю специальности) ПП.04является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»в части освоения квалификации «Техник по защите информации» и основного вида ПМ.04: Выполнение работ по профессии «Оператор электронно-вычислительных и вычислительных машин».

Рабочая программа производственной практики (по профилю специальности)может быть использована в дополнительном профессиональном образовании, повышении квалификации и переподготовки кадров по специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

1.2. Цели и задачи производственной практики:

формирование у обучающихся практических умений (приобретение практического опыта) в рамках освоения профессиональных модулей по основным видам деятельности.

1.3. Требования к результатам освоения производственной практики(по профилю специальности):

В результате прохождения производственной практики(по профилю специальности)по видам деятельности обучающийся должен:

Виды деятельности	Требования к умениям (практическому опыту)
1	2
04Выполнение работ по профессии «Оператор электронно-вычислительных и вычислительных машин»	иметь практический опыт в: − выполнения требований техники безопасности при работе с вычислительной техникой; − организации рабочего места оператора электронно-вычислительных и вычислительных машин; − подготовки оборудования компьютерной системы к работе; − инсталяции, настройки и обслуживания программного обеспечения компьютерной системы; − управления файлами; − применения офисного программного обеспечения в соответствии с прикладной задачей; − использования ресурсов локальной вычислительной сети; − использования ресурсов, технологий и сервисов Интернет; применения средств защиты информации в компьютерной системе уметь: − выполнять требования техники безопасности при работе с вычислительной техникой; − производить подключение блоков персонального компьютера и периферийных

	устройств; – производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; – диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; – выполнять инсталляцию системного и прикладного программного обеспечения; – создавать и управлять содержимым документов с помощью текстовых процессоров; – создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; – создавать и управлять содержимым презентаций с помощью редакторов презентаций; – использовать мультимедиа проектор для демонстрации презентаций; – вводить, редактировать и удалять записи в базе данных; – эффективно пользоваться запросами базы данных; – создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; – производить сканирование документов и их распознавание; – производить распечатку, копирование и тиражирование документов на принтере и других устройствах; – управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; – осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; – осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; – осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ; осуществлять резервное копирование и восстановление данных

1.4. Количество часов на освоение рабочей программыпроизводственной практики:
Всего –108часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Результатом освоения рабочей программы производственной практики(по профилю специальности)является освоение обучающимися профессиональных и общих компетенций в рамках модуля по основным видам деятельности,сформированность у обучающихся практических профессиональных умений в рамках освоения профессиональногомодуля ПМ.04 Выполнение работ по профессии " Оператор электронно-вычислительных и вычислительных машин"по специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по основным видам профессиональной деятельности: ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих, необходимых для последующего освоения ими следующих профессиональных и общих компетенций:

Код компетенции	Наименование результата освоения практики
2	2
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ПК 4.1.	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК 4.4.	Обеспечивать применение средств защиты информации в компьютерной системе

3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРОГРАММЫПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

3.1. Тематический план производственной практики (по профилю специальности)

Виды работ	Наименование тем производственной практики	Коды осваиваемых компетенций	Количество часов по темам	Уровни освоения
1	2	3	4	5
Проведение инструктажа по технике безопасности. Ознакомление с планом проведения производственной практики.	Тема 1. Инструктаж по технике безопасности.	ОК 01-10 ПК 4.1-4.4	6	2
Сборка системного блока ПК	Тема 2.Архитектура ВС. Операционные системы	ОК 01-10 ПК 4.1-4.4	6	2
Установка операционной системы. Настройка интерфейса		ОК 01-10 ПК 4.1-4.4	6	2
Подключение периферийного оборудования. Установка драйверов	Тема 3.Подключение периферийного оборудования	ОК 01-10 ПК 4.1-4.4	6	2
Тестирование аппаратных средств с помощью диагностических программ		ОК 01-10 ПК 4.1-4.4	6	2
Установка и настройка прикладного программного обеспечения. Работа с антивирусными программами и утилитами		ОК 01-10 ПК 4.1-4.4	6	2-3
Установка и настройка прикладного программного обеспечения. Работа с антивирусными программами и		ОК 01-10 ПК 4.1-4.4	6	2-3

утилитами				
Создание виртуальной машины с операционной системой Windows, Windows 7, Linux		ОК 01-10 ПК 4.1-4.4	6	2-3
Создание ЛВС	Тема 4.Администрирование и настройка локальной вычислительной сети	ОК 01-10 ПК 4.1-4.4	6	2-3
Обжим кабеля витая пара и розеток. Проверка обжатого кабеля и розетки с помощью тестера		ОК 01-10 ПК 4.1-4.4	6	2-3
Подключение к локальной вычислительной сети. Настройка локальной вычислительной сети и подключение к сети Интернет		ОК 01-10 ПК 4.1-4.4	6	2-3
Общий доступ к ресурсам сети. Обеспечение безопасности локальной сети		ОК 01-10 ПК 3.1-3.5	6	2-3
Настройка беспроводной сети		ОК 01-10 ПК 4.1-4.4	6	2-3
Администрирование сети		ОК 01-10 ПК 4.1-4.4	6	3
Администрирование сети		ОК 01-10 ПК 4.1-4.4	6	2
Оформление отчета по практике		ОК 01-10 ПК 4.1-4.4	6	2-3
Оформление отчета по практике		ОК 01-10 ПК 4.1-4.4	6	2-3
Промежуточная аттестация проводится в форме дифференцированного зачета				
Всего			108	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

4.1. Требований к минимальному материально-техническому обеспечению

Реализация рабочей программы производственной практики (по профилю специальности) предполагает наличие рабочих мест организациях на основе заключенных прямых договоров.

4.2. Оснащение

Реализация рабочей программы производственной практики предполагает наличие рабочих мест в организациях, направление деятельности которых соответствует профилю подготовки обучающихся где проводится производственная практика.

4.3. Общие требования к организации производственной практики (по профилю специальности)

Производственная практика (по профилю специальности) проводится руководителем практики от образовательного учреждения и руководителем практики от организации.

4.4. Кадровое обеспечение образовательного процесса

Требования к руководителям практики от структурного подразделения техникума - наличие высшего профессионального образования по специальности и трудового стажа по специальности не менее трех лет соответствующего профилю производственной практики.

Требования к руководителям практики от организации - наличие высшего профессионального образования, соответствующего профилю производственной практики.

4.5. Перечень учебных изданий, Интернет - ресурсов, дополнительной литературы

4.5.1. Обязательная литература

1. Мамонова, Т. Е. Информационные технологии. Лабораторный практикум : учебное пособие для среднего профессионального образования / Т. Е. Мамонова. — Москва : Издательство Юрайт, 2020. — 178 с. — (Профессиональное образование). — ISBN 978-5-534-07791-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/455793 (дата обращения: 17.02.2021)..

2. Журавлева, Т. Ю. Практикум по дисциплине «Операционные системы» : автоматизированный практикум / Т. Ю. Журавлева. — Саратов : Вузовское образование, 2014. — 40 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/20692.html (дата обращения: 12.02.2021). — Режим доступа: для авторизир. Пользователей

3. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебное пособие для среднего профессионального образования / О. М. Замятина. — Москва : Издательство Юрайт, 2020. — 159 с. — (Профессиональное образование). — ISBN 978-5-534-10682-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456799 (дата обращения: 17.02.2021).

4. Толстобров, А. П. Архитектура ЭВМ : учебное пособие для среднего профессионального образования / А. П. Толстобров. — 2-е изд., испр. и доп. — Москва :

Издательство Юрайт, 2020. — 154 с. — (Профессиональное образование). — ISBN 978-5-534-13398-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/459009 (дата обращения: 17.02.2021)..

4.5.2. Дополнительные печатные источники:

1. Филиппов, М. В. Операционные системы : учебно-методическое пособие / М. В. Филиппов, Д. В. Завьялов. — Волгоград : Волгоградский институт бизнеса, 2014. — 163 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/56020.html (дата обращения: 12.02.2021). — Режим доступа: для авторизир. Пользователей
2. *Новожилов, О. П.* Архитектура компьютерных систем в 2 ч. Часть 2 : учебное пособие для среднего профессионального образования / О. П. Новожилов. — Москва : Издательство Юрайт, 2020. — 246 с. — (Профессиональное образование). — ISBN 978-5-534-10301-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456522 (дата обращения: 17.02.2021).

.

4.5.3 Электронные источники:

1. Информационный портал по безопасности www.SecurityLab.ru.
2. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
3. Сайт Научной электронной библиотеки www.elibrary.ru
4. Справочно-правовая система «Гарант» » www.garant.ru
5. Справочно-правовая система «Консультант Плюс» www.consultant.ru
6. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
7. Федеральный портал «Российское образование www.edu.ru

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Контроль и оценка результатов освоения производственнойпрактики осуществляется руководителем практики в процессе проведения практики. В результате освоения производственной практики обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты обучения (освоенные умения в рамках ВД)	Основные показатели оценки результатов	Формы и методы контроля и оценки результатов обучения
ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	Демонстрировать умениями практические навыки в подготовке оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	Дифференцированный зачет
ПК 4.2 Создавать и	Проявление умения и практического	Дифференцированный

управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах	опыта в работе с текстовыми документами, таблицами и презентациями ,а также базами данных	зачет
ПК 4.3 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	Умение пользоваться ресурсами локальных вычислительных сетей, осуществлять поиск, анализ и интерпретацию информации	Дифференцированный зачет
ПК 4.4 Обеспечивать применение средств защиты информации в компьютерной системе	Применение средств защиты информации в компьютерной системе	Дифференцированный зачет