



УТВЕРЖДАЮ
Заместитель директора Ур СЭИ (филиал)
ОУП ВО «АТиСО» по УВР

_____ О.В. Зубкова

« 17 » февраля 2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПЦ.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**СПЕЦИАЛЬНОСТЬ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО
ОБРАЗОВАНИЯ**

09.02.11 Разработка и управление программным обеспечением
(код профессии, специальности СПО)

Программист
(наименование квалификации)

Кафедра: Информатики и математики

Разработчик программы:
Зав. кафедрой

Маскайкин Е.П.

17 февраля 2026 г.

Оглавление

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОГО ПРЕДМЕТА, КУРСА, ДИСЦИПЛИНЫ (МОДУЛЯ)	3
2. ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	3
3. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ПРОГРАММЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА	3
4. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ:.....	4
5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	5
6. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	9
7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	10
8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	11
9. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ СО.02.02. ИНФОРМАТИКА	11

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОГО ПРЕДМЕТА, КУРСА, ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа учебной дисциплины «Основы информационной безопасности» является частью программы подготовки специалистов среднего звена (ППССЗ) в соответствии с ФГОС СПО по специальности 09.02.11 Разработка и управление программным обеспечением, квалификация – программист.

Программа может быть использована в дополнительном профессиональном образовании и профессиональной подготовке специалистов в области информационных технологий.

2. ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель изучения: 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 для обеспечения безопасности при проектировании баз данных, разработке и сопровождении бизнес-приложений.

Задачи:

- изучить основные понятия, принципы и нормативно-правовую базу информационной безопасности;
- освоить методы криптографической защиты информации (симметричные, асимметричные алгоритмы, хеширование, цифровые подписи);
- научиться выявлять и анализировать уязвимости веб-приложений и баз данных;
- сформировать навыки безопасного программирования и тестирования на проникновение;
- изучить методы защиты сетевой инфраструктуры и облачных сред;
- освоить подходы к управлению доступом, резервному копированию и защите данных;
- развить умения реагировать на инциденты безопасности и применять меры по их предотвращению;
- сформировать культуру кибербезопасности и осознание человеческого фактора.

3. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ПРОГРАММЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА

Учебная дисциплина «Основы информационной безопасности» относится к общепрофессиональному циклу (ОПЦ.05) специальности 09.02.11 Разработка и управление программным обеспечением.

Дисциплина базируется на знаниях, умениях и навыках, полученных при изучении информатики, операционных систем, архитектуры аппаратных средств, информационных технологий в профессиональной деятельности.

Знания, умения и навыки, полученные при изучении данной дисциплины, являются основой для освоения профессиональных модулей, связанных с разработкой баз данных, бизнес-приложений, а также для практической деятельности по обеспечению безопасности разрабатываемых программных продуктов и информационных систем.

4. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ:

В результате освоения дисциплины обучающийся должен овладеть следующими общими компетенциями:

Код	Формулировка компетенции
ПК 1.1	Проектировать базы данных.
ПК 3.1	Выполнять техническое проектирование бизнес-приложений и сопровождение проектных решений.
ПК 3.2	Разрабатывать бизнес-приложения.
ПК 3.6	Осуществлять поддержку и обслуживание бизнес-приложений.

Таким образом, в результате освоения дисциплины обучающийся должен:
уметь:

- У1 – распознавать задачи и проблемы в области информационной безопасности;
- У2 – выявлять и эффективно искать информацию, необходимую для решения задач безопасности;
- У3 – применять средства информационных технологий для защиты информации;
- У4 – шифровать данные и обеспечивать их конфиденциальность;
- У5 – анализировать требования безопасности информационных систем;
- У6 – разрабатывать и реализовывать меры безопасности для баз данных и приложений;
- У7 – реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию;
- У8 – проводить анализ уязвимостей и тестирование на проникновение;
- У9 – применять методы защиты сетевой инфраструктуры;
- У10 – реагировать на инциденты безопасности и восстанавливать системы.

знать:

- 31 – актуальный профессиональный и социальный контекст в области ИБ;
- 32 – основные источники информации и ресурсы для решения задач ИБ;
- 33 – номенклатуру информационных источников, применяемых в профессиональной деятельности;
- 34 – принципы безопасности хранения данных;
- 35 – методы защиты баз данных от внешних угроз;
- 36 – принципы криптографии и методов шифрования данных;
- 37 – стандарты и протоколы безопасности (SSL/TLS, SSH, Kerberos, HTTPS, OAuth и др.);
- 38 – методы аутентификации и авторизации пользователей;
- 39 – законодательство и стандарты безопасности (GDPR, HIPAA, PCI DSS и др.);
- 310 – современные методы и технологии в области безопасности информационных систем;
- 311 – источники угроз информационной безопасности и меры по их предотвращению;
- 312 – основные угрозы безопасности веб-приложений и мобильных приложений;
- 313 – основы безопасности приложений и инфраструктуры;
- 314 – методы анализа на уязвимости и мониторинга безопасности;

- 315 – инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры (брандмауэры, системы обнаружения вторжений, антивирусные программы).

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

5.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	4 семестр	Итого
Максимальная учебная нагрузка (всего)	32	32
Обязательная аудиторная учебная нагрузка (всего)	20	20
в том числе: лекции	10	10
практические занятия	10	10
Самостоятельная работа обучающегося (всего)	12	12
Промежуточная аттестация	—	—
Итоговая аттестация	Зачет (4 семестр)	Зачет

5.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
Раздел 1. Основы информационной безопасности		32	
Тема 1.1. Введение в информационную безопасность	Лекция: Основные понятия и определения. История и развитие ИБ. Актуальные угрозы и риски. Триада CIA (конфиденциальность, целостность, доступность). Самостоятельная работа: подготовка реферата «История развития информационной безопасности».	3 (1 лекция + 2 СР)	1
Тема 1.2. Управление безопасностью информации	Лекция: Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам (ISO 27001, GDPR и др.). Самостоятельная работа: изучение Федерального закона «О персональных данных» № 152-ФЗ.	3 (1 лекция + 2 СР)	1
Тема 1.3. Криптография	Лекция: Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография. Практические занятия: Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения. Самостоятельная работа: изучение алгоритмов AES, RSA, SHA.	4 (1 лекция + 2 практики + 1 СР)	2

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
Тема 1.4. Защита сетевой инфраструктуры	Лекция: Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.). Использование VPN и межсетевых экранов (Firewall). Практические занятия: Организация защиты от атак. Организация работы VPN и межсетевого экрана. Самостоятельная работа: настройка iptables в Linux.	4 (1 лекция + 2 практики + 1 СР)	2
Тема 1.5. Безопасность приложений	Лекция: Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей. Практические занятия: Тестирование на проникновение и анализ уязвимостей (на примере OWASP WebGoat). Самостоятельная работа: подготовка отчета по анализу уязвимостей.	4 (1 лекция + 2 практики + 1 СР)	2
Тема 1.6. Защита данных	Лекция: Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным. Практические занятия: Выполнение резервного копирования и восстановления данных. Управление доступом к данным (ACL, RBAC). Самостоятельная работа: разработка политики резервного копирования.	4 (1 лекция + 2 практики + 1 СР)	2
Тема 1.7. Безопасность облачных технологий	Лекция: Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасность. Практические занятия: Изучение модели облачных услуг и их безопасности (на примере Яндекс Облака). Самостоятельная работа: анализ безопасности облачного хранилища.	3 (1 лекция + 2 практики)	2

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
Тема 1.8. Инциденты безопасности	Лекция: Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика. Практические занятия: Работа с инцидентами: анализ логов, реагирование. Самостоятельная работа: подготовка плана реагирования на инциденты.	3 (1 лекция + 2 практики)	2
Тема 1.9. Социальная инженерия и человеческий фактор	Лекция: Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности. Практические занятия: Разработка политики информационной безопасности для организации. Самостоятельная работа: подготовка чек-листа по защите от социальной инженерии.	2 (1 лекция + 1 практика)	2
Тема 1.10. Будущее информационной безопасности	Лекция: Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности. Самостоятельная работа: подготовка доклада о современных трендах в ИБ.	2 (2 СР)	1
Всего		32	

6. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

6.1. Требования к минимальному материально-техническому обеспечению

Реализация программы требует наличия лаборатории «Компьютерных сетей и основ информационной безопасности», оснащённой в соответствии с требованиями ФГОС.

Оборудование лаборатории:

- рабочие места по количеству обучающихся (компьютеры с доступом в Интернет);
- рабочее место преподавателя;
- мультимедийное оборудование;
- программное обеспечение для моделирования сетей, криптографии, тестирования на проникновение (Wireshark, Nmap, OWASP WebGoat, OpenSSL, VirtualBox).

Технические средства обучения:

- компьютер, мультимедийный проектор, экран;
- доступ к сети Интернет для использования электронных образовательных ресурсов.

6.2. 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, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/587458>.
2. 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>.
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 [сайт]. — URL: <https://urait.ru/bcode/588374>.

Дополнительная литература

4. Нормативное сопровождение информационной безопасности : учебное пособие : [16+] / С. И. Фокина, А. В. Выволокина, А. Ю. Гарькушев, А. В. Липис. — Москва ; Вологда : Инфра-Инженерия, 2025. — 136 с. : ил., табл. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=725664>. — Библиогр. в кн. — ISBN 978-5-9729-2530-8. — Текст : электронный.
5. Зенков, А. В. Основы информационной безопасности : учебное пособие : [16+] / А. В. Зенков. — Москва ; Вологда : Инфра-Инженерия, 2022. — 104 с. : ил., табл. — Режим

доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=725671>. – Библиогр.: с. 95. – ISBN 978-5-9729-0864-6. – Текст : электронный.

6. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/584372>.

Ресурсы информационно-телекоммуникационной сети «Интернет», необходимые для освоения дисциплины

<https://owasp.org/>
<https://www.cisa.gov/>
<https://www.kaspersky.ru/>
<https://www.consultant.ru/>

7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Рабочая программа учебной дисциплины обеспечена оценочными материалами для проведения текущего контроля и промежуточной аттестации.

Оценочные материалы включают в себя тестовые задания, практические задания, вопросы к зачёту.

Текущий контроль осуществляется в форме проверки выполнения практических работ, устных опросов, тестирования, защиты отчётов по самостоятельной работе.

Промежуточная аттестация – зачёт в 4 семестре (включает теоретические вопросы и практическое задание).

Примерный перечень вопросов к зачёту:

1. Основные понятия информационной безопасности (CIA).
2. Нормативно-правовое регулирование ИБ в РФ.
3. Симметричные и асимметричные алгоритмы шифрования.
4. Хеширование и цифровые подписи.
5. Основные уязвимости веб-приложений (OWASP Top Ten).
6. Защита от DDoS-атак.
7. Назначение и работа межсетевого экрана.
8. VPN-технологии.
9. Шифрование данных в покое и в транзите.
10. Управление доступом к данным (ACL, RBAC).
11. Резервное копирование и восстановление данных.
12. Особенности безопасности облачных сред.
13. Реагирование на инциденты безопасности.
14. Социальная инженерия и методы защиты.
15. Тренды и новые технологии в ИБ.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

По выполнению лекционных занятий:

- вести конспект, фиксируя основные термины, алгоритмы, нормативные акты;
- после лекции прорабатывать материал по учебнику;
- выделять неясные вопросы для обсуждения с преподавателем.

По выполнению практических занятий:

- выполнять лабораторные работы, следуя инструкциям;
- фиксировать результаты, делать выводы;
- использовать программные инструменты для моделирования атак и защиты.

По самостоятельной работе:

- выполнять домашние задания, готовиться к практическим работам;
- изучать дополнительную литературу и официальную документацию;
- готовить доклады и рефераты по актуальным темам ИБ.

По подготовке к зачёту:

- повторить теоретические положения по разделам;
- проработать типовые практические задания;
- использовать вопросы для самопроверки.

9. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Фонд оценочных средств включает задания разных типов, проверяющих как знание теории, так и умение применять математические методы.

Тип задания	Инструкция	Пример задания
Задание закрытого типа на установление соответствия (Знать)	Прочитайте текст и установите соответствие между угрозами и их характеристиками.	Установите соответствие между типом угрозы и её характеристикой: А) Фишинг; Б) DDoS; В) MITM; Г) SQL-инъекция. 1) Перехват и изменение данных между узлами; 2) Массовая рассылка поддельных писем; 3) Внедрение вредоносного кода в запросы к БД; 4) Перегрузка сервера трафиком.

Тип задания	Инструкция	Пример задания
Задание закрытого типа на установление соответствия (Уметь)	Прочитайте текст и установите соответствие между алгоритмами шифрования и их типами.	Установите соответствие между алгоритмом и его типом: А) AES; Б) RSA; В) SHA-256; Г) ECDSA. 1) Асимметричное шифрование; 2) Симметричное шифрование; 3) Хеширование; 4) Цифровая подпись.
Задание закрытого типа на установление последовательности (Знать)	Прочитайте текст и установите правильную последовательность этапов реагирования на инцидент.	Расположите в правильном порядке этапы реагирования на инцидент: 1) Восстановление; 2) Обнаружение; 3) Сдерживание; 4) Анализ и устранение причины; 5) Извлечение уроков.
Задание закрытого типа на установление последовательности (Уметь)	Прочитайте текст и установите правильную последовательность действий при шифровании данных.	Расположите в правильном порядке действия при шифровании файла: 1) Выбор алгоритма; 2) Генерация ключа; 3) Шифрование данных; 4) Сохранение зашифрованного файла.
Задание с выбором одного верного ответа (Знать)	Прочитайте текст, выберите правильный ответ и запишите аргументы.	Какой протокол используется для защищённой передачи данных в вебе? 1) HTTP; 2) FTP; 3) HTTPS; 4) SMTP.
Задание с выбором одного верного ответа (Уметь)	Прочитайте текст, выберите правильный ответ и запишите аргументы.	Какой алгоритм является симметричным? 1) RSA; 2) AES; 3) ECDSA; 4) DSA.
Задание с выбором нескольких вариантов (Знать)	Прочитайте текст, выберите все правильные ответы и запишите обоснование.	Какие из перечисленных угроз относятся к веб-приложениям? 1) SQL-инъекция; 2) XSS; 3) DDoS; 4) CSRF.

Тип задания	Инструкция	Пример задания
Задание с выбором нескольких вариантов (Уметь)	Прочитайте текст, выберите все правильные ответы и запишите обоснование.	Какие меры помогут защитить данные в облаке? 1) Шифрование перед передачей; 2) Использование многофакторной аутентификации; 3) Открытый доступ ко всем данным; 4) Регулярное резервное копирование.
Задание комбинированное с выбором одного верного ответа и обоснованием (Знать)	Прочитайте текст, выберите правильный ответ и запишите развёрнутое обоснование.	Что такое принцип наименьших привилегий? 1) Каждый пользователь имеет минимальные права, необходимые для работы; 2) Все пользователи имеют одинаковые права; 3) Администратор имеет все права; 4) Права назначаются случайным образом.
Задание комбинированное с выбором одного верного ответа и обоснованием (Уметь)	Прочитайте текст, выберите правильный ответ и запишите развёрнутое обоснование.	Какой метод используется для защиты паролей в базе данных? 1) Хеширование; 2) Шифрование; 3) Компрессия; 4) Кодирование.
Задание комбинированное с выбором нескольких вариантов и обоснованием (Знать)	Прочитайте текст, выберите все правильные ответы и запишите развёрнутое обоснование.	Какие стандарты относятся к информационной безопасности? 1) ISO 27001; 2) GDPR; 3) IEEE 802.11; 4) PCI DSS.
Задание комбинированное с выбором нескольких вариантов и обоснованием (Уметь)	Прочитайте текст, выберите все правильные ответы и запишите развёрнутое обоснование.	Какие действия следует предпринять при обнаружении утечки данных? 1) Изолировать затронутые системы; 2) Сообщить руководству; 3) Удалить все логи; 4) Провести анализ инцидента.
Задание открытого типа с развёрнутым ответом (Знать)	Прочитайте текст и запишите развёрнутый обоснованный ответ.	Объясните разницу между симметричным и асимметричным

Тип задания	Инструкция	Пример задания
		шифрованием. Приведите примеры.
Задание открытого типа с развёрнутым ответом (Уметь)	Прочитайте текст и запишите развёрнутый обоснованный ответ.	Опишите процесс защиты веб-приложения от SQL-инъекций.
Задание открытого типа с развёрнутым ответом (Знать)	Прочитайте текст и запишите развёрнутый обоснованный ответ.	Что такое двухфакторная аутентификация и как она работает?
Задание открытого типа с развёрнутым ответом (Уметь)	Прочитайте текст и запишите развёрнутый обоснованный ответ.	Разработайте политику паролей для бизнес-приложения.
Практическое задание (Уметь)	Выполните задание и запишите результат.	Создайте хеш пароля с использованием алгоритма SHA-256 в Python.
Практическое задание (Уметь)	Выполните задание и запишите результат.	Настройте межсетевой экран (iptables) для блокировки входящего трафика с определённого IP.
Практическое задание (Уметь)	Выполните задание и запишите результат.	Проведите анализ логов на предмет подозрительной активности (задание по логам).
Практическое задание (Уметь)	Выполните задание и запишите результат.	Предложите план реагирования на инцидент для утечки персональных данных.