

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное автономное образовательное учреждение высшего образования  
**«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**  
(национальный исследовательский университет)»  
**ИНСТИТУТ СПОРТА, ТУРИЗМА И СЕРВИСА**  
**МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ**



УТВЕРЖДАЮ:  
директор  
Многопрофильного колледжа

О.Б. Прохорова

31 марта 2023 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**  
**ОП.ДВ.13 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**


основной профессиональной образовательной программы  
**09.02.07 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ПРОГРАММИРОВАНИЕ**

Челябинск 2023


Рабочая программа учебной дисциплины ОП.ДВ.13 Основы информационной безопасности основной профессиональной образовательной программы специальности среднего профессионального образования (далее – СПО) 09.02.07 Информационные системы и программирование рассмотрена и одобрена на заседании Педагогического совета №5, протокол №5 от «30» марта 2023 г.

СОГЛАСОВАНО:

Зам. директора по НМР

  
И.Н. Романенко  
«30» марта 2023 г.

Специалист по УМР

  
О.А. Швецова  
«30» марта 2023 г.

Разработчик: А.В. Смолин – преподаватель Многопрофильного колледжа

Рабочая программа учебной дисциплины общепрофессионального цикла ОП.ДВ.13 Основы информационной безопасности разработана в соответствии с требованиями Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 09.02.07 Информационные системы и программирование (утв. Приказом № 1547 Минобрнауки РФ 09.12.2016 г.).

# 1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

## 1.1 Область применения рабочей программы

Рабочая программа учебной дисциплины ОП.ДВ.13 Основы информационной безопасности является частью основной профессиональной образовательной программы среднего профессионального образования по программе подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.07 Информационные системы и программирование.

## 1.2 Место учебной дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина ОП.ДВ.13 Основы информационной безопасности относится к общепрофессиональному циклу.

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

В результате освоения учебной дисциплины обучающийся должен освоить умения и знания, необходимые для формирования общих компетенций (таблица 1) и профессиональных компетенций (таблица 2).

Таблица 1 – Общие компетенции

| Код и наименование общей компетенции   | Знания, умения   |
|--|--|
| ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам | <b>Умения:</b> распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) |
|  | <b>Знания:</b> актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности  |

|  |  |
|--|--|
| ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности | <b>Умения:</b> определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение                                    |
|  | <b>Знания:</b> номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности  |
| ОК 04. Эффективно взаимодействовать и работать в коллективе и команде  | <b>Умения:</b> организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности   |
|  | <b>Знания:</b> психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности   |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста       | <b>Умения:</b> грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе  |
|  | <b>Знания:</b> особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.   |
| ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках   | <b>Умения:</b> понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы |
|  | <b>Знания:</b> правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности.   |

Таблица 2 – Профессиональные компетенции

| <b>Код и наименование профессиональной компетенции</b>                                | <b>Показатели освоения профессиональной компетенции</b>  |
|---|--|
| ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными | <b>Умения:</b> применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности; выявлять основные угрозы информационной безопасности; производить установку и настройку типовых программных средств |

|  |  |
|--|--|
| <p>средствами.</p>   | <p>защиты информации;<br/> обеспечивать антивирусную защиту;<br/> фильтровать сетевые пакеты межсетевым экраном;<br/> использовать типовые криптографические средства и методы защиты информации, в том числе электронную цифровую подпись;<br/> выполнять операции резервного копирования и восстановления данных.</p>  |
|  | <p><b>Знания:</b><br/> сущность и понятие информационной безопасности, характеристику её составляющих;<br/> место информационной безопасности в системе национальной безопасности страны;<br/> виды угроз информационной безопасности;<br/> основные положения комплексного подхода к защите информации;<br/> основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ и ФСТЭК РФ в данной области;<br/> принципы архитектурной безопасности;<br/> современные программно-технические средства обеспечения информационной безопасности;<br/> виды систем идентификации и аутентификации;<br/>  типовые модели управления доступом;<br/>  типовые средства и методы ведения аудита;<br/> основные понятия криптографии;<br/>  типовые криптографические алгоритмы, применяемые для защиты информации;</p> |
| <p>ПК 11.6. Защищать информацию в базе данных с использованием технологии защиты информации.</p> | <p><b>Умения:</b><br/> применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности;<br/> выявлять основные угрозы информационной безопасности;<br/> использовать типовые криптографические средства и методы защиты информации, в том числе электронную цифровую подпись;<br/> выполнять операции резервного копирования и восстановления данных.</p>   |
|  | <p><b>Знания:</b><br/> сущность и понятие информационной безопасности, характеристику её составляющих;<br/> место информационной безопасности в системе национальной безопасности страны;<br/> виды угроз информационной безопасности;<br/> основные положения комплексного подхода к защите информации;<br/> основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ и ФСТЭК РФ в данной области;<br/> принципы архитектурной безопасности;<br/> современные программно-технические средства обеспечения информационной безопасности;<br/> виды систем идентификации и аутентификации;<br/>  типовые модели управления доступом;<br/>  типовые средства и методы ведения аудита;<br/> основные понятия криптографии;<br/>  типовые криптографические алгоритмы, применяемые для защиты информации;</p> |

## 2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 2.1 Объем учебной дисциплины и виды учебной работы

| <b>Вид учебной работы</b>   | <b>Количество часов</b> |
|---|-------------------------|
| <b>Объем образовательной нагрузки (всего)</b>                               | 88                      |
| <b>Обязательная аудиторная учебная нагрузка (всего)</b>                     | 80                      |
| <b>Практическая подготовка</b>  | 80                      |
| в том числе:  |                         |
| теоретические занятия   | 26                      |
| практические занятия  | 50                      |
| контрольные занятия   | -                       |
| курсовая работа/проект  | -                       |
| <b>Самостоятельная учебная работа обучающегося (всего)</b>                  | 4                       |
| <b>Консультации</b>   | 4                       |
| <b>Промежуточная аттестация (итоговая по дисциплине) – в форме экзамена</b> | 4                       |

## 2.2 Тематический план учебной дисциплины

| Наименование разделов и тем  | Объем образовательной нагрузки (час) | Обязательная нагрузка |                         |                             |                            |                           |                              | Самостоятельная учебная работа (час) | Консультации (час) | Промежуточная аттестация (итоговая по дисциплине) (час) |
|--|--------------------------------------|-----------------------|-------------------------|-----------------------------|----------------------------|---------------------------|------------------------------|--------------------------------------|--------------------|---|
|  |                                      | Всего часов           | Практическая подготовка | в том числе                 |                            |                           |                              |                                      |                    |   |
|  |                                      |                       |                         | теоретических занятий (час) | практических занятий (час) | контрольных занятий (час) | курсовая работа/проект (час) |                                      |                    |   |
| 1  | 2                                    | 3                     | 4                       | 5                           | 6                          | 7                         | 8                            | 9                                    | 10                 | 11  |
| <i>4 курс</i>  |                                      |                       |                         |                             |                            |                           |                              |                                      |                    |   |
| <b>Раздел 1. Понятие и основные составляющие ИБ</b>  | <b>4</b>                             | <b>4</b>              | <b>4</b>                | <b>2</b>                    | <b>2</b>                   | -                         | -                            | -                                    | -                  | -   |
| Тема 1.1 Введение. Сущность и понятие ИБ. Стартовая диагностика обучающихся  | 2                                    | 2                     | 2                       | 2                           | -                          | -                         | -                            | -                                    | -                  | -   |
| Практическое занятие № 1 Анализ примеров нарушений ИБ. Выявление значимых составляющих ИБ и характеристик ИС в конкретных ситуациях.   | 2                                    | 2                     | 2                       | -                           | 2                          | -                         | -                            | -                                    | -                  | -   |
| <b>Раздел 2. Виды угроз ИБ</b>   | <b>6</b>                             | <b>6</b>              | <b>6</b>                | <b>4</b>                    | <b>2</b>                   | -                         | -                            | -                                    | -                  | -   |
| Тема 2.1 Понятие угрозы.   | 2                                    | 2                     | 2                       | 2                           | -                          | -                         | -                            | -                                    | -                  | -   |
| Тема 2.2 Угрозы нарушения конфиденциальности, целостности, доступности.  | 2                                    | 2                     | 2                       | 2                           | -                          | -                         | -                            | -                                    | -                  | -   |
| Практическое занятие №2 Решение ситуационных задач: выявление угроз ИБ в конкретных ситуациях. Демонстрация подлога при разрешении символического имени в IP-адрес путём модификации файла hosts. Изложение схемы атаки на отказ в обслуживании (атаки SYN-шторм, ICMP-шторм). | 2                                    | 2                     | 2                       | -                           | 2                          | -                         | -                            | -                                    | -                  | -   |
| <b>Раздел 3. Вредоносное программное обеспечение (ПО)</b>  | <b>10</b>                            | <b>10</b>             | <b>10</b>               | <b>2</b>                    | <b>8</b>                   | -                         | -                            | -                                    | -                  | -   |

|  |          |          |          |          |          |   |   |          |   |   |
|--|----------|----------|----------|----------|----------|---|---|----------|---|---|
| Тема 3.1 Понятие вредоносного ПО и каналы его распространения.   | 2        | 2        | 2        | 2        | -        | - | - | -        | - | - |
| Практическое занятие № 3<br>Определение функциональных возможностей и принципов работы троянской программы на примере клавиатурного шпиона.  | 2        | 2        | 2        | -        | 2        | - | - | -        | - | - |
| Практическое занятие №4<br>Выполнение проверки компьютера на наличие признаков заражения вредоносным ПО: исследование настроек браузера, запущенных процессов, элементов автозапуска, сетевой активности.  | 2        | 2        | 2        | -        | 2        | - | - | -        | - | - |
| Практическое занятие № 5<br>Обоснование применения норм уголовного права в конкретных ситуациях, связанных с созданием и использованием вредоносного ПО.   | 2        | 2        | 2        | -        | 2        | - | - | -        | - | - |
| Практическое занятие № 6<br>Выполнение установки антивирусного ПО. Обоснование выбора устанавливаемых компонентов. Обновление антивирусных баз. Выполнение настройки параметров антивирусной и проактивной защиты. Настройка уведомлений. Выполнение антивирусного сканирования с заданными параметрами. | 2        | 2        | 2        | -        | 2        | - | - | -        | - | - |
| <b>Раздел 4. Правовые основы обеспечения ИБ</b>  | <b>6</b> | <b>6</b> | <b>4</b> | <b>2</b> | <b>2</b> | - | - | <b>2</b> | - | - |
| Тема 4.1 Структура правового обеспечения ИБ.   | 2        | 2        | 2        | 2        | -        | - | - | -        | - | - |
| Самостоятельная работа № 1<br>Классификация информации по видам тайн. Защита прав собственности на информацию.   | 2        | 2        | 2        | -        | -        | - | - | 2        | - | - |



|   |           |          |           |          |          |          |   |          |   |   |
|---|-----------|----------|-----------|----------|----------|----------|---|----------|---|---|
| Практическое занятие № 7<br>Решение ситуационных задач: нахождение применимых правовых норм в заданных условиях.  | 2         | 2        | 2         | -        | 2        | -        | - | -        | - | - |
| <b>Раздел 5. Оценочные стандарты и технические спецификации в области ИБ</b>  | <b>10</b> | <b>8</b> | <b>10</b> | <b>2</b> | <b>6</b> | -        | - | <b>2</b> | - | - |
| Тема 5.1 «Оранжевая книга». ИБ распределённых систем. Рекомендации X.800.   | 2         | 2        | 2         | 2        | -        | -        | - | -        | - | - |
| Самостоятельная работа № 2 «Общие критерии». Стандарт ISO/IEC 15408. Управление ИБ. Серия стандартов ISO/IEC 27000. Руководящие документы ФСТЭК (Гостехкомиссии) и ФСБ. Спецификации RFC.                                       | 2         | 2        | 2         | -        | -        | -        | - | 2        | - | - |
| Практическое занятие №8<br>Изложение практических рекомендаций по управлению ИБ по отношению к одному из сервисов безопасности, описанных в ГОСТ Р 17799-2005.  | 2         | 2        | 2         | -        | 2        | -        | - | -        | - | - |
| Практическое занятие №9<br>Определение класса ИС персональных данных (ИСПДн) для ИС гипотетической организации в соответствии с совместным приказом ФСТЭК, ФСБ и Мининформсвязи РФ № 55/86/20 от 13 февраля 2008 г.             | 2         | 2        | 2         | -        | 2        | -        | - | -        | - | - |
| Практическое занятие №10<br>Выполнение оценки исходной степени защищённости ИСПДн, выделение актуальных угроз безопасности в соответствии с «Методикой определения актуальных угроз безопасности ПДн при их обработке в ИСПДн». | 2         | 2        | 2         | -        | 2        | -        | - | -        | - | - |
| <b>Раздел 6. Принципы обеспечения ИБ на программно-техническом уровне</b>   | <b>8</b>  | <b>8</b> | <b>8</b>  | <b>4</b> | <b>2</b> | <b>2</b> | - | -        | - | - |

|   |           |           |           |          |           |   |   |   |   |   |
|---|-----------|-----------|-----------|----------|-----------|---|---|---|---|---|
| Тема 6.1 Административный уровень ИБ. Процедурный уровень ИБ.   | 2         | 2         | 2         | 2        | -         | - | - | - | - | - |
| Тема 6.2 Основные понятия программно-технического уровня ИБ. Принципы архитектурной безопасности.   | 2         | 2         | 2         | 2        | -         | - | - | - | - | - |
| Практическое занятие №11<br>Решение ситуационных задач: обоснование применения принципов архитектурной безопасности в заданных условиях.                | 2         | 2         | 2         | -        | 2         | - | - | - | - | - |
| Контрольное занятие № 1.<br>Выполнение комплексных заданий  | 2         | 2         | 2         | -        | -         | 2 | - | - | - | - |
| <b>Раздел 7. Средства обеспечения конфиденциальности</b>  | <b>24</b> | <b>24</b> | <b>24</b> | <b>4</b> | <b>20</b> | - | - | - | - | - |
| Тема 7.1 Построение систем защиты от угроз нарушения конфиденциальности. Идентификация и аутентификация. Управление доступом. Протоколирование и аудит. | 2         | 2         | 2         | 2        | -         | - | - | - | - | - |
| Тема 7.2 Симметричное и асимметричное шифрование. Скрытие информации (стеганография). Экранирование и анализ защищённости. Туннелирование.              | 2         | 2         | 2         | 2        | -         | - | - | - | - | - |
| Практическое занятие №12<br>Создание пользователей и групп в операционной системе (ОС) Windows. Решение задач поиска и сброса паролей пользователей.    | 2         | 2         | 2         | -        | 2         | - | - | - | - | - |
| Практическое занятие №13<br>Выполнение настройки системы парольной защиты в локальной политике безопасности ОС Windows.                                 | 2         | 2         | 2         | -        | 2         | - | - | - | - | - |
| Практическое занятие №14<br>Создание списков контроля доступа и назначение прав доступа на уровне файловой системы NTFS в заданных условиях.            | 2         | 2         | 2         | -        | 2         | - | - | - | - | - |

|  |          |          |          |          |          |   |   |   |   |   |
|--|----------|----------|----------|----------|----------|---|---|---|---|---|
| Практическое занятие №15<br>Выполнение настройки параметров аудита в ОС Windows в заданных условиях. Получение и интерпретация результатов аудита.         | 2        | 2        | 2        | -        | 2        | - | - | - | - | - |
| Практическое занятие №16<br>Выполнение установки ПО для работы с инфраструктурой открытых ключей. Создание открытого и закрытого криптографических ключей. | 2        | 2        | 2        | -        | 2        | - | - | - | - | - |
| Практическое занятие №17<br>Создание открытого и закрытого криптографических ключей.   | 2        | 2        | 2        | -        | 2        | - | - | - | - | - |
| Практическое занятие №18<br>Выполнение установки ПО для стеганографического преобразования. Выполнение операций по скрытию и обмену скрытой информацией.   | 2        | 2        | 2        | -        | 2        | - | - | - | - | - |
| Практическое занятие №19<br>Выполнение установки сетевого сканера. Определение списка открытых портов в ОС Windows при помощи сетевого сканера.            | 2        | 2        | 2        | -        | 2        | - | - | - | - | - |
| Практическое занятие №20<br>Выполнение настройки межсетевого экрана: создание правил фильтрации пакетов для предотвращения доступа к внутренним сервисам.  | 2        | 2        | 2        | -        | 2        | - | - | - | - | - |
| Практическое занятие №21<br>Выполнение настройки межсетевого экрана: создание правил фильтрации пакетов для предотвращения доступа к внутренним сервисам.  | 2        | 2        | 2        | -        | 2        | - | - | - | - | - |
| <b>Раздел 8. Средства обеспечения целостности</b>  | <b>6</b> | <b>6</b> | <b>6</b> | <b>2</b> | <b>4</b> | - | - | - | - | - |
| Тема 8.1 Построение систем защиты от угроз нарушения целостности. Криптографические хеш-функции. Электронная цифровая подпись (ЭЦП).                       | 2        | 2        | 2        | 2        | -        | - | - | - | - | - |

|   |           |           |           |           |           |          |   |          |          |          |
|---|-----------|-----------|-----------|-----------|-----------|----------|---|----------|----------|----------|
| Практическое занятие №22<br>Установка ПО для расчёта хешей. Определение целостности файла при помощи хеш-функций MD5 и SHA-1.   | 2         | 2         | 2         | -         | 2         | -        | - | -        | -        | -        |
| Практическое занятие №23<br>Выполнение операций по обмену открытыми ключами через инфраструктуру открытых ключей, отправке и получению зашифрованных и подписанных ЭЦП документов.          | 2         | 2         | 2         | -         | 2         | -        | - | -        | -        | -        |
| <b>Раздел 9. Средства обеспечения доступности</b>   | <b>6</b>  | <b>6</b>  | <b>6</b>  | <b>2</b>  | <b>4</b>  | -        | - | -        | -        | -        |
| Тема 9.1 Задача обеспечения высокой доступности. Построение систем защиты от угроз нарушения доступности. Управление информационными сервисами и сервисами безопасности.                    | 2         | 2         | 2         | 2         | -         | -        | - | -        | -        | -        |
| Практическое занятие №24<br>Выполнение настройки параметров резервного копирования дисков в соответствии с разработанным планом. Выполнение резервного копирования и восстановления данных. | 2         | 2         | 2         | -         | 2         | -        | - | -        | -        | -        |
| Практическое занятие №25<br>Создание программного RAID-массива типа «зеркало». Выполнение замеров производительности и тестирование отказа одного из элементов RAID-массива.                | 2         | 2         | 2         | -         | 2         | -        | - | -        | -        | -        |
| <b>Консультации</b>   | <b>4</b>  | -         | -         | -         | -         | -        | - | -        | <b>4</b> | -        |
| <b>Экзамен</b>  | <b>4</b>  | -         | -         | -         | -         | -        | - | -        | -        | <b>4</b> |
| <b>Всего:</b>   | <b>88</b> | <b>76</b> | <b>80</b> | <b>24</b> | <b>50</b> | <b>2</b> | - | <b>4</b> | <b>4</b> | <b>4</b> |

### **3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ**

#### **3.1 Требования к минимальному материально-техническому обеспечению**

Освоение программы учебной дисциплины предполагает наличие мастерской «Организации и принципов построения информационных систем».

##### **Оборудование и технические средства обучения:**

1. Комплект компьютерного оборудования (системный блок, монитор, клавиатура, мышь) – 15 шт.
2. Проектор – 1 шт.
3. Мультимедийная доска – 1 шт.
4. Колонки компьютерные – 2 шт.

##### **Имущество:**

1. Стол ученический (одноместный) – 14 шт.
2. Стол ученический (двухместный) – 12 шт.
3. Стол преподавателя – 2 шт.
4. Стул – 41 шт.
5. Тумба (кафедра) – 1 шт.

#### **3.2. Информационное обеспечение обучения**

##### **Основная 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, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518006>.

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, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518005>.

3. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519614>.

### **Дополнительная литература**

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 ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/512861>.

2. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/156401>. — Режим доступа: для авториз. пользователей.

### **Перечень используемого программного обеспечения:**

1. Microsoft Office
2. Microsoft Windows

### **Перечень используемых профессиональных баз данных и информационных справочных систем:**

1. ЭБС Электронного издания ЮРАЙТ
2. ЭБС «ЛАНЬ»

#### 4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины ОП.ДВ.13 Основы информационной безопасности осуществляется преподавателем в процессе Мониторинга динамики индивидуальных достижений обучающихся по учебной дисциплине, включающего текущий контроль и промежуточную аттестацию.

| Тип задания   | Формы и методы контроля и оценки  | Проверяемые образовательные результаты          |
|---|---|---|
| Задания для текущего контроля   |   |   |
| Задания для стартовой диагностики   | Устный опрос  | 31-35<br>ОК 5                                   |
| Тестовые задания  | Оценка результатов тестирования   | 31-35,<br>У1-У3<br>ОК ПК                        |
| Практические задания  | Оценка выполненных заданий<br>Наблюдение за деятельностью обучающихся<br>Сравнение с эталоном<br>Контроль правильности алгоритма выполнения | У1-У3,<br>31-35,<br>ОК 1,2,4,5,9<br>ПК 4.1, 4.2 |
| Подготовка и защита научно-исследовательской работы (проекты, рефераты, сообщения, презентации) | Экспертная оценка работы, устной защиты, презентации по критериям   | У1-У3,<br>31-35,<br>ОК 1,2,4,5,9<br>ПК 4.1, 4.2 |
| Контрольная работа (контрольное занятие)  | Оценка результатов тестирования<br>Наблюдение за деятельностью обучающихся<br>Сравнение с эталоном  | У1-У3,<br>31-35,<br>ОК 1,2,4,5,9<br>ПК 4.1, 4.2 |
| Задания для промежуточной аттестации  |   |   |
| Тестовые задания  | Оценка результатов тестирования   | 31-35,<br>У1-У3<br>ОК ПК                        |
| Практические задания  | Оценка выполненных заданий<br>Наблюдение за деятельностью обучающихся   | У1-У3,<br>31-35,<br>ОК 1,2,4,5,9<br>ПК 4.1, 4.2 |

Текущий контроль успеваемости подразумевает регулярную объективную оценку качества освоения обучающимися содержания учебной дисциплины ОП.ДВ.13 Основы информационной безопасности способствует успешному овладению учебным материалом в разнообразных формах аудиторной работы, в процессе внеаудиторной подготовки и оценивает систематичность учебной работы студента.

В начале изучения дисциплины ОП.ДВ.13 Основы информационной безопасности (в течение первых двух недель) осуществляется стартовая диагностика обучающихся. Входной контроль проводится с целью определения стартового уровня подготовки студентов, который в дальнейшем сравнивается с результатами следующих этапов мониторинга уровня достижения планируемых образовательных результатов; выстраивания индивидуальной траектории обучения на основе контроля их знаний. Результаты входного контроля являются основанием для проведения корректирующих мероприятий, а также формирования подгрупп и организации дополнительных консультаций.

Промежуточная аттестация по учебной дисциплине ОП.ДВ.13 Основы информационной безопасности осуществляется в форме дифференцированного зачета.

Условием допуска к дифференцированному зачету является положительная аттестация обучающихся по результатам текущего и рубежного контроля, выполнение всех заданий для внеаудиторной самостоятельной работы.

Дифференцированный зачет по учебной дисциплине проводится с учетом результатов текущего и рубежного контроля на основе балльно-рейтинговой системы оценивания. Обучающийся, имеющий итоговый рейтинг от 4,5 до 5 баллов, освобождается от выполнения заданий и получает оценку «отлично». Обучающийся, имеющий рейтинг от 4,0 до 4,4 баллов, освобождается от выполнения заданий и получает оценку «хорошо», если студент претендует на оценку «отлично», проходит тестирование. При этом педагогом учитывается, что обучающийся за оцениваемый период не пропустил ни одного занятия, при определении «итоговой» оценки за семестр средневзвешенная оценка по результатам текущего контроля увеличивается на 0,5 баллов.