**ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**
**«ВЛАДИКАВКАЗСКИЙ ПРОФЕССИОНАЛЬНЫЙ КОЛЛЕДЖ»**
**(ЧПОУ ВПК)**

**РАССМОТРЕНО**
на заседании Педагогического совета
Протокол № 12
от «29» мая 2026 г.

**УТВЕРЖДАЮ**
Директор ЧПОУ ВПК

Сведения об электронной подписи
**Подписано:** Хутинаева Светлана Зураповна
**Должность:** директор
**Пользователь:** skhutinaeva

Приказ № 30-Д от «29» мая 2026г.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

# ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

среднего профессионального образования
по программе подготовки специалистов среднего звена (ППССЗ)
**09.02.11 Разработка и управление программным обеспечением**

Квалификация:
программист
Форма обучения: очная
Нормативный срок обучения:
2 год 10 месяцев на базе среднего общего образования

2026

Рабочая программа дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности **09.02.11 Разработка и управление программным обеспечением**

**Организация - разработчик:**ЧПОУ ВПК

**Разработчики:** к.пед.н., Хутинаева С.З., нач.уч.части Томаева З.А.

## СОДЕРЖАНИЕ

1. **ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**
2. **СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**
3. **УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ**
4. **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ**

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

**1.1. Цель и место дисциплины в структуре основной образовательной программы:**

Цель дисциплины «Основы информационной безопасности»: формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Дисциплина «Основы информационной безопасности» включена в обязательную часть общепрофессионального цикла образовательной программы.

**1.2. Планируемые результаты освоения дисциплины:**

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ПОП).

В результате освоения дисциплины обучающийся должен:

| Код ОК, ПК | Уметь | Знать | Владеть навыками |
|---|---|---|---|
| ОК.01 | 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; составлять план действия; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) | 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 | определять задачи для поиска информации; определять | номенклатура информационных | - |

| | | | |
|---|---|---|---|
| | 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; использовать различные цифровые средства для решения профессиональных задач | 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 в том числе с использованием цифровых средств. | |
| ОК.09 | понимать тексты на базовые профессиональные темы | лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности | - |
| ПК 1.1 | - | принципы безопасности хранения данных | - |
| ПК 1.4 | - | методы защиты баз данных от внешних угроз | - |
| ПК 1.5 | шифровать данные и обеспечивать их конфиденциальность | принципы криптографии и методов шифрования данных<br>стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.<br>методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных<br>законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др. | - |
| ПК 3.1 | - | отраслевая нормативная техническая | - |

| | | | |
|---|---|---|---|
| | | документация источники информации, необходимой для профессиональной деятельности | |
| | | современный отечественный и зарубежный опыт в профессиональной деятельности | - |
| ПК 3.2 | - | принципы и методы обеспечения безопасности информационных систем | - |
| ПК 3.3 | анализ требований безопасности информационных систем | принципов безопасности информационных систем<br>современных методов и технологий в области безопасности информационных систем<br>законодательных и нормативных актов в области безопасности информационных систем | применение современных методов и технологий в области безопасности информационных систем |
| ПК 3.5 | - | источники угроз информационной безопасности и меры по их предотвращению | - |
| ПК 3.7 | разрабатывать и реализовывать меры безопасности<br>реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию | основные угрозы безопасности мобильных приложений<br>принципы криптографии и шифрования данных.<br>стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect<br>законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA<br>основные принципы безопасности информации и методов ее защиты. | использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные.<br>применение механизмов хеширования для защиты паролей пользователей от несанкционированного доступа.<br>обеспечение |

| | | | |
|---|---|---|---|
| | | стандартные криптографические алгоритмы для шифрования данных<br>принципы обеспечения безопасности передачи данных по сети<br>основы безопасности приложений и инфраструктуры<br>методы анализа на уязвимости и мониторинга безопасности<br>знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений<br>понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения<br>знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы | безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS<br>соблюдение законодательства и регуляций в области защиты данных |

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

| Вид учебной работы | Объем в часах |
|---|---|
| **Объем образовательной программы учебной дисциплины** | 32 |
| **в т.ч. в форме практической подготовки** | 16 |
| в т. ч.: | |
| теоретическое обучение | 10 |
| практические занятия | 16 |
| **Промежуточная аттестация (экзамен)** | 6 |

**2.2. Тематический план и содержание учебной дисциплины**

| Наименование разделов и тем | Содержание учебного материала, практических и лабораторных занятий | Объем, акад. ч. /в том числе в форме практической подготовки, акад. ч | Коды компетенций, формированию которых способствует элемент программы |
|---|---|---|---|
| **Тема 1. Введение в информационную безопасность** | **Содержание** | **1** | ОК.01, ОК.02, ОК.09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7 |
| | Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности | 1 | |
| **Тема 2. Управление безопасностью информации** | **Содержание** | **1** | |
| | Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.) | 1 | |
| **Тема 3. Криптография** | **Содержание** | **3/2** | |
| | Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография. | 1 | |
| | **В том числе практических и лабораторных занятий** | | |
| | Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой2 подписи сообщения. | 2 | |
| **Тема 4. Защита сетевой инфраструктуры** | **Содержание** | **5/4** | |
| | Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов | 1 | |
| | **В том числе практических и лабораторных занятий** | | |
| | Организация защиты от атак | 2 | |
| | Организация работы VPN и межсетевого экрана | 2 | |
| **Тема 5. Безопасность приложений** | **Содержание** | **3/2** | |
| | Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей. | 1 | |
| | **В том числе практических и лабораторных занятий** | | |

| | | | |
|---|---|---|---|
| | Тестирование на проникновение и анализ уязвимостей. | 2 | |
| **Тема 6. Защита данных** | **Содержание** | **3/2** | |
| | Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным | 1 | |
| | **В том числе практических и лабораторных занятий** | | |
| | Выполнение резервного копирования и восстановления данных. Управление доступом к данным | 2 | |
| **Тема 7. Безопасность облачных технологий** | **Содержание** | **3/2** | |
| | Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности | 1 | |
| | **В том числе практических и лабораторных занятий** | | |
| | Изучение модели облачных услуг и их безопасности | 2 | |
| **Тема 8. Инциденты безопасности** | **Содержание** | **3/2** | |
| | Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика | 1 | |
| | **В том числе практических и лабораторных занятий** | | |
| | Работа с инцидентами. | 2 | |
| **Тема 9. Социальная инженерия и человеческий фактор** | **Содержание** | **3/2** | |
| | Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности | 1 | |
| | **В том числе практических и лабораторных занятий** | | |
| | Разработка политики информационной безопасности | 2 | |
| **Тема 10. Будущее информационной безопасности** | **Содержание** | **1** | |
| | Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности | 1 | |
| **Промежуточная аттестация (экзамен)** | | **6** | |
| **Всего** | | **32** | |

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 3.1 Материально-техническое обеспечение

Реализация программы учебной дисциплины производится с применением дистанционных технологий и требует наличия электронной образовательной среды; учебного кабинета, лаборатории «Компьютерных сетей и основ информационной безопасности».

**Оборудование учебного кабинета:**

- классная доска;
- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- учебно-практическое оборудование, необходимое для проведения предусмотренных программой практических занятий. В соответствие с п.4.4 ФГОС СПО допускается замена оборудования его виртуальными аналогами.

**Технические средства обучения:**

- компьютеры с выходом в сеть Internet;
- сайт «Личная студия» с возможностью работы с электронным образовательным ресурсом;
- электронные библиотечные ресурсы.

**Учебно-методическое обеспечение дисциплины:**

• методические указания по организации практических занятий;

• методические указания по самостоятельной работе.

**Программное обеспечение:**

Программное обеспечение, являющееся частью электронной информационно-образовательной среды и базирующееся на телекоммуникационных технологиях:

- компьютерные обучающие программы;
- тренинговые и тестирующие программы;
- интеллектуальные роботизированные системы оценки качества выполненных работ;
- справочно-правовая система «Консультант плюс», «Гарант»;
- электронно-библиотечная система (ЭБС) ЭБС «IPR SMART» http://iprbookshop.ru/;
- программа управления образовательным процессом в ЭИОС (Информационная технология. Программа управления образовательным процессом. КОМБАТ).

### 3.2. Информационное обеспечение реализации программы

**Основные источники**

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 84 с. — ISBN 978-5-507-48808-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394547 (дата обращения: 16.11.2024).

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 284 с. — ISBN 978-5-507-49251-0.

— Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414950 (дата обращения: 16.11.2024).

3. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 16.11.2024)

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082 (дата обращения: 16.11.2024)

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

| Результаты обучения | Критерии оценки | Методы оценки |
|---|---|---|
| ***Знает:***<br>- актуальный профессиональный и социальный контекст, в котором приходится работать и жить;<br>-основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;<br>- алгоритмы выполнения работ в профессиональной и смежных областях;<br>- методы работы в профессиональной и смежных сферах;<br>- структуру плана для решения задач;<br>- порядок оценки результатов решения задач профессиональной деятельности<br>- номенклатуру информационных источников, применяемых в профессиональной деятельности;<br>- приемы структурирования информации;<br>- формат оформления результатов поиска информации, современные | Ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить;<br>Владеет основными источниками информации и ресурсами для решения задач и проблем в профессиональном и/или социальном контексте;<br>Знает алгоритмы выполнения работ в профессиональной и смежных областях;<br>Знает методы работы в профессиональной и смежных сферах;<br>Знает структуру плана для решения задач;<br>Может произвести оценку результатов решения задач профессиональной деятельности<br>Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности;<br>Знает приемы структурирования информации;<br>Знает формат оформления результатов поиска информации, современные средства и устройства информатизации;<br>Может применять современные средства и устройства | Штудирование<br><br>Тестирование<br><br>Выполнение практических заданий<br><br>Выполнение заданий на экзамене |

| | | |
|---|---|---|
| средства и устройства информатизации;<br>- порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств;<br>- лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности;<br>- принципы безопасности хранения данных;<br><br>- методы защиты баз данных от внешних угроз<br>- принципы криптографии и методов шифрования данных;<br>- стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.;<br>- методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных<br>законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.;<br>- отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности;<br>- современный отечественный и зарубежный опыт в профессиональной деятельности;<br>- принципы и методы обеспечения безопасности информационных систем;<br>- принципы безопасности информационных систем;<br><br>- современные методы и технологии в области безопасности информационных | информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств;<br><br>Владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности;<br>Знает принципы безопасности хранения данных;<br>Владеет методами защиты баз данных от внешних угроз<br>Знает принципы криптографии и методов шифрования данных;<br>Ориентируется в стандартах и протоколах безопасности, таких как SSL/TLS, SSH, Kerberos и др.;<br>Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных<br>законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.;<br>Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности;<br><br>Знает современный отечественный и зарубежный опыт в профессиональной деятельности;<br>Владеет принципами и методами обеспечения безопасности информационных систем;<br>Знает принципы безопасности информационных систем;<br>Владеет современными методами и технологиями в области безопасности информационных систем;<br>Знает законодательные и нормативные акты в области безопасности информационных систем;<br>Знает источники угроз информационной безопасности и | |

| | | |
|---|---|---|
| систем;<br>- законодательные и нормативные акты в области безопасности информационных систем;<br>-источники угроз информационной безопасности и меры по их предотвращению;<br>- основные угрозы безопасности мобильных приложений;<br><br>- принципы криптографии и шифрования данных;<br><br>- стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect;<br>- законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA;<br>- основные принципы безопасности информации и методов ее защиты;<br><br>- стандартные криптографические алгоритмы для шифрования данных;<br>- принципы обеспечения безопасности передачи данных по сети;<br><br>- основы безопасности приложений и инфраструктуры;<br>- методы анализа на уязвимости и мониторинга безопасности;<br>- знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений;<br>- понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения;<br>- знание инструментов и технологий для обеспечения безопасности ИТ- | меры по их предотвращению;<br>Имеет представление об основных угрозах безопасности мобильных приложений;<br>Ориентируется в принципах криптографии и шифрования данных;<br>Знает стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect;<br>Знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA;<br>Владеет основными принципами безопасности информации и методов ее защиты;<br>Знает стандартные криптографические алгоритмы для шифрования данных;<br>Имеет представление о принципах обеспечения безопасности передачи данных по сети;<br>Знает основы безопасности приложений и инфраструктуры;<br>Знает методы анализа на уязвимости и мониторинга безопасности;<br><br>Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений;<br>Понимает различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения;<br><br>Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.<br><br>Может распознавать задачу и/или проблему в профессиональном и/или социальном контексте;<br>Анализирует задачу и/или проблему и может выделить её составные части; | |

| | | |
|---|---|---|
| инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.<br><br>***Умеет:***<br>-распознавать задачу и/или проблему в профессиональном и/или социальном контексте;<br>-анализировать задачу и/или проблему и выделять её составные части;<br>- определять этапы решения задачи;<br>- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;<br>-составлять план действия;<br>- определять необходимые ресурсы;<br>- владеть актуальными методами работы в профессиональной и смежных сферах;<br>- реализовывать составленный план;<br>- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);<br>- определять задачи для поиска информации;<br>- определять необходимые источники информации;<br><br>- планировать процесс поиска;<br>- структурировать получаемую информацию; - выделять наиболее значимое в перечне информации;<br>- оценивать практическую значимость результатов поиска;<br>- оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач;<br>- использовать современное программное обеспечение;<br>- использовать различные | Умеет определять этапы решения задачи;<br>Может выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;<br>Составляет план действия;<br><br>Может определять необходимые ресурсы;<br>Владеет актуальными методами работы в профессиональной и смежных сферах;<br>Может реализовывать составленный план;<br>Оценивает результат и последствия своих действий (самостоятельно или с помощью наставника);<br><br>Умеет определять задачи для поиска информации;<br>Умеет определять необходимые источники информации;<br>Планирует процесс поиска;<br><br>Умеет структурировать получаемую информацию;<br>Может выделить наиболее значимое в перечне информации;<br>Умеет оценивать практическую значимость результатов поиска;<br>Оформляет результаты поиска и применяет средства информационных технологий для решения профессиональных задач;<br><br>Может использовать современное программное обеспечение;<br>Может использовать различные цифровые средства для решения профессиональных задач;<br>Понимает тексты на базовые профессиональные темы;<br><br>Умеет шифровать данные и обеспечивать их конфиденциальность;<br>Умеет анализировать требования безопасности информационных систем; | |

| | | |
|---|---|---|
| цифровые средства для решения профессиональных задач;<br>- понимать тексты на базовые профессиональные темы;<br>- шифрование данных и обеспечивает их конфиденциальность;<br>- анализировать требования безопасности информационных систем;<br>- разрабатывать и реализовывать меры безопасности;<br>- реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию. | Может разрабатывать и реализовывать меры безопасности; Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию. | |