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

## Рабочая программа учебной дисциплины

# ОП 01. Основы информационной безопасности

**для специальности**

10.02.05 Обеспечение информационной безопасности автоматизированных систем

г. Алексеевка
2024

Рабочая программа 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 УЧЕБНОЙ ДИСЦИПЛИНЫ
## Основы информационной безопасности

### 1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы среднего профессионального образования - программы подготовки специалистов среднего звена в соответствии с ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

### 1.2. Место учебной дисциплины в структуре ППССЗ:

Дисциплина является общепрофессиональной и входит в общепрофессиональный цикл.

### 1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины:

В результате освоения учебной дисциплины обучающийся должен **уметь**:

У1 классифицировать защищаемую информацию по видам тайны и степеням секретности;

У2 классифицировать основные угрозы безопасности информации.

В результате освоения учебной дисциплины обучающийся должен **знать**:

З1 сущность и понятие информационной безопасности, характеристику ее составляющих;

З2 место информационной безопасности в системе национальной безопасности страны;

З3 виды, источники и носители защищаемой информации;

З4 источники угроз безопасности информации и меры по их предотвращению;

З5 факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;

З6 жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;

З7 современные средства и способы обеспечения информационной безопасности;

З8 основные методики анализа угроз и рисков информационной безопасности.

Профессиональные (ПК) и общие (ОК) **компетенции**, которые актуализируются при изучении учебной дисциплины:

ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие

ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей

ОК 09 Использовать информационные технологии в профессиональной

деятельности
ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

**Перечень знаний и умений в соответствии с профессиональными стандартами «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н, «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н., «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н., «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н., которые актуализируются при изучении междисциплинарного курса:**

1) способы защиты информации от утечки по техническим каналам;
2) основные методы управления защитой информации;
3) применять антивирусные средства защиты информации в операционных системах;
4) организационные меры по защите информации.

**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 профессионального модуля:**

1) знать и понимать: скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню;
2) знать и понимать: подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;
3) знать и понимать: особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, MWare Workstation;
4) знать и понимать: типы угроз информационной безопасности, типы инцидентов;
5) знать и понимать: Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;

6) знать и понимать: структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей;

7) знать и понимать: подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз

**1.4. 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 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.

**1.5. Количество часов на освоение рабочей программы учебной дисциплины:**

максимальной учебной нагрузки обучающегося - 48 часов, в том числе: аудиторной учебной работы обучающегося - 48 часа, из них в форме практической подготовки – 38 часов; в том числе практических занятий - 18 часов; самостоятельной учебной работы обучающегося - 0 часов; консультаций - 0 часов.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 2.1. Объем учебной дисциплины и виды учебной работы

| Вид учебной работы | Объем часов |
|---|---|
| **Максимальная учебная нагрузка (всего)** | **48** |
| **Аудиторная учебная работа (обязательные учебные занятия) (всего)** | **48** |
| **из них в форме практической подготовки** | **38** |
| в том числе: | * |
| лекционные занятия | **30** |
| лабораторные работы | * |
| практические занятия | **18** |
| контрольные работы | |
| **Самостоятельная работа обучающегося (всего)** | * |
| **Консультации** | * |
| **Промежуточная аттестация:** *дифференцированный зачет* | **2** |

## 2.2. Тематический план и содержание учебной дисциплины Основы информационной безопасности

| Наименование разделов и тем | Содержание учебного материала, лабораторные работы и практические занятия, в том числе в форме практической подготовки, самостоятельная работа обучающихся | Объем часов | Коды личностных результатов (ЛР), формированию которых способствует элемент программы |
|---|---|---|---|
| **1** | **2** | **3** | |
| **Раздел 1. Теоретические основы информационной безопасности** | | | |
| Тема 1.1. Основные понятия и задачи информационной безопасности | Содержание учебного материала, в том числе в форме практической подготовки | **4/0/4** | ЛР 4<br>ЛР 7 |
| | 1 Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. | | |
| | 2 Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности | | |
| | Лабораторные занятия | * | |
| | Практические занятия, в том числе в форме практической подготовки | */* | |
| | Контрольные работы | * | |
| Тема 1.2. Основы защиты информации | Содержание учебного материала | **6/0/6** | ЛР 4<br>ЛР 7<br>ЛР 10<br>ЛР 11 |
| | 1. Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. | | |
| | 2. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации. | | |
| | 3. Элементы процесса менеджмента ИБ. Модель интеграции информационной | | |

| | | | | |
|---|---|---|---|---|
| | | безопасности в основную деятельность организации. Понятие Политики безопасности | | |
| | Лабораторные занятия | | * | |
| | Практические занятия, в том числе в форме практической подготовки<br>Определение объектов защиты на типовом объекте информатизации.<br>Классификация защищаемой информации по видам тайны и степеням конфиденциальности | | **0/4/4** | |
| | Контрольные работы | | * | |
| Тема 1.3. Угрозы безопасности защищаемой информации. | Содержание учебного материала, в том числе в форме практической подготовки | | **6/0/0** | ЛР 4 |
| | 1 | Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. | | |
| | 2 | Каналы и методы несанкционированного доступа к информации | | |
| | 3 | Применение потоков. Классификация потоков. Реализация потоков. Уязвимости. Методы оценки уязвимости информации | | |
| | Лабораторные занятия | | * | |
| | Практические занятия, в том числе в форме практической подготовки<br>Определение угроз объекта информатизации и их классификация | | **0/4/4** | |
| **Раздел 2. Методология защиты информации** | | | | |
| Тема 2.1. Методологические подходы к защите информации | Содержание учебного материала, в том числе в форме практической подготовки | | **4/0/4** | ЛР 4<br>ЛР 7<br>ЛР 10<br>ЛР 11 |
| | 1 | Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. | | |
| | 2 | Виды мер и основные принципы защиты информации. | | |
| | Лабораторные занятия | | * | |
| | Практические занятия, в том числе в форме практической подготовки<br>Диагностика и коррекция ошибок операционной системы, контроль доступа к операционной системе. | | **0/2/2** | |
| Тема 2.2. Нормативно правовое регулирование защиты информации | Содержание учебного материала, в том числе в форме практической подготовки | | **4/0/4** | ЛР 4<br>ЛР 7<br>ЛР 10<br>ЛР 11 |
| | 1 | Организационная структура системы защиты информации. Законодательные акты в области защиты информации. | | |
| | 2 | Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты ин-формации. Основные правила и документы системы сертификации РФ в области защиты информации | | |

| | | | | |
|---|---|---|---|---|
| | Лабораторные занятия | | * | |
| | Практические занятия, в том числе в форме практической подготовки<br>Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности | | **0/4/4** | |
| Тема 2.3. Защита информации в автоматизированных (информационных) системах | Содержание учебного материала, в том числе в форме практической подготовки | | **4/0/0** | ЛР 4<br>ЛР 7<br>ЛР 10<br>ЛР 11 |
| | 1 | Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации. | 2 | |
| | 2 | Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы. | 2 | |
| | Лабораторные занятия | | * | |
| | Практические занятия, в том числе в форме практической подготовки<br>Выбор мер защиты информации для автоматизированного рабочего места | | **0/4/4** | |
| | Дифференцированный зачет | | **2/2** | |
| | **Всего:** | | **48** | |

# 3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

## 3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия учебного кабинета лаборатории программных и программно-аппаратных средств защиты информации.

**Оборудование учебного кабинета:**

Комплект учебно-методической документации. Специализированная учебная мебель: стол преподавателя, стул преподавателя, столы для студентов, стулья для студентов, классная доска. Автоматизированные рабочие места на 15 обучающихся с наличием локальной и глобальной компьютерной сети: 15 столов, 15 стульев; автоматизированное рабочее место преподавателя (ПК, принтер, сканер); мультимедийный проектор; экран; программное обеспечение общего и профессионального назначения; программное обеспечение сетевого оборудования (операционные системы, пакет прикладных программ, графические редакторы, справочная правовая система, браузер, антивирусная программа.

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

## 3.2. Информационное обеспечение обучения:

**Основные источники:**

1. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с.
2. 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
3. Основы информационной безопасности. Учебник/ Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. – М.: Академия. 2019-256 с.
4. 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.

**Дополнительные источники:**

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ.

2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2016.
3. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М. : КНОРУС, 2016.
4. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2016.
5. Нестеров С.А. Основы информационной безопасности. Учебное пособие. – С-Пб.: Лань. 2016.
6. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности. –М.: Академия. 2015.
7. Проскурин В.Г. Защита программ и данных: Учебное пособие для ВУЗов. - –М.: Академия. 2012.
8. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2017.
9. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. ДМК Пресс, 2012.

**Электронные издания (электронные ресурсы)**

10. 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
11. 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. —https://urait.ru/bcode/456792
12. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

**Цифровая образовательная среда СПО PROFобразование:**

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/97562 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. пользователей
2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/91640 (дата

обращения: 18.11.2020). — Режим доступа: для авторизир. пользователей
3. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 c. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/89453 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. пользователей

**Электронно-библиотечная система:**
IPR BOOKS
https://www.iprbookshop.ru/10746.html
https://www.iprbookshop.ru/43960.html

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

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

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

**Контроль и оценка** результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения теоретических и практических занятий, дифференцированного зачета.

| **Результаты обучения (освоенные умения, усвоенные знания), с учетом личностных результатов, профессионального стандарта** | **Формы и методы контроля и оценки результатов обучения** |
|---|---|
| **умения:**<br>классифицировать защищаемую информацию по видам тайны и степеням секретности;<br>классифицировать основные угрозы безопасности информации;<br>**знания**:<br>сущность и понятие информационной безопасности, характеристику ее составляющих;<br>место информационной безопасности в системе национальной безопасности страны;<br>виды, источники и носители защищаемой информации;<br>источники угроз безопасности информации и меры по их предотвращению;<br>факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;<br>жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;<br>современные средства и способы обеспечения информационной безопасности;<br>основные методики анализа угроз и рисков информационной безопасности. | Дифференцированный зачет<br>Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.<br>Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий.<br>Тестирование<br>Умения проводить классификацию информации по видам тайны и степе-ни секретности, основных угроз информации в профессиональной деятельности<br>Экспертное наблюдение в процессе практических занятий |