Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Краюшкина Марина Викторовна
Должность: Исполнительный директор
Дата подписания: 18.08.2026 22:23:05
Уникальный программный ключ:
b60019126a3f15cfd49eff4247dfc09aa2f09f7a

**Автономная некоммерческая организация профессионального образования**
**«Университетский колледж»**
**(АНО ПО «Университетский колледж»)**



**УТВЕРЖДЕНО:**
Исполнительный директор АНО ПО
«Университетский колледж»
Краюшкина М.В.
«30» марта 2026

# РАБОЧАЯ ПРОГРАММА

учебной дисциплины общего профессионального цикла

# «ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

по специальности среднего профессионального образования

**09.02.11 Разработка и управление программным обеспечением**
(код, наименование специальности)

Квалификация выпускника: Программист

Москва, 2026

# СОДЕРЖАНИЕ ПРОГРАММЫ

**СОДЕРЖАНИЕ ПРОГРАММЫ ..... 2**

**1. Общая характеристика ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ..... 3**

*1.1. Цель и место дисциплины в структуре образовательной программы ..... 3*

*1.2. Планируемые результаты освоения дисциплины ..... 3*

**2. Структура и содержание ДИСЦИПЛИНЫ ..... 7**

*2.1. Трудоемкость освоения дисциплины ..... 7*

*2.2. Примерное содержание дисциплины ..... 7*

**3. Условия реализации ДИСЦИПЛИНЫ ..... 9**

*3.1. Материально-техническое обеспечение ..... 9*

*3.2. Учебно-методическое обеспечение ..... 9*

**4. Контроль и оценка результатов освоения ДИСЦИПЛИНЫ ..... 9**

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОП.05 Основы информационной безопасности»

## 1.1. Цель и место дисциплины в структуре 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[1]:

| ***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 | 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 | - |

[1] *Берутся сведения, указанные по данному виду деятельности в п. 4.2.*

| | | | |
|---|---|---|---|
| | действий (самостоятельно или с помощью наставника) | | |
| ОК.02 | 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; использовать различные цифровые средства для решения профессиональных задач | 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 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<br>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.<br>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 | 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 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 |

| | | | |
|---|---|---|---|
| | | брандмауэры, системы обнаружения вторжений и антивирусные программы | |

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 2.1. Трудоемкость освоения дисциплины

| Наименование составных частей дисциплины | Объем в часах | В т.ч. в форме практ. подготовки |
|---|---|---|
| Учебные занятия | 64 | 46 |
| Самостоятельная работа | - | - |
| Промежуточная аттестация | XX | XX |
| Всего | **64** | **46** |

### 2.2. Примерное содержание дисциплины

| Наименование разделов и тем | Примерное содержание учебного материала, практических и лабораторных занятий, *курсовой проект (работа)* |
|---|---|
| **Раздел 1. Основы информационной безопасности (64 часа)** | |
| **Тема 1.1. Введение в информационную безопасность** | **Содержание** |
| | Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности |
| | **В том числе самостоятельная работа обучающихся** *Необходимость и тематика определяются образовательной организацией* |
| **Тема 1.2. Управление безопасностью информации** | **Содержание** |
| | Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.) |
| | **В том числе самостоятельная работа обучающихся** *Необходимость и тематика определяются образовательной организацией* |
| **Тема 1.3. Криптография** | **Содержание** |
| | Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография. |
| | **В том числе практических и лабораторных занятий** |
| | Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения. |
| | **В том числе самостоятельная работа обучающихся** *Необходимость и тематика определяются образовательной организацией* |
| **Тема 1.4. Защита сетевой инфраструктуры** | **Содержание** |
| | Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов |
| | **В том числе практических и лабораторных занятий** |
| | Организация защиты от атак |

| | |
|---|---|
| | Организация работы VPN и межсетевого экрана |
| | **В том числе самостоятельная работа обучающихся**<br>*Необходимость и тематика определяются образовательной организацией* |
| **Тема 1.5. Безопасность приложений** | **Содержание** |
| | Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей. |
| | **В том числе практических и лабораторных занятий** |
| | Тестирование на проникновение и анализ уязвимостей. |
| | **В том числе самостоятельная работа обучающихся**<br>*Необходимость и тематика определяются образовательной организацией* |
| **Тема 1.6. Защита данных** | **Содержание** |
| | Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным |
| | **В том числе практических и лабораторных занятий** |
| | Выполнение резервного копирования и восстановления данных. Управление доступом к данным |
| | **В том числе самостоятельная работа обучающихся**<br>*Необходимость и тематика определяются образовательной организацией* |
| **Тема 1.7. Безопасность облачных технологий** | **Содержание** |
| | Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности |
| | **В том числе практических и лабораторных занятий** |
| | Изучение модели облачных услуг и их безопасности |
| | **В том числе самостоятельная работа обучающихся**<br>*Необходимость и тематика определяются образовательной организацией* |
| **Тема 1.8. Инциденты безопасности** | **Содержание** |
| | Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика |
| | **В том числе практических и лабораторных занятий** |
| | Работа с инцидентами. |
| | **В том числе самостоятельная работа обучающихся**<br>*Необходимость и тематика определяются образовательной организацией* |
| **Тема 1.9. Социальная инженерия и человеческий фактор** | **Содержание** |
| | Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности |
| | **В том числе практических и лабораторных занятий** |
| | Разработка политики информационной безопасности |
| | **В том числе самостоятельная работа обучающихся**<br>*Необходимость и тематика определяются образовательной организацией* |
| **Тема 1.10. Будущее информационной безопасности** | **Содержание** |
| | Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности |
| | **В том числе самостоятельная работа обучающихся**<br>*Необходимость и тематика определяются образовательной организацией* |
| **Промежуточная аттестация** | |
| **Всего 64 часа** | |

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

### 3.1. Материально-техническое обеспечение

Лаборатория «Компьютерных сетей и основ информационной безопасности»: 1 доска ученическая, 1 рабочее место преподавателя, 15 столов ученических, 30 стульев ученических, 15 персональных компьютеров, 1 принтер RICOH SP 220, 1 МФУ DCP Brother LTR A4, 1 МФУ HP Laser Jet MFP M436n. Программное обеспечение: 15 Microsoft®WindowsProfessional 10 Russian Upgrade Academic OLV 1License NoLevel AdditionalProduct Each, 15 Microsoft®Office 2019 Russian Academic OLV 1License NoLevel AdditionalProduct Each, Справочно-правовая система «Консультант плюс» .

### 3.2. Учебно-методическое обеспечение

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

#### 3.2.1. Основные печатные и/или электронные издания

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587457.

2. 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, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587458.

3. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт.

4. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588515

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

| Результаты обучения | Показатели освоенности компетенций | Методы оценки |
|---|---|---|
| ***Знает:*** | | Экспертное наблюдение выполнения практических |

| | | |
|---|---|---|
| - 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 средства и устройства информатизации;<br>- порядок применения современных средств и устройств информатизации и программное обеспечение в | 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 информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; | работ и видов работ по практике<br>Диагностика (тестирование, контрольные работы) |

| | | |
|---|---|---|
| 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 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; | 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 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; | |

| | | |
|---|---|---|
| - принципы и методы обеспечения безопасности информационных систем;<br>- принципы безопасности информационных систем;<br><br>- современные методы и технологии в области безопасности информационных 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; | 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 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 | |

| | | |
|---|---|---|
| - 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-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; | 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;<br><br>Умеет определять этапы решения задачи;<br>Может выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; | |

| | | |
|---|---|---|
| - 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 | 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; | |

| | | |
|---|---|---|
| программное обеспечение;<br>- использовать различные 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. | Понимает тексты на базовые профессиональные темы;<br><br>Умеет шифровать данные и обеспечивать их конфиденциальность;<br>Умеет анализировать требования безопасности информационных систем;<br>Может разрабатывать и реализовывать меры безопасности;<br>Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию. | |