**МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ**
**ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**
**«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»»**

## Рабочая программа практики

# УП.02 Учебная практика

**для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем**

г. Алексеевка
**2024**

Рабочая программа учебной практики разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 года № 1553, с учетом профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 536н, и с учетом профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 533н, и с учетом профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 525н.

Разработчик:
Ковалев Н.А., преподаватель ОГАПОУ «Алексеевский колледж»

**СОДЕРЖАНИЕ:**

# 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

## 1.1. Область применения рабочей программы

Рабочая программа учебной практики является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем СПО в части освоения основного вида деятельности: Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующих профессиональных компетенций (ПК):

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

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

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

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

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

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

**1.2. Место практики в структуре образовательной программы:** Профессиональный цикл. Учебная практика проводятся образовательным учреждением при освоении студентами профессиональных компетенций в рамках профессионального модуля ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

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

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

С целью овладения видом деятельности Защита информации в

автоматизированных системах программными и программно-аппаратными средствами и соответствующими профессиональными компетенциями обучающийся в ходе освоения программы учебной практики должен

**иметь практический опыт:**

– установка, настройка программных средств защиты информации в автоматизированной системе;

– обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами;

– использование программных и программно-аппаратных средств для защиты информации в сети;

– тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации ;

– решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

– применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных;

– учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности;

– работа с подсистемами регистрации событий;

– выявление событий и инцидентов безопасности в автоматизированной системе.

**уметь:**

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

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

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

– применять программные и программно-аппаратные средства для защиты информации в базах данных;

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

– применять математический аппарат для выполнения криптографических преобразований;

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

– применять средства гарантированного уничтожения информации;

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

– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

**знать:**

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

– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

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

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

– особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

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

**Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции чемпионатного движения по профессиональному мастерству «Профессионалы» и Чемпионата высоких технологий Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении практики:**

1) знать и понимать: типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;

2) знать и понимать: каналы передачи данных: определение и виды;

3) знать и понимать: технологии работы с политиками информационной безопасности;

4) уметь: создать объекты защиты и политику ИБ, используя технологии анализа в системе корпоративной защиты;

5) уметь: администрирование автоматизированных технические средства управления и контроля информации и информационных потоков;

6) уметь: создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты.

**Планируемые личностные результаты освоения рабочей программы**

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в

сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

**1.4. Количество часов на освоение рабочей программы учебной практики:** всего - 108 часов.

## 2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

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

| Код | Наименование компетенции |
|---|---|
| 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. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

| Наименование разделов и тем / виды работ | Содержание учебного материала / содержание работ | Объем часов, в том числе в форме практической подготовки | Коды компетенций (ОК, ПК), личностных результатов (ЛР), формированию которых способствует элемент программы |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Тема 1. Защита информации в автоматизированных системах программными и программно-аппаратными средствами | Содержание учебного материала | **106/106** | ОК 1-11<br>ПК 2.1-2.6<br>ЛР 4,7,9,10,11 |
| | | | |
| | Практические занятия<br>Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.<br>Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности.<br>Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности.<br>Составление документации по учету, обработке, хранению и передаче конфиденциальной информации.<br>Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации<br>Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.<br>Устранение замечаний по результатам проверки.<br>Анализ и составление нормативных методических документов по обеспечению | | |

| | | | |
|---|---|---|---|
| | информационной безопасности программно-аппаратными средствами, с учетом нормативно правовых актов.<br>Применение математических методов для оценки качества и выбора наилучшего программного средства<br>Использование типовых криптографических средств в и методов защиты информации.<br>Использование электронной подписи | | |
| | Контрольные работы | * | |
| | **Дифференцированный зачет** | **2/2** | |
| | **Всего:** | **108** | |

# 4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

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

Практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся на основе договоров, заключаемых между ОГАПОУ «Алексеевский колледж» и организациями.

Материально-техническая база должна соответствовать действующим санитарным и противопожарным нормам.

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

**4.2. Информационное обеспечение реализации рабочей программы учебной практики**:

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

**Основные источники:**


1. 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
2. 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.


**Дополнительные источники:**


1. Белов В.В. Проектирование информационных систем: учебник для студ. учреждений высш. проф. образования / В. В. Белов, В. И. Чистякова; под ред. В. В. Белова – М.: Издательский центр «Академия», 2013.
2. Гвоздева В.А., Лаврентьева И.Ю., Основы построения автоматизированных информационных систем, Москва, ИД Форум – ИНФРА-М, 2009.
3. Гвоздева Т.В., Баллод Б.А., Проектирование информационных систем: учеб.пособие / Т.В. Гвоздева, Б.А. Баллод. – Ростов н/Д: Феникс, 2009. – 508 с.

4. Емельянова Н.З., Устройство и функционирование информационных систем: учеб.пособие для СПО / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – 2-е изд., перераб. и доп. – М.: Форум, 2015. – 448 с.
5. Избачков Ю.С., Информационные системы: учебник для вузов [Гриф УМО МО РФ]. 3-е изд. / Избачков Ю.С., Петров В.Н [и др.]. – СПб.: Питер, 2011. – 544 с.

**Электронные издания (электронные ресурсы):**

1. Адаменко, М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 https://e.lanbook.com/book/82817
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. https://urait.ru/bcode/449548
3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. https://urait.ru/bcode/456793
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. https://urait.ru/bcode/451933

**Цифровая образовательная среда СПО PROFобразование:**

- Абрамов, Г. В. Проектирование и разработка информационных систем : учебное пособие для СПО / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. — Саратов : Профобразование, 2020. — 169 с. — ISBN 978-5-4488-0730-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/88888 (дата обращения: 07.09.2020). — Режим доступа: для авторизир. пользователей.

**Электронно-библиотечная система:**

IPR BOOKS - http://www.iprbookshop.ru/78574.html

**Веб-система для организации дистанционного обучения и управления им:**

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/

# 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

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

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

| **Результаты (освоенные профессиональные компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. | Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации | Защита отчетов по практическим и лабораторным работам<br>Экспертное наблюдение за выполнением различных видов работ<br>Дифференцированный зачет |
| ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. | Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами | Защита отчетов по практическим и лабораторным работам<br>Экспертное наблюдение за выполнением различных видов работ<br>Дифференцированный зачет |
| 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 | Защита отчетов по практическим и лабораторным работам<br>Экспертное наблюдение за выполнением различных видов работ<br>Дифференцированн |

| | | |
|---|---|---|
| | | ый зачет |
| ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. | Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа | Защита отчетов по практическим и лабораторным работам<br>Экспертное наблюдение за выполнением различных видов работ<br>Дифференцированный зачет |
| 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 | Защита отчетов по практическим и лабораторным работам<br>Экспертное наблюдение за выполнением различных видов работ<br>Дифференцированный зачет |
| ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. | Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак | Защита отчетов по практическим и лабораторным работам<br>Экспертное наблюдение за выполнением различных видов работ<br>Дифференцированный зачет |