Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Северо-Кавказский федеральный университет»

Колледж СКФУ в г. Ставрополе

УТВЕРЖДАЮ

и.о. директора института перспективной инженерии, канд. тех. наук,
доцент Порохня А.А.

Рабочая программа учебной дисциплины

ОП.05 Основы информационной безопасности

Специальность 09.02.11 Разработка и управление программным обеспечением

Форма обучения очная

2026

Рабочая программа учебной дисциплины ОП.05 Основы информационной безопасности разработана на основании федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением, утвержденного приказом Минобрнауки России от 24.02.2025 № 138, и примерной основной образовательной программы СПО, с учетом направленности на удовлетворение потребностей регионального рынка труда и работодателей.

Рабочая программа учебной дисциплины разработана:
Масаловой Л.С., преподавателем колледжа СКФУ в г. Ставрополе

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 Основы информационной безопасности

1.1 Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина «Основы информационной безопасности» является обязательной частью общепрофессионального цикла примерной образовательной программы в соответствии с ФГОС СПО по специальности.

Особое значение дисциплина имеет при формировании и развитии ОК 01; ОК 02; ОК 03; ОК 04; ПК 1.5; ПК 2.4; ПК 3.8.

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ПК, ОК	Умения	Знания
ОК 01	- распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; - определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; - составлять план действия; определять необходимые ресурсы; - владеть актуальными методами работы в профессиональной и смежных сферах; - реализовывать составленный план; - оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	- актуальный профессиональный и социальный контекст, в котором приходится работать и жить; - основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; - алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; - структуру плана для решения задач; - порядок оценки результатов решения задач профессиональной деятельности
ОК 02	- определять задачи для поиска информации; - определять 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;	- номенклатуру 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

	- использовать различные цифровые средства для решения профессиональных задач	
ОК 03	планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности
ОК 04	эффективно взаимодействовать и работать в коллективе и команде	основы проектной деятельности
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 2.4	выполнять тестирование и отладку программного обеспечения	отраслевую нормативную техническую документацию, источники информации, необходимой для профессиональной деятельности
ПК 3.8	- производить оценку информационной системы для выявления возможности ее модернизации; - использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные;	- 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;

	- применять механизмы хеширования для защиты паролей пользователей от несанкционированного доступа; - обеспечивать безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS; - соблюдать законодательства и регуляции в области защиты данных	- 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; - основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения; - инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы

2. Структура и содержание учебной дисциплины

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Максимальная учебная нагрузка (всего)	**135**
в том числе:	
лекционные занятия	52
практические занятия	76
Самостоятельная работа	7
Промежуточная аттестация: *экзамен*	

2.2. Тематический план и 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, формированию которых способствует элемент программы
Введение	**Содержание учебного материала**	**2**	
	Понятия информационной безопасности, основы информационной безопасности.		ОК 01; ОК 02; ОК 03; ОК 04; ПК 1.5; ПК 2.4; ПК 3.8.
Раздел 1 Основы информационной безопасности		**8**	
Тема 1.1: Введение в информационную безопасность	**Содержание учебного материала**	2	
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности		
	в том числе:		
	практические занятия	6	
Раздел 2 Основы и принципы работы сетевой безопасности		**93**	ОК 01; ОК 02; ОК 03; ОК 04; ПК 1.5; ПК 2.4; ПК 3.8.
Тема 2.1 Управление безопасностью информации	**Содержание учебного материала**	6	
	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:		
	практические занятия	8	
Тема 2.2. Криптография	**Содержание учебного материала**	6	
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография		
	в том числе:		
	практические занятия	6	
	Содержание учебного материала		

Тема 2.3. Защита сетевой инфраструктуры	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.). Использование VPN и межсетевых экранов	6	
	в том числе:		
	практические занятия	12	
Тема 2.4. Безопасность приложений	**Содержание учебного материала**	6	
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей		
	в том числе:		
	практические занятия	12	
Тема 2.5. Защита данных	**Содержание учебного материала**	10	
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным		
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения		
	Организация защиты от атак		
	Организация работы VPN и межсетевого экрана		
	Тестирование на проникновение и анализ уязвимостей		
	в том числе:		
	практические занятия	6	
Тема 2.6. Безопасность облачных технологий	**Содержание учебного материала**	2	
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности		
	в том числе:		
	практические занятия	6	
	Самостоятельная работа обучающихся Написать реферат на тему: Выполнение резервного копирования и восстановления данных. Управление доступом к данным	7	
Раздел 3. Политика информационной безопасности		**32**	

Тема 3.1. Инциденты безопасности	**Содержание учебного материала**	4	ОК 01; ОК 02; ОК 03; ОК 04; ПК 1.5; ПК 2.4; ПК 3.8.
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика		
	Работа с инцидентами		
Тема 3.2. Социальная инженерия и человеческий фактор	**Содержание учебного материала**	4	
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности		
	В том числе:		
	практические занятия	10	
Тема 3.3. Будущее информационной безопасности	**Содержание учебного материала**	4	
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности		
	В том числе:		
	практические занятия	10	
Промежуточная аттестация (экзамен)			
Всего:		**135**	

3.УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;

Мультимедийное оборудование:

- ПК;
- принтер;
- сканер;
- проектор;
- модем;
- колонки.

3.2. Информационное обеспечение реализации программы

3.2.1. Основные электронные издания

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

2. Баланов А.Н. Комплексная информационная безопасность: учебное пособие для СПО А.Н. Баланов. - Санкт-Петербург: Лань, 2024. - 284 с. - ISBN 978-5-507-49251-0. - Текст: электронный // Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/414950 (дата обращения: 16.11.2024).

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

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

3.2.3. Дополнительные источники

1. www.edu.ru – Федеральный образовательный портал «Российское образование». Форма доступа:

2. http://iit.metodist.ru – Информатика и информационные технологии: сайт лаборатории информатики МИОО

3. http://www.intuit.ru – Интернет-университет информационных технологий (ИНТУИТ.ру)

4. http://www.osp.ru – Открытые системы: издания по информационным технологиям

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляются преподавателем в процессе проведения занятий, а также выполнения обучающимися индивидуальных заданий.

Результаты обучения	Показатели освоенности компетенций	Методы оценки
- 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;	- 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 средства и устройства информатизации; - может применять современные средства и устройства информатизации и программное обеспечение в	Экспертное наблюдение выполнения практических работ и видов работ по практике. Диагностика (тестирование, контрольная работа). *Промежуточный контроль:* экзамен (устный опрос, выполнение практического задания)

- 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; - 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 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.; - 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	

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; - 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	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;	

алгоритмы для шифрования данных; - принципы обеспечения безопасности передачи данных по сети; - основы безопасности приложений и инфраструктуры; - методы анализа на уязвимости и мониторинга безопасности; - основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения; - инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы. ***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;	- 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;	

- 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	- 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,	

программное обеспечение; - использовать различные цифровые средства для решения профессиональных задач; - понимать тексты на базовые профессиональные темы; - шифровать данные и обеспечивать их конфиденциальность; - анализировать требования безопасности информационных систем; - разрабатывать и реализовывать меры безопасности; - реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	сессионные токены и двухфакторную аутентификацию	