

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Минцаев Магомед Шаралович

Должность: Ректор

Дата подписания: 30.01.2026 15:34:40

Уникальный программный ключ:

236bcc35c296f119d6aafdc22836b21db52dbc07971a86865a5825f9fa4304cc

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Грозненский государственный нефтяной технический университет
имени академика М.Д. Миллионщикова**



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 «Основы информационной безопасности»

Специальность

09.02.11 Разработка и управление программным обеспечением

Квалификация

Программист

Грозный – 2026 г.

СОДЕРЖАНИЕ ПРОГРАММЫ

1. Общая характеристика 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.....	4
2.1. Трудоемкость освоения дисциплины	4
2.2. Содержание дисциплины	6
3. Условия реализации ДИСЦИПЛИНЫ	8
3.1. Материально-техническое обеспечение	8
3.2. Учебно-методическое обеспечение	<i>Ошибка! Закладка не определена.</i>
4. Контроль и оценка результатов освоения ДИСЦИПЛИНЫ....	<i>Ошибка! Закладка не определена.</i>

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«Основы информационной безопасности» (наименование дисциплины)

1.1. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины «ОП.05 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 «ОП.05 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 ОПОП-П).

В результате освоения дисциплины обучающийся должен:

Код ОК	Уметь	Знать	Владеть
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, планировать процесс поиска, выбирать необходимые источники информации выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска оценивать практическую значимость результатов поиска применять средства информационных технологий для решения профессиональных задач использовать современное программное обеспечение в профессиональной деятельности 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 цифровые средства	
ОК.09	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы участвовать в диалогах на знакомые общие и профессиональные темы строить простые высказывания о себе и о своей профессиональной деятельности кратко обосновывать и объяснять свои действия (текущие и планируемые) писать простые связные сообщения на знакомые или интересующие профессиональные темы	правила построения простых и сложных предложений на профессиональные темы основные общеупотребительные глаголы (бытовая и профессиональная лексика) лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности особенности произношения правила чтения текстов профессиональной направленности	
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 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.	
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 современных методов и технологий в области безопасности	применение современных методов и технологий в области безопасности информационных систем

		информационных систем законодательных и нормативных актов 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 реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию	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	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

		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	
--	--	---	--

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	12	6
<i>Курсовая работа (проект)</i>	-	-
Самостоятельная работа	64	-
Промежуточная аттестация в <i>форме (экзамен)</i>	10	-
Всего	86	6

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Коды компетенций, формирование которых способствует элемент программы
1	2	3	4
Раздел 1. Основы информационной безопасности		12/ 6	
Тема 1.1. Введение в информационную безопасность	Содержание	4	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 ПК 3.9
	Основные понятия и определения. История и развитие информационной безопасности.	2	
	В том числе практических занятий	2	
	Актуальные угрозы и риски в информационной безопасности	2	
	Самостоятельная работа обучающихся 1. Триада CIA (конфиденциальность, целостность, доступность): примеры нарушений и методы защиты. 2. Уровни обеспечения ИБ: законодательный, административный, процедурный, технический. 3. Классификация угроз ИБ: естественные vs искусственные, внутренние vs внешние. 4. Модели нарушителя: типовые мотивы, компетенции, сценарии действий. 5. Принципы защиты информации: минимизация привилегий, разделение обязанностей, «защита в глубину». 6. ФЗ-152 «О персональных данных»: требования к операторам, меры защиты, ответственность. 7. ФЗ-187 «О безопасности КИИ»: категории объектов, требования к защите. 8. ГОСТ Р 57580.1-2017: уровни зрелости ИБ в финансовых организациях. 9. Международные стандарты ISO/IEC 27001–27005: структура, ключевые требования. 10. Ответственность за компьютерные преступления (ст. 272–274 УК РФ): анализ судебной практики. 11. Методика оценки рисков ИБ: CRAMM, OCTAVE, NIST SP 800-30.	22	
Тема 1.2.	Содержание	4	

Управление безопасностью информации	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими.	2	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 ПК 3.9
	В том числе практических занятий	2	
	Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	2	
	Самостоятельная работа обучающихся 1. Аудит информационной безопасности: чек-листы, методы сбора доказательств. 2. План реагирования на инциденты (IRP): структура, этапы, роли. 3. Business Impact Analysis (BIA): оценка критичности процессов и данных. 4. Страхование киберрисков: виды полисов, условия возмещения ущерба. 5. Симметричные алгоритмы (AES, ГОСТ Р 34.12-2015): принципы, области применения. 6. Асимметричные алгоритмы (RSA, ECC): ключевые длины, сценарии использования. 7. Электронная подпись: ГОСТ Р 34.10-2021, форматы CAdES/XAdES. 8. Хэш-функции (SHA-256, ГОСТ Р 34.11-2012): коллизии, применение в блокчейне. 9. PKI: структура УЦ, жизненный цикл сертификата, OCSP/CRL. 10. Межсетевые экраны (NGFW): правила фильтрации, IDS/IPS, анализ логов. 11. VPN-технологии (IPsec, OpenVPN, WireGuard): схемы развёртывания, ключи.	22	
Тема 1.3 Криптография	Содержание	4	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 ПК 3.9
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	2	
	В том числе практических занятий	2	
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	2	
	Самостоятельная работа обучающихся 1. Защита Wi-Fi: WPA3, 802.1X, изоляция гостевых сетей. 2. DNS-безопасность: DNSSEC, защита от спуфинга, DoH/DoT. 3. Сегментация сети: VLAN, микросегментация, Zero Trust. 4. Антивирусные решения: эвристика, песочницы, EDR-системы. 5. Обновление ПО и управление уязвимостями: patch management, CVSS. 6. Защищённые конфигурации ОС (Windows, Linux): шаблоны, автоматизация. 7. Контроль приложений (AppLocker, SELinux): белые списки, политики выполнения. 8. Шифрование дисков (BitLocker, LUKS): ключи восстановления, TPM. 9. Уязвимости веб-приложений (OWASP Top 10): SQL-инъекции, XSS, CSRF. 10. SAST/DAST-анализ кода: инструменты, интерпретация результатов.	20	
Промежуточная аттестация		10	
Всего:		86	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Кабинет «Компьютерных сетей и основ информационной безопасности», оснащенный в соответствии с приложением 3 ОПОП-П.

Лаборатория «_» оснащенная в соответствии с приложением 3 ОПОП-П.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные или электронные издания

1. Башмакова, Е. И. Информатика и информационные технологии. Умный Excel 2016: библиотека функций : учебное пособие / Е. И. Башмакова. — Москва : Ай Пи Ар Медиа, 2020. — 109 с. — ISBN 978-5-4497-0516-7. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование : [сайт]. — URL: <https://profspo.ru/books/94205>

2. Гагарина Л.Г., Теплова Я.О., Румянцева Е.Л., Баин А.М. Информационные технологии: учебное пособие под ред. Л.Г. Гагариной. – М.: ФОРУМ: ИНФРА-М, 2019. – 320 с. (Профессиональное образование). – ISBN 978-5-8199-0608-8. – Текст: электронный. – URL: <https://znanium.com/catalog/product/1018534>

3. Цветкова, А. В. Информатика и информационные технологии: учебное пособие для СПО / А. В. Цветкова. — Саратов : Научная книга, 2019. — 190 с. — ISBN 978-5-9758-1891-1. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование : [сайт]. — URL: <https://profspo.ru/books/87074>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоённости компетенций	Методы оценки
Знает - 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 - номенклатуру информационных источников, применяемых в профессиональной деятельности; - приемы структурирования информации; - формат оформления результатов поиска информации, современные средства и устройства информатизации; - порядок применения современных средств и устройств информатизации 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;	Демонстрирует Ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить; Владеет основными источниками информации и ресурсами для решения задач и проблем в профессиональном и/или социальном контексте; Знает алгоритмы выполнения работ в профессиональной и смежных областях; Знает методы работы в профессиональной и смежных сферах; Знает структуру плана для решения задач; Может произвести оценку результатов решения задач профессиональной деятельности Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности; Знает приемы структурирования информации; Знает формат оформления результатов поиска информации, современные	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

- 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.; - отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; - современный отечественный и зарубежный опыт в профессиональной деятельности; - принципы и методы обеспечения безопасности информационных систем; - принципы безопасности информационных систем; - современные методы и технологии в области безопасности информационных систем; - законодательные и нормативные акты в области безопасности информационных систем; -источники угроз информационной безопасности и меры по их предотвращению; - основные угрозы безопасности мобильных приложений; - принципы криптографии и шифрования данных;	средства и устройства информатизации; Может применять современные средства и устройства информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; Владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности; Знает принципы безопасности хранения данных; Владеет методами защиты баз данных от внешних угроз Знает принципы криптографии и методов шифрования данных; Ориентируется в стандартах и протоколах безопасности, таких как SSL/TLS, SSH, Kerberos и др.; 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.;	
---	--	--

- 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.	Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; Знает современный отечественный и зарубежный опыт в профессиональной деятельности; Владеет принципами и методами обеспечения безопасности информационных систем; Знает принципы безопасности информационных систем; Владеет современными методами и технологиями в области безопасности информационных систем; Знает законодательные и нормативные акты в области безопасности информационных систем; Знает источники угроз информационной безопасности и меры по их предотвращению; Имеет представление об основных угрозах безопасности мобильных приложений; Ориентируется в принципах криптографии и шифрования данных; Знает стандарты и протоколы безопасности, такие как	
---	--	--

	HTTPS, OAuth и OpenID Connect; Знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; Владеет основными принципами безопасности информации и методов ее защиты; Знает стандартные криптографические алгоритмы для шифрования данных; Имеет представление о принципах обеспечения безопасности передачи данных по сети; Знает основы безопасности приложений и инфраструктуры; Знает методы анализа на уязвимости и мониторинга безопасности; Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений; Понимает различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения; Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как	
--	--	--

	брандмауэры, системы обнаружения вторжений и антивирусные программы. Может распознавать задачу и/или проблему в профессиональном и/или социальном контексте; Анализирует задачу и/или проблему и может выделить её составные части; Умеет определять этапы решения задачи; Может выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; Составляет план действия; Может определять необходимые ресурсы; Владеет актуальными методами работы в профессиональной и смежных сферах; Может реализовывать составленный план; Оценивает результат и последствия своих действий (самостоятельно или с помощью наставника); Умеет определять задачи для поиска информации;	
--	--	--

	Умеет определять необходимые источники информации; Планирует процесс поиска; Умеет структурировать получаемую информацию; Может выделить наиболее значимое в перечне информации; Умеет оценивать практическую значимость результатов поиска; Оформляет результаты поиска и применяет средства информационных технологий для решения профессиональных задач; Может использовать современное программное обеспечение; Может использовать различные цифровые средства для решения профессиональных задач; Понимает тексты на базовые профессиональные темы; Умеет шифровать данные и обеспечивать их конфиденциальность; Умеет анализировать требования безопасности информационных систем; Может разрабатывать и реализовывать меры безопасности;	
--	---	--

	Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	
Умеет: -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	использует рациональные методы и средства обработки информации	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

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

Разработчик:

Преподаватель ФСПО

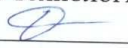


(подпись)

/А.А. Базаева/

Согласовано:

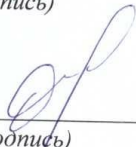
Председатель ПЦК «Информационные технологии»



(подпись)

/И.М. Дубаев/

1-й зам.-зам. декана по УМР ФСПО



(подпись)

/М.И. Дагаев/

Директор ДУМР



/М.А. Магомаева /