МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ»

СРЕДНЕПРОФЕССИОНАЛЬНЫЙ КОЛЛЕДЖ

УТВЕРЖДАЮ
Зам. директора по УР
М.А. Малеева
«19» 02 2026г.

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности 09.02.11 Разработка и управление программным обеспечением

Черкесск 2026г.

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 09.02.11 Разработка и управление программным обеспечением, направление подготовки – 09.00.00 Информатика и вычислительная техника

Организация-разработчик: СПК ФГБОУ ВО «СевКавГА»

Разработчики:
Мамхягов Д.Ф. - преподаватель СПК ФГБОУ ВО «СевКавГА»

Одобрена на заседании цикловой комиссии «Информационные дисциплины»

от «06» 02 2026г. протокол № 6

Руководитель образовательной программы _____ Л.А. Черных

Рекомендована методическим советом колледжа

от «10» 02 2026г. протокол № 3

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	**3**
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	**5**
3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ	**10**
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	**12**

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина ОП.05 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.

Учебная дисциплина ОП.05 Основы информационной безопасности обеспечивает формирование профессиональных и общих компетенций по всем видам деятельности ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением. Особое значение дисциплина имеет при формировании и развитии:

ОК 1. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках.
ПК 1.1Проектировать базы данных.
ПК 1.4 Администрировать базы данных.
ПК 1.5Защищать информацию в базе данных с использованием технологии защиты информации.
ПК 3.1.Собирать исходные данные для разработки проектной документации на информационную систему
ПК 3.2.Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика
ПК 3.3Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием
ПК 3.5.Интегрировать информационную систему с существующими информационными системами заказчика.
ПК 3.7.Разрабатывать техническую документацию на эксплуатацию информационной системы

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания.

Код ОК, ПК	**Уметь**	**Знать**	**Владеть навыками**
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;	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном	-

	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)	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	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.	-

	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	применение современных методов и технологий 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	основные угрозы безопасности мобильных приложений принципы криптографии и шифрования данных.	использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и

	двухфакторную аутентификацию	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	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

		безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы	

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объём учебной дисциплины и виды учебной работы

Вид учебной работы	Объём в часах
Объём образовательной программы	**40**
Самостоятельная работа	**4**
Консультации	–
Суммарная учебная нагрузка во взаимодействии с преподавателем	**32**
в том числе:	
лекции, уроки	16
практические занятия	16
лабораторные занятия	–
Промежуточная аттестация (ДЗ)	**4**

2.2. Тематический план и содержание учебной дисциплины ОП.05 Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объём в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Основы информационной безопасности			
Тема 1.1. Введение в информационную безопасность	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	2	ОК 1–7, ОК 9; ПК 1.1, ПК 3.1, ПК 3.2
	Практические работы	–	
	Самостоятельная работа обучающихся Самостоятельное изучение лекционного материала, основной и дополнительной литературы.	2	
Тема 1.2. Управление безопасностью информации	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	ОК 1, ОК 2, ОК 9; ПК 1.5, ПК 3.7
	Практические работы	–	
	Самостоятельная работа обучающихся	–	
Тема 1.3. Криптография	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	2	ОК 1, ОК 2; ПК 1.5, ПК 3.7
	Практические работы Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	2	
	Самостоятельная работа обучающихся	–	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объём в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Основы информационной безопасности			
Тема 1.4. Защита сетевой инфраструктуры	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	2	ОК 1, ОК 2, ОК 9; ПК 3.1, ПК 3.2, ПК 3.3
	Практические работы Организация защиты от атак Организация работы VPN и межсетевого экрана	4	
	Самостоятельная работа обучающихся	–	
Тема 1.5. Безопасность приложений	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2	ОК 1, ОК 2; ПК 3.2, ПК 3.5, ПК 3.7
	Практические работы Тестирование на проникновение и анализ уязвимостей.	2	
	Самостоятельная работа обучающихся	–	
Тема 1.6. Защита данных	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным	2	ОК 1, ОК 2; ПК 1.5, ПК 3.3, ПК 3.7
	Практические работы Выполнение резервного копирования и восстановления данных. Управление доступом к данным	2	
	Самостоятельная работа обучающихся	–	
Тема 1.7. Безопасность облачных технологий	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	1	ОК 1, ОК 2;

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объём в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Основы информационной безопасности			
	Практические работы Изучение модели облачных услуг и их безопасности	2	ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.3
	Самостоятельная работа обучающихся	–	
Тема 1.8. Инциденты безопасности	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	1	ОК 1, ОК 2; ПК 3.2, ПК 3.5, ПК 3.7
	Практические работы Работа с инцидентами.	2	
	Самостоятельная работа обучающихся	–	
Тема 1.9. Социальная инженерия и человеческий фактор	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	1	ОК 1, ОК 2; ПК 3.5, ПК 3.7
	Практические работы Разработка политики информационной безопасности	2	
	Самостоятельная работа обучающихся	–	
Тема 1.10. Будущее информационной безопасности	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	1	ОК 1, ОК 2
	Практические работы	–	
	Самостоятельная работа обучающихся	2	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объём в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Основы информационной безопасности			
	Самостоятельное изучение лекционного материала, основной и дополнительной литературы.		
Промежуточная аттестация (ДЗ)	**Дифференцированный зачёт**	**4**	
Всего:		**40**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Лаборатория «Компьютерных сетей и основ информационной безопасности», оснащённые необходимым для реализации программы учебной дисциплины оборудованием:

Комплект учебной мебели: доска меловая – 1 шт., стол ученический – 18 шт., стул ученический – 26 шт., стол – 1 шт., стул – 1 шт.

Комплект учебно-методической документации

Технические средства обучения: компьютер в сборе (системный блок *IntelCore 17-9700K, плата CICABYNELCA-1151, корпусCorsair 270R, блок питанияATX-2.3 120мм, жесткий дискSATA-3.1 tb, мониторLG-21.5 22 MK 400H-B 1920/1080, клавиатура + мышь) – 1 шт.; компьютер в сборе (корпусAEROCOOLV-2XVX-500 (10 шт.), корпусAerocoolAero 500 USB 3.0 (2 шт.), системный блок IntelCore 137100 3.9, платаMSILCA 1151 H110 H110M, блок питания – 350WATX 2.3, памятьDIMMDDR4 8192 MB, жесткий дискSATA-3.1 tb, мониторLG-21.5 22 MK 400H-B 1920/1080, клавиатура + мышь) – 12 шт.; принтер HPLaserJet 1320;проектор EPSONE6-X400 1024x768; настенный экран DEXPWM-80 203*203 см 113.

3.2. Информационное обеспечение реализации программы

Список основной литературы	
1	Баланов А.Н. Защита информационных систем. Кибербезопасность : учебное пособие / А.Н. Баланов. — Санкт-Петербург : Лань, 2024. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394547
2	Баланов А.Н. Комплексная информационная безопасность : учебное пособие / А.Н. Баланов. — Санкт-Петербург : Лань, 2024. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414950
3	Нестеров С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров. — Санкт-Петербург : Лань, 2022. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510
4	Прохорова О.В. Информационная безопасность и защита информации : учебное пособие / О.В. Прохорова. — Санкт-Петербург : Лань, 2024. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082
Список дополнительной литературы	
1	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». — Текст : электронный //

Список основной литературы	
	КонсультантПлюс. — URL: https://www.consultant.ru/document/cons_doc_LAW_61798/
2	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». — Текст : электронный // КонсультантПлюс. — URL: https://www.consultant.ru/document/cons_doc_LAW_61801/
3	ФСТЭК России. Банк данных угроз безопасности информации (БДУ). — Текст : электронный // ФСТЭК России : [сайт]. — URL: https://bdu.fstec.ru
4	НКЦКИ. Национальный координационный центр по компьютерным инцидентам. — Текст : электронный // cert.gov.ru : [сайт]. — URL: https://cert.gov.ru
5	ГОСТ Р ИСО/МЭК 27001-2021. Информационная безопасность. Системы менеджмента информационной безопасности. Требования. — М. : Стандартинформ, 2021.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Результаты обучения	Критерии оценки	Методы оценки
Перечень осваиваемых компетенций в рамках дисциплины: ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 7, ОК 9; ПК 1.1, ПК 1.4, ПК 1.5; ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7. **Перечень знаний, осваиваемых в рамках дисциплины:** - 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;	**Оценка «отлично»** Обучающийся показывает полные и глубокие знания программного материала, логично и аргументировано отвечает на поставленный вопрос, а также дополнительные вопросы, показывает высокий уровень теоретических знаний. Практическую часть выполняет на 100%. **Оценка «хорошо»** Обучающийся показывает глубокие знания программного материала, грамотно его излагает, достаточно полно отвечает на поставленный вопрос и дополнительные вопросы, умело формулирует выводы. При ответе допускает несущественные погрешности. Практическую часть выполняет на 90%–80%. **Оценка «удовлетворительно»** Обучающийся показывает достаточные, но неглубокие знания; не допускает грубых ошибок, однако в ответе отсутствует должная связь между анализом, аргументацией и выводами. Требуются уточняющие вопросы.	**Текущий контроль в форме:** практических заданий; тестовых опросов; фронтальных опросов; самостоятельной работы. **Промежуточная аттестация:** ДЗ (дифференцированный зачёт). **Оценка:** результативности работы обучающегося при выполнении практических заданий; тестовых и фронтальных опросов; самостоятельной работы.

Результаты обучения	Критерии оценки	Методы оценки
- 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; - 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,	Практическую часть выполняет на 70%–60%. **Оценка «неудовлетворительно»** Обучающийся показывает недостаточные знания, не способен аргументировано излагать материал, допускает грубые ошибки или затрудняется с ответом. Практическую часть выполняет менее чем на 50%.	

Результаты обучения	Критерии оценки	Методы оценки
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; - стандарты и протоколы безопасности, такие как		

Результаты обучения	Критерии оценки	Методы оценки
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.		

Результаты обучения	Критерии оценки	Методы оценки
Перечень умений, осваиваемых в рамках дисциплины: -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;		

Результаты обучения	Критерии оценки	Методы оценки
- 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; - шифрование данных и обеспечивает их конфиденциальность; - анализировать требования безопасности информационных систем; - разрабатывать и реализовывать меры безопасности; - реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.		