МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» ФИЛИАЛ В Г. ХАСАВЮРТЕ

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по программе подготовки специалистов среднего звена (ППССЗ) среднего профессионального образования

Специальность:	09.02.11 Разработка и управление программным обеспечением
Обучение:	по программе базовой подготовке
Уровень образования, на базе которого осваивается ППССЗ:	основное общее образование
Квалификация:	программист
Форма обучения:	очная

Хасавюрт 2026

Рабочая программа дисциплины ОП.05 Основы информационной безопасности разработана на основе требований Федерального государственного образовательного стандарта (далее - ФГОС) среднего профессионального образования (СПО) по специальности 09.02.11 Разработка и управление программным обеспечением от 24.02.2025 N 138, для реализации основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования.

Рабочая программа подготовлена на основе и с использованием учебно-методических материалов и учебников образовательной платформы «Юрайт»

Разработчики:

филиал федерального государственного бюджетного образовательного учреждения высшего образования «Дагестанский государственный университет» в г. Хасавюрте (Филиал ДГУ в г. Хасавюрте)

Алиева П.А - преподаватель кафедры гуманитарных и естественно-научных дисциплин

Рецензент:
Абдусаламов Р.А. – зав. кафедрой информационного права и информатики ФГБОУ ВО ДГУ, к.п.н., доцент.

Рабочая программа дисциплины рассмотрена и рекомендована к утверждению на заседании кафедры гуманитарных и естественно-научных дисциплин филиала ДГУ в г. Хасавюрте.

Протокол № 4 от «25. 12.» 2025 г.

Зав. кафедрой _____ Разаков Р.М.

Рабочая программа дисциплины согласована на заседании Учебно-методической комиссии филиала

Председатель УМК _____/Дадаев Д. Х./

«20» 01 2026 г.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОП.05 «Основы информационной безопасности»

1.1. Место дисциплины в структуре образовательной программы

Учебная дисциплина ОП.05 «Основы информационной безопасности» является обязательной частью общепрофессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

Дисциплина реализуется в традиционном формате, с использованием интерактивных форм проведения учебных занятий, в синхронном и асинхронном режиме на образовательной платформе ЮРАЙТ https://urait.ru/ .

1.2. Цель и планируемые результаты освоения дисциплины:

Содержание программы учебной дисциплины ОП.05 «Основы информационной безопасности» направлено на достижение следующей цели – освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации и информационной безопасности.

Результатом освоения программы является овладение обучающимися общими (ОК) и профессиональными (ПК) компетенциями, личностными результатами (ЛР):

Общие компетенции:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности;

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках

Профессиональные компетенции:

ПК 1.1. Проектировать базы данных.

ПК 1.4. Администрировать базы данных.

ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации.

ПК 3.1. Разрабатывать модули программного обеспечения для мобильных платформ.

ПК 3.2. Проектировать и разрабатывать пользовательский интерфейс и пользовательский опыт.

ПК 3.3. Проектировать и разрабатывать базы данных для мобильных платформ.

ПК 3.5. Выполнять тестирование и отладку программного обеспечения.

ПК 3.7. Осуществлять защиту данных в мобильных приложениях.

Личностные результаты:

ЛР 1. Осознающий себя гражданином России и защитником Отечества, выражающий свою российскую идентичность в поликультурном и многоконфессиональном российском обществе, и современном мировом сообществе. Сознающий свое единство с народом России, с Российским государством, демонстрирующий ответственность за развитие страны. Проявляющий готовность к защите

Родины, способный аргументированно отстаивать суверенитет и достоинство народа России, сохранять и защищать историческую правду о Российском государстве.

ЛР 2. Проявляющий активную гражданскую позицию на основе уважения закона и правопорядка, прав и свобод сограждан, уважения к историческому и культурному наследию России. Осознанно и деятельно выражающий неприятие дискриминации в обществе по социальным, национальным, религиозным признакам; экстремизма, терроризма, коррупции, антигосударственной деятельности. Обладающий опытом гражданской социально значимой деятельности (в студенческом самоуправлении, добровольчестве, экологических, природоохранных, военно-патриотических и др. объединениях, акциях, программах). Принимающий роль избирателя и участника общественных отношений, связанных с взаимодействием с народными избранниками.

ЛР 4. Проявляющий и демонстрирующий уважение к труду человека, осознающий ценность собственного труда и труда других людей. Экономически активный, ориентированный на осознанный выбор сферы профессиональной деятельности с учетом личных жизненных планов, потребностей своей семьи, российского общества. Выражающий осознанную готовность к получению профессионального образования, к непрерывному образованию в течение жизни Демонстрирующий позитивное отношение к регулированию трудовых отношений. Ориентированный на самообразование и профессиональную переподготовку в условиях смены технологического уклада и сопутствующих социальных перемен. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 6. Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации.

ЛР 7. Осознающий и деятельно выражающий приоритетную ценность каждой человеческой жизни, уважающий достоинство личности каждого человека, собственную и чужую уникальность, свободу мировоззренческого выбора, самоопределения. Проявляющий бережливое и чуткое отношение к религиозной принадлежности каждого человека, предупредительный в отношении выражения прав и законных интересов других людей.

ЛР 9. Сознающий ценность жизни, здоровья и безопасности. Соблюдающий и пропагандирующий здоровый образ жизни (здоровое питание, соблюдение гигиены, режим занятий и отдыха, физическая активность), демонстрирующий стремление к физическому совершенствованию. Проявляющий сознательное и обоснованное неприятие вредных привычек и опасных наклонностей (курение, употребление алкоголя, наркотиков, психоактивных веществ, азартных игр, любых форм зависимостей), деструктивного поведения в обществе, в том числе в цифровой среде.

ЛР 13. Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности.

ЛР 14. Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.

ЛР 15. Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем.

ЛР 16. Соответствующий ожиданиям работодателей: креативно мыслящий, эффективно сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, распределяющий время и другие ресурсы для выполнения поставленной задачи в установленный срок, ответственный, дисциплинированный, целеустремленный, стрессоустойчивый.

ЛР 17. Демонстрирующий культуру речи, в том числе в деловой переписке/переговорах, способный презентовать себя и продукт профессиональной деятельности.

ЛР 18. Демонстрирующий способность использовать в цифровой среде различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве.

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения должен:

уметь:

- 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)
- 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
- понимать тексты на базовые профессиональные темы
- шифровать данные и обеспечивать их конфиденциальность
- анализ требований безопасности информационных систем
- разрабатывать и реализовывать меры безопасности
- реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию

знать:

- 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
- 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.
- лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности
- принципы безопасности хранения данных
- методы защиты баз данных от внешних угроз
- принципы криптографии и методов шифрования данных
- стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.

- методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных
- законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.
- отраслевая нормативная техническая документация
- источники информации, необходимой для профессиональной деятельности
- современный отечественный и зарубежный опыт в профессиональной деятельности
- принципы и методы обеспечения безопасности информационных систем
- принципов безопасности информационных систем
- современных методов и технологий в области безопасности информационных систем
- законодательных и нормативных актов в области безопасности информационных систем
- источники угроз информационной безопасности и меры по их предотвращению
- основные угрозы безопасности мобильных приложений
- принципы криптографии и шифрования данных.
- стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect
- законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA
- основные принципы безопасности информации и методов ее защиты.
- стандартные криптографические алгоритмы для шифрования данных
- принципы обеспечения безопасности передачи данных по сети
- основы безопасности приложений и инфраструктуры
- методы анализа на уязвимости и мониторинга безопасности
- знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений
- понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения
- знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы

Владеть навыками:

- применение современных методов и технологий в области безопасности информационных систем
- использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные.
- применение механизмов хеширования для защиты паролей пользователей от несанкционированного доступа.
- обеспечение безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS
- 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 часов***

Максимальная учебная нагрузка (всего)	**108**
Обязательная аудиторная учебная нагрузка (всего)	64
в том числе:	
лекции	32
практические занятия	32
Самостоятельная работа обучающегося (всего)	39
Промежуточная аттестация в форме **экзамена** - *4 семестр*	9

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала лекций, лабораторные и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов	Формы и методы контроля и оценки результатов обучения
Тема 1. Введение в информационную безопасность	**Содержание учебного материала** **Лекция** Цели защиты. Слабые места и угрозы. Типы атак и атакующих. Инциденты информационной безопасности. Правила безопасности и многосторонняя безопасность. Новые угрозы.	**1**	
	Практическое занятие Задание 1, стр. 20 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/20	**2**	оценка навыка анализа и решения профессиональных задач
Тема 2. Угрозы.	**Содержание учебного материала** **Лекция** Вредоносное программное обеспечение. Переполнение буфера. Компьютерные вирусы. Черви. Троянский конь (троян). Ботнет. Спам. Мобильные приложения. Новые виды угроз: атаки Meltdown и Spectre.	**2**	
	Практическое занятие Задание 1, стр. 28 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/28	**2**	оценка навыка анализа и решения профессиональных задач
Тема 3. Проблемы	**Содержание учебного материала** **Лекция**	**2**	

безопасности интернет-протоколов.	Введение в проблему безопасности интернет-протоколов. Протокол IP. Протокол TCP. Проблемы безопасности IP. Маршрутизационные атаки. Проблемы безопасности ICMP. Проблемы безопасности ARP. Проблемы безопасности IPv6. Проблемы безопасности UDP и TCP. DNS. NFS. Электронная почта. File Transfer Protocol. Веб-приложения. Динамические веб-сайты. Куки. Проблемы безопасности HTML5.		
	Практическое занятие Задание 1, стр. 51 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/51	**2**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 57 — URL: https://urait.ru/bcode/567521/p.57 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/51	**2**	Устный/ письменный опрос Тестирование
Тема 4. Построение системы безопасности.	**Содержание учебного материала** **Лекция** Общие принципы создания IT-систем. Структурный анализ. Определение потребности в защите. Анализ угроз. Анализ рисков. Архитектура безопасности. Базовые функции безопасности. Жизненный цикл безопасной разработки (Security Development Lifecycle).	**2**	
	Практическое занятие Задание 1, стр. 60 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/60	**2**	оценка навыка анализа и решения профессиональных задач

	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 66 — URL: https://urait.ru/bcode/567521/p.66 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/60	**2**	Устный/ письменный опрос Тестирование
Тема 5. Критерии оценки.	**Содержание учебного материала** **Лекция** Введение в проблематику. TCSEC — Trusted Computer System Evaluation Criteria. ITSEC — Information Technology Security Evaluation Criteria. Common Criteria for Information Technology Security Evaluation.	**2**	
	Практическое занятие Задание 1, стр. 67 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/67	**2**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 72 — URL: https://urait.ru/bcode/567521/p.72 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/67	**2**	Устный/ письменный опрос Тестирование
Тема 6. Модели безопасности.	**Содержание учебного материала** **Лекция** Введение в проблематику. Матричная модель доступа. Модели, основанные на ролях.	**2**	

	Модель «Китайская стена». Модель Белла — Лападулы.		
	Практическое занятие Задание 1-6, стр. 80 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/80	**2**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 86 — URL: https://urait.ru/bcode/567521/p.86 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/80	**2**	Устный/ письменный опрос Тестирование
Тема 7. Технологии работы с ключами.	**Содержание учебного материала** **Лекция** Введение в проблематику. Создание ключей. Техники создания ключей. Хранение и уничтожение ключей. Обмен ключами. Иерархия ключей. Наивный протокол обмена ключами. Симметричные алгоритмы обмена ключами. Асимметричные протоколы обмена ключами. Принципы разработки протоколов обмена ключами. Восстановление ключей.	**2**	
	Практическое занятие Задание 1, стр. 92 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/92	**2**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). —	**2**	Устный/ письменный опрос Тестирование

	ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 97 — URL: https://urait.ru/bcode/567521/p.97 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/92		
Тема 8. Аутентификация на основе знания.	**Содержание учебного материала** **Лекция** Введение в проблематику. Создание ключей. Техники создания ключей. Хранение и уничтожение ключей. Обмен ключами. Иерархия ключей. Наивный протокол обмена ключами. Симметричные алгоритмы обмена ключами. Асимметричные протоколы обмена ключами. Принципы разработки протоколов обмена ключами. Восстановление ключей.	**2**	
	Практическое занятие Задание 1, стр. 99 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/99	**2**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 105 — URL: https://urait.ru/bcode/567521/p.105 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/99	**2**	Устный/ письменный опрос Тестирование
Тема 9. Аутентификация на основе обладания предметом.	**Содержание учебного материала** **Лекция** Смарт-карты. Универсальная аутентификация по двум факторам. Trusted Computing. Физически неклонируемые функции.	**2**	
	Практическое занятие Задание 1, стр. 110 https://urait.ru/viewer/informacionnaya-	**2**	оценка навыка анализа и решения профессиональных

	bezopasnost-567521#page/110		задач
Тема 10. Биометрическая аутентификация.	**Содержание учебного материала** **Лекция** Общие сведения о биометрических технологиях. Особенности процесса биометрической аутентификации.	**2**	
	Практическое занятие Задание 1, стр. 115 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/115	**2**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 120 — URL: https://urait.ru/bcode/567521/p.120 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/115	**2**	Устный/ письменный опрос Тестирование
Тема 11. Основы криптографической защиты информации.	**Содержание учебного материала** **Лекция 1** Введение в проблематику. Шифр Цезаря. Шифр перестановки. Шифр перестановки «сцитала». Диск и линейка Энея. Квадрат Полибия. Тюремный шифр. Магические квадраты. Шифр Аве Мария	**2**	
	Лекция 2 Таблица Тритемия. Шифр Бэкона. Шифр Порты. Шифр Кардано. Шифр Ришелье. Симметричное и асимметричное шифрование. Безопасность методов шифрования.	**2**	
	Практическое занятие Задание 1-14, стр. 141 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/141	**2**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В.	**3**	Устный/ письменный опрос

	Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 147 — URL: https://urait.ru/bcode/567521/p.147 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/141		Тестирование
Тема 12. Современные криптографические алгоритмы.	**Содержание учебного материала** **Лекция** Блочные шифры. Режимы шифрования. Поточные шифры. Понятие и свойства идеального шифра. Асимметричные шифры. RSA-алгоритм. Шифр Рабина. Обмен ключами Диффи — Хеллмана. Алгоритм Эль-Гамаля.	**2**	
	Практическое занятие Задание 1-3, стр. 158 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/158	**1**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 164 — URL: https://urait.ru/bcode/567521/p.164 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/158	**3**	Устный/ письменный опрос Тестирование
Тема 13. Электронная цифровая подпись.	**Содержание учебного материала** **Лекция** Общие сведения об электронной цифровой подписи. Одноразовая подпись Лемпорта — Диффи. Подпись RSA. Подпись Эль-Гамаля.	**2**	
	Практическое занятие Задание 1-3, стр. 163 https://urait.ru/viewer/informacionnaya-	**1**	оценка навыка анализа и решения профессиональных

	bezopasnost-567521#page/163		задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 168 — URL: https://urait.ru/bcode/567521/p.168 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/163	**4**	Устный/ письменный опрос Тестирование
Тема 14. Безопасность сетей.	**Содержание учебного материала** **Лекция** Технология межсетевого экрана (брандмауэра, файрвола). Пакетные фильтры. Прокси межсетевые экраны. Фильтры приложений. Варианты архитектуры, использующей межсетевые экраны. Протоколы безопасной коммуникации. Виртуальная частная сеть. IPSec. Протокол TLS/SSL. DNSSEC. Электронная почта. PGP.	**2**	
	Практическое занятие Задание 1, стр. 192 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/192	**2**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 198 — URL: https://urait.ru/bcode/567521/p.198 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/192	**2**	Устный/ письменный опрос Тестирование

Тема 15. Безопасность мобильной и беспроводной связи.	**Содержание учебного материала** **Лекция** GSM. GPRS. UMTS. LTE и SAE. 5G и будущее сотовой связи. WLAN. Bluetooth. ZigBee.	**2**	
	Практическое занятие Задание 1, стр. 212 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/212	**2**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 218 — URL: https://urait.ru/bcode/567521/p.218 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/212	**4**	Устный/ письменный опрос Тестирование
Тема 16. Правовые основы информационной безопасности.	**Содержание учебного материала** **Лекция** Введение в проблематику. Конституция РФ. Федеральный закон «О персональных данных». Федеральный закон «Об информации, информационных технологиях и о защите информации». Федеральный закон «Об электронной подписи». Федеральный закон «О безопасности критической информационной инфраструктуры РФ». Указы Президента Российской Федерации. Постановления Правительства РФ. Приказы ФСБ и ФСТЭК. Приказы Минцифры.	**1**	
	Практическое занятие Задание 1, стр. 235 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/235	**2**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования /	**4**	Устный/ письменный опрос Тестирование

	А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 241 — URL: https://urait.ru/bcode/567521/p.241 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/235		
Тема 17. Управление IT-проектом как эффективный способ организации действий по повышению уровня информационной безопасности.	**Содержание учебного материала** **Лекция** Введение в проблематику. Понятие проекта. Виды и фазы проектов. Управление проектами как специфический вид менеджмента. Типичные проблемы реализации проектов. Проект от определения до завершения.	**1**	
	Практическое занятие Задание 1, стр. 242 https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/242	**2**	оценка навыка анализа и решения профессиональных задач
	Самостоятельная работа **Изучение основной и дополнительной литературы:** Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 248 — URL: https://urait.ru/bcode/567521/p.248 **Интерактивные формирующие тесты:** https://urait.ru/viewer/informacionnaya-bezopasnost-567521#page/242	**4**	Устный/ письменный опрос Тестирование
	Патт	**9**	
	ИТОГО	**108**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Для проведения учебных занятий используются, оборудованные техническими средствами кабинеты и лаборатории. Реализация программы дисциплины «Основы

информационной безопасности» осуществляется в учебном кабинете нормативного правового обеспечения информационной безопасности, в котором есть возможность проводить занятия, групповые и индивидуальные консультации, текущий контроль и промежуточную аттестацию, как в традиционной форме, так и с использованием интерактивных технологий и различных образовательных методик. Имеются также учебные аудитории для самостоятельной работы, кабинеты для проведения практических занятий, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования ФГОС СПО.

Оборудование учебного кабинета: компьютер либо ноутбук с предустановленным стандартным программным обеспечением (по количеству обучающихся), широкополосный доступ в сеть Интернет. Используется либо свободно распространяемое программное обеспечение, либо поставляемое по лицензии образовательной организации; посадочные места по количеству обучающихся; рабочее место преподавателя; комплект учебно-наглядных пособий.

Технические средства обучения: для отображения презентаций используется проектор, стационарный или переносной экран либо интерактивная доска. В филиале созданы все условия, позволяющие широко использовать в образовательном процессе информационные технологии, своевременно обеспечивать обновление нормативной документации, необходимой информации и оперативный доступ к ней. Установлены лицензионные программы, справочно-правовая система «КонсультантПлюс»

Учебники и учебные пособия по дисциплине «Основы информационной безопасности» находятся в свободном доступе для преподавателей и студентов в библиотеке филиала ДГУ, в том числе электронные издания на официальном сайте филиала ДГУ. Библиотека филиала оборудована рабочими местами в читальном зале и выходом в Интернет для работы с электронными книгами, учебниками, учебными пособиями, размещёнными на сайте филиала ДГУ.

При проведении синхронных и асинхронных занятий используется электронная образовательная платформа «Юрайт» и электронные образовательные ресурсы Научной библиотеки ДГУ.

Доступ к контенту и сервисам на образовательной платформе «Юрайт» и электронном ресурсе цифровой образовательной среды СПО PROFобразование предоставляется в соответствии с условиями подписки учебного заведения. Пароль и логин к личному кабинету студент указывает при регистрации на образовательной платформе.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература

1. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 1 — URL: https://urait.ru/bcode/567521/p.1

Дополнительная литература

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст :

электронный // Образовательная платформа Юрайт [сайт]. с. 1 — URL: https://urait.ru/bcode/567283/p.1

3. Нетесова, О. Ю. Информационные системы в экономике : учебник для среднего профессионального образования / О. Ю. Нетесова. — 5-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 152 с. — (Профессиональное образование). — ISBN 978-5-534-20212-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 1 — URL: https://urait.ru/bcode/562512/p.1

Интернет-ресурсы:

1. Образовательная платформа Юрайт - urait.ru
2. Образовательная платформа СПО PROFобразование https://profspo.ru/
3. Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения обо всех видах литературы, поступающих в фонд НБ ДГУ / Дагестанский государственный университет. – Махачкала, 2010. – Режим доступа: http://elib.dgu.ru , свободный
4. Электронно-библиотечная система «Университетская библиотека онлайн». - URL: www.biblioclub.ru
5. Научная электронная библиотека eLIBRARY.RU. - URL: http://elibrary.ru
6. Справочно-правовая система «КонсультантПлюс». - URL: http://www.consultant.ru

3.3. Образовательные технологии

Учебная деятельность обучающихся по дисциплине предусматривает учебные занятия (практическое занятие, лекция), самостоятельную работу, а также другие виды учебной деятельности.

В учебной деятельности по дисциплине используются различные образовательные технологии, в том числе:

синхронные занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана. На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс. Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

В смешанном обучении с применением дистанционных образовательных технологий студенты могут изучать лекционный материал в асинхронном режиме, готовить вопросы к занятиям семинарского типа.

Синхронные занятия семинарского (практического) типа

Занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса. Активность на занятиях оценивается по следующим критериям:

ответы на вопросы, предлагаемые преподавателем;

участие в дискуссиях;

выполнение разноуровневых заданий (задач).

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.
В синхронном и асинхронном режиме используется сервис «Юрайт.Задания».

Асинхронные дистанционные занятия

В смешанном обучении с применением дистанционных образовательных технологий студенты могут осваивать лекционный материал в асинхронном режиме, готовить вопросы к синхронным семинарским (практическим) занятиям.
Для асинхронных занятий применяется следующая методика:
повторение и закрепление предыдущей темы (раздела);
изучение базовой и дополнительной рекомендуемой литературы, просмотр (прослушивание) медиаматериалов к новой теме (разделу);
тезисное конспектирование ключевых положений, терминологии, алгоритмов;
самостоятельная проверка освоения материала через интерактивный фонд оценочных средств (тесты);
выполнение рекомендуемых заданий;
фиксация возникающих вопросов и затруднений.

4. Контроль и оценка результатов освоения дисциплины

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований и др.

Результаты (основные умения, освоенные профессиональные компетенции)	**Коды формируемых профессиональных и общих компетенций**	**Формы и методы контроля и оценки результатов обучения**
уметь: 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) определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне	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, ЛР1, ЛР 2, ЛР 4, ЛР 6, ЛР 7, ЛР 9, ЛР 13–18	Текущий контроль: - устный (письменный) опрос; Тестирование; оценка навыка анализа и решения профессиональных задач, самостоятельная работа.

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 понимать тексты на базовые профессиональные темы шифровать данные и обеспечивать их конфиденциальность анализ требований безопасности информационных систем разрабатывать и реализовывать меры безопасности реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию **знать:** 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 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.		

лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности принципы безопасности хранения данных методы защиты баз данных от внешних угроз принципы криптографии и методов шифрования данных стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др. методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др. отраслевая нормативная техническая документация источники информации, необходимой для профессиональной деятельности современный отечественный и зарубежный опыт в профессиональной деятельности принципы и методы обеспечения безопасности информационных систем принципов безопасности информационных систем современных методов и технологий в области безопасности информационных систем законодательных и нормативных актов в области безопасности информационных систем источники угроз информационной безопасности и меры по их предотвращению основные угрозы безопасности мобильных приложений принципы криптографии и шифрования данных. стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect законодательные и регуляторные требования к защите данных,		

включая GDPR и HIPAA основные принципы безопасности информации и методов ее защиты. стандартные криптографические алгоритмы для шифрования данных принципы обеспечения безопасности передачи данных по сети основы безопасности приложений и инфраструктуры методы анализа на уязвимости и мониторинга безопасности знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы **Владеть навыками:** применение современных методов и технологий в области безопасности информационных систем использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные. применение механизмов хеширования для защиты паролей пользователей от несанкционированного доступа. обеспечение безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS соблюдение законодательства и регуляций в области защиты данных		
Форма контроля: может проводиться в форме тестирования, в письменной, а также в устной		

форме.
Экзаменационные билеты по дисциплине могут включать теоретические вопросы, тестовые задания, разно-уровневые задания (задачи).