Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Северо-Кавказский федеральный университет»
Пятигорский институт (филиал) СКФУ
Колледж Пятигорского института (филиал) СКФУ

УТВЕРЖДАЮ
И.О. директора Пятигорского института (филиал) СКФУ
В.А. Фурсов

Рабочая программа учебной дисциплины

ОП.05 Основы информационной безопасности
индекс и наименование учебной дисциплины, согласно учебного плана

Специальность 09.02.11 Разработка и управление программным обеспечением
код наименование специальности

Форма обучения очная
очная, заочная, очно-заочная

2026 год

Рабочая программа учебной дисциплины разработана на основании федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением и примерной основной образовательной программы СПО, с учетом направленности на удовлетворение потребностей регионального рынка труда и работодателей.

1 Скворцов А.А., преподаватель колледжа Пятигорского института (филиал) СКФУ

фамилия, имя, отчество, ученая степень, ученое звание, место работы преподавателя

2

фамилия, имя, отчество, ученая степень, ученое звание, место работы преподавателя

3

фамилия, имя, отчество, ученая степень, ученое звание, место работы преподавателя

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы информационной безопасности

(наименование дисциплины)

1.1 Место дисциплины в структуре основной образовательной программы:

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

Особое значение дисциплина имеет при формировании и развитии 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.

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	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.

	технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач	
ОК.09	понимать тексты на базовые профессиональные темы	лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности
ПК 1.1	-	принципы безопасности хранения данных
ПК 1.4	-	методы защиты баз данных от внешних угроз
ПК 1.5	шифровать данные и обеспечивать их конфиденциальность	принципы криптографии и методов шифрования данных 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 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 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 УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы учебной дисциплины	**60**
в т.ч. в форме практической подготовки	**18**
в т.ч.:	
лабораторные работы	**12**
практические работы	**12**
Самостоятельные работы	**12**
Промежуточная аттестация	**12**

2.2. Тематический план и содержание учебной 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
1	*2*	*3*	*4*
Раздел 1. Основы информационной безопасности		48/18	
Тема 1.1. Введение в информационную безопасность	**Содержание учебного материала**	***4***	ОК 01 ОК 02 ОК 09 ПК 3.5
	1.Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	***2***	
	в том числе:		
	практические работы		
	Понятия информационной безопасности. Угрозы информационной безопасности.	***2***	
	лабораторная работа	***-***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся Анализ нормативно-правовой базы в области информационной безопасности	***2***	
Тема 1.2. Управление безопасностью информации	**Содержание учебного материала**	***4***	ОК 01 ОК 02 ОК 09 ПК 3.7
	1. Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	***2***	
	в том числе:		
	лабораторные работы		
	Информационная безопасность. Моделирование угроз	***2***	
	практические занятия	***-***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся		
Тема 1.3.	**Содержание учебного материала**	***4***	ОК 01 ОК 02

Криптография	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	***2***	ОК 09 ПК 3.1
	в том числе:		
	лабораторные работы		
	практические занятия	***-***	
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	***2***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся Сравнительный анализ симметричных и асимметричных алгоритмов шифрования	***2***	
Тема 1.4. Защита сетевой инфраструктуры	**Содержание учебного материала**	***4***	ОК 01 ОК 02 ОК 09 ПК 3.3
	1. Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	***2***	
	в том числе:		
	лабораторные работы		
	Правовые и нормативные основы информационной безопасности	***2***	
	практические занятия	***-***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся Моделирование угроз информационной безопасности для веб-приложения	***2***	
Тема 1.5. Безопасность приложений	**Содержание учебного материала**	***4***	ОК 01 ОК 02 ОК 09 ПК 3.3
	1. Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	***2***	
	в том числе:		
	лабораторные работы		
	практические занятия	***-***	
	Тестирование на проникновение и анализ уязвимостей.	***2***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся	***-***	
Тема 1.6. Защита	**Содержание учебного материала**	***4***	ОК 01 ОК 02

данных	1. Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным	***2***	ОК 09 ПК 3.2
	в том числе:		
	лабораторные работы		
	Криптографические методы защиты. Шифрование данных	***2***	
	практические занятия	***-***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся Исследование методов защиты данных в облачных средах	***2***	
Тема 1.7. Безопасность облачных технологий	**Содержание учебного материала**	***4***	ОК 01 ОК 02 ОК 09 ПК 3.1
	1. Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	***2***	
	в том числе:		
	лабораторные работы		
	практические занятия	***-***	
	Изучение модели облачных услуг и их безопасности	***2***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся	***-***	
Тема 1.8. Инциденты безопасности	**Содержание учебного материала**	***4***	ОК 01 ОК 02 ОК 09 ПК 1.5
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	***2***	
	в том числе:		
	лабораторные работы		
	Управление учетными записями и политиками безопасности в Windows	***2***	
	практические занятия	***-***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся Анализ методов социальной инженерии и разработка программы обучения пользователей	***2***	
Тема 1.9. Социальная	**Содержание учебного материала**	***4***	ОК 01 ОК 02

инженерия и человеческий фактор	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	***2***	ОК 09 ПК 1.1
	в том числе:		
	лабораторные работы		
	практические занятия	***-***	
	Разработка политики информационной безопасности	***2***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся	***-***	
Тема 1.10. Будущее информационной безопасности	**Содержание учебного материала**	***4***	ОК 01 ОК 02 ОК 09 ПК 1.4
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	***2***	
	в том числе:		
	лабораторные работы	***-***	
	Защита от вредоносного программного обеспечения. Антивирусы	***2***	
	практические занятия	***-***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся Эволюция киберугроз: применение искусственного интеллекта в атаках и защите	***2***	
Тема 1.11. Киберугрозы будущего: ИИ и машинное обучение в информационной безопасности	**Содержание учебного материала**	***4***	ОК 01 ОК 02 ОК 09 ПК 1.3
	Применение искусственного интеллекта для предотвращения угроз. Эволюция угроз с учетом новых технологий. Риски и вызовы, связанные с ИИ и машинным обучением в кибербезопасности.	***2***	
	в том числе:		
	лабораторные работы		
	практические занятия	***-***	
	Создание реферат на тему киберугрозы будущего	***2***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся	***-***	
Тама 1.12. Кибероружие и его	**Содержание учебного материала**	***4***	ОК 01 ОК 02 ОК 09 ПК 1.3
	Типы кибератак, поддерживаемых государственными структурами. Примеры использования кибероружия в международных конфликтах. Регулирование и	***2***	

влияние на глобальную безопасность	международные соглашения по киберугрозам.		
	в том числе:		
	лабораторные работы		
	Сетевая безопасность. Межсетевые экраны	***2***	
	практические занятия	***-***	
	контрольные работы	***-***	
	самостоятельная работа обучающихся	***-***	
Промежуточная аттестация		***12***	
Всего:		***60***	

В таблице пункта 2.2 в графе 3 указывается общее количество часов на изучение раздела дисциплины, а через дробь указывается количество часов, отводимое на изучение раздела дисциплины в форме практической подготовки.

3.УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Лаборатория «Компьютерных сетей и основ информационной безопасности».

ЦПУ:
- Intel(R) Core(TM) i3-10100
- количество физических ядер - 4
- количество потоков - 8

Сетевой адаптер:
- технология Ethernet - 10/100/1000 mbps

ОЗУ: - 8 ГБ

Графический адаптер:
- NVIDIA GeForce GT730

ПЗУ:- SSD 256 ГБ

3.2. Информационное обеспечение реализации программы

3.2.1. Основные печатные издания

1. Основы информационной безопасности : учебное пособие / составитель С. П. Середкин. — Иркутск : ИрГУПС, 2024. — 80 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/458102

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для СПО / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 284 с. — ISBN 978-5-507-52953-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/463001

3.2.2. 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.

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.

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

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

3.2.3. Дополнительные источники

1. Мельников, А. В. Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. — Москва : РГУП, 2025. — 220 с. — ISBN 978-5-00209-188-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/504758.

2. Рейн, Т. С. Основы информационной безопасности : учебное пособие / Т. С. Рейн, В. В. Торгулькин. — Кемерово : КемГУ, 2024. — 117 с. — ISBN 978-5-8353-3270-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/427526.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоенности 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	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	Экспертное наблюдение выполнения практических и лабораторных работ, экзамен

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; - 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	результатов поиска информации, современные 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.; Знает отраслевую нормативную техническую документацию и	

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; - 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	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	

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. ***Умеет:*** -распознавать задачу и/или проблему в профессиональном и/или социальном контексте; -анализировать задачу и/или проблему и	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	

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;	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;	

- использовать современное программное обеспечение; - использовать различные цифровые средства для 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.	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.	