

Федеральное государственное образовательное бюджетное учреждение
высшего образования

**«Финансовый университет при Правительстве
Российской Федерации»
(Финансовый университет)**

Владикавказский филиал Финуниверситета

УТВЕРЖДАЮ

Заместитель директора
по учебно-методической работе
Владикавказского филиала
Финуниверситета

З. Аглаф З.К. Айларова
« 31 » августа 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ОП.11 ИНФОРМАЦИОННАЯ

БЕЗОПАСНОСТЬ»

по специальности 09.02.13 Интеграция решений с применением
технологий искусственного интеллекта

Владикавказ 2026

Рабочая программа дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 09.02.13 Интеграция решений с применением технологий искусственного интеллекта.

Разработчик:

Теблосева Анжела Викторовна, преподаватель.

Рабочая программа дисциплины рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии математики и информатики

Протокол от «28» 08 2026г. № 1

Председатель предметной (цикловой)
комиссии математики и информатики

 М.К. Ходова

1. Общая характеристика рабочей программы дисциплины

1.1. Место дисциплины в структуре основной образовательной программы

Дисциплина «ОП. 11 Информационная безопасность» является дисциплиной вариативной части общепрофессионального цикла образовательной программы среднего профессионального образования - программы подготовки специалистов среднего звена по специальности 09.02.13 Интеграция решений с применением технологий искусственного интеллекта.

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы дисциплины студентами осваиваются умения и знания:

Код общих и профессиональных компетенций	Умения	Знания
ОК 01	– распознавать базовые угрозы ИБ в профессиональном контексте; выделять этапы анализа угроз и составлять план действий – анализировать архитектуру системы на предмет уязвимостей; Составлять модель угроз для ИС с элементами ИИ; – проводить качественную оценку рисков; выбирать меры обработки рисков (снижение, принятие, передача); – разрабатывать регламенты реагирования на инциденты; планировать действия по ликвидации последствий сбоев;	– структуру базовых угроз и источников риска; алгоритмы идентификации угроз в нормативных документах; – классификацию угроз по источникам и способам реализации; – методы построения моделей угроз; – этапы процесса управления рисками; – шкалы оценки вероятности и ущерба; – структуру политики ИБ и стандартов (ISO 27001, ГОСТ); порядок документирования процедур реагирования;
ОК 02	– находить и анализировать нормативные акты в области защиты информации; оформлять результаты правового анализа; – применять сетевые сканеры и анализаторы трафика; настраивать правила межсетевого экрана и VPN; – выявлять уязвимости по методике OWASP Top 10 – работать с профессиональными тезаурусами и базами стандартов; – использовать	– номенклатуру источников правовой информации (152-ФЗ, приказы ФСТЭК); форматы оформления локальных нормативных актов; – принципы работы фаерволов, IDS/IPS, VPN-протоколов; методы анализа сетевого трафика; – типовые уязвимости веб-приложений и способы их эксплуатации; – методы защиты от инъекций,

	специализированные инструменты тестирования; –сравнивать требования ГОСТ, ФСТЭК, ISO	XSS, небезопасной аутентификации; – действующие стандарты в области ИБ (серии 27000, 56545, 56546); – правила интерпретации терминологии в нормативных документах
ОК 03	– применять современную научную профессиональную терминологию; – определять актуальность нормативной базы для конкретной организации; – выявлять достоинства и недостатки коммерческой идеи; – презентовать идеи по улучшению системы защиты информации; – составлять различные правовые документы; – находить интересные проектные идеи, грамотно их формулировать и документировать; – оценивать жизнеспособность проектной идеи, составлять план проекта в области ИБ	– содержание 152-ФЗ, законов «О безопасности», «Об информации»; основы правовой ответственности в информационной сфере; – правовое регулирование использования ЭП и СКЗИ в РФ; основы управления ключами и инфраструктурой PKI; – основные этапы разработки и реализации проектов в сфере ИБ; правила подготовки презентаций и проектной документации; – основы правового регулирования ИИ в РФ и мире; принципы дифференциальной приватности и объяснимости ИИ
ОК 09	– читать и понимать техническую документацию на СКЗИ (в т.ч. на английском); кратко обосновывать выбор криптоалгоритма; – участвовать в обсуждении настроек сетевого оборудования на профессиональном языке; писать простые отчёты по результатам аудита безопасности; – анализировать отчёты об инцидентах и угрозах (в т.ч. международные источники) – строить связные сообщения о методах защиты от вредоносного ПО	– лексику, описывающую криптографические процессы и протоколы; правила чтения технических спецификаций и стандартов; – профессиональную терминологию в области сетевых протоколов, атак, средств защиты; особенности произношения и написания англоязычных аббревиатур (DoS, IDS, PKI, XSS); – лексический минимум для описания вредоносного ПО, методов анализа и защит; правила работы с англоязычными базами уязвимостей (CVE, NVD)

2. Структура и содержание дисциплины

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объём в часах
Объём образовательной программы дисциплины	74
Объём работы студентов во взаимодействии с преподавателем	68
в том числе:	
теоретическое обучение	30
практические занятия	38
лабораторные занятия	-
контрольные работы	-
Курсовой проект (работа) (если предусмотрено)	-
самостоятельная работа	6
Промежуточная аттестация в форме дифференцированного зачета	-

2.2. Тематический план и содержание учебной дисциплины

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 и угрозы		8	ОК 01, ОК 02
Тема 1.1. Введение в информационную безопасность	Содержание учебного материала 1. Понятие информации, информационной безопасности. Основные составляющие ИБ: конфиденциальность, целостность, доступность. 2. Национальные интересы в информационной сфере. Место ИБ в системе национальной безопасности. 3. Нормативно-правовое регулирование в области ИБ: Конституция РФ, законы «О безопасности», «Об информации, информационных технологиях и о защите информации». 4. Понятие угрозы информационной безопасности. Классификация угроз (природные, техногенные, антропогенные). Источники угроз.	4	ОК 01
	В том числе практических занятий	2	
	Практическое занятие «Правовой анализ и идентификация базовых угроз информационной безопасности»	2	
Тема 1.2. Классификация угроз и уязвимости автоматизированных систем	Содержание учебного материала 1. Детальная классификация угроз: по природе возникновения, по степени преднамеренности, по положению источника. 2. Понятие уязвимости. Классификация уязвимостей (программные, технические, организационные, человеческий фактор). 3. Анализ угроз и уязвимостей, характерных для систем, обрабатывающих большие данные и использующих технологии искусственного интеллекта (отравление данных, искажение модели, состязательные атаки). 4. Понятие угрозы информационной безопасности	4	ОК 01, ОК 02
	В том числе практических занятий	2	
	Практическое занятие «Разработка модели угроз и уязвимостей для информационной системы с элементами ИИ»	2	

Раздел 2. Организационно-правовые и технические основы защиты информации		12	ОК 01, ОК 02, ОК 03, ОК 09
Тема 2.1. Правовое обеспечение информационно й безопасности и защита персональных данных	Содержание учебного материала 1. Законодательство РФ в области защиты информации. Ответственность за правонарушения в информационной сфере. 2. Правовой режим защиты государственной тайны, коммерческой тайны, конфиденциальной информации. 3. Федеральный закон «О персональных данных» №152-ФЗ. Принципы и условия обработки персональных данных. Права субъектов персональных данных. 4. Хранение и уничтожение персональных данных	4	ОК 03
	В том числе практических занятий	2	
	Практическое занятие «Разработка организационно-распорядительной документации по защите персональных данных»	2	
Тема 2.2. Инженерно-техническая защита информации и безопасность объектов	Содержание учебного материала 1. Основные понятия и концепция инженерно-технической защиты 2. Физическая защита объектов информатизации. Средства охраны, контроля доступа, видеонаблюдения. 3. Технические каналы утечки информации (акустические, визуально-оптические, электромагнитные). Методы и средства их перекрытия. 4. Угрозы безопасности информации и технические каналы утечки	4	ОК 02, ОК 09
	В том числе практических занятий	2	
	Практическое занятие «Исследование и классификация средств инженерно-технической защиты информации»	2	
Тема 2.3. Криптографические методы защиты информации	Содержание учебного материала 1. Основные понятия криптографии: шифрование, дешифрование, ключ. Симметричные и асимметричные криптосистемы. 2. Электронная подпись (ЭП): понятие, назначение, виды. Правовое регулирование ЭП. 3. Хэш-функции. Управление ключами. Инфраструктура открытых ключей (PKI). 3. Основные криптосистемы с открытым ключом 4. Прикладные аспекты и реализация криптографических методов	4	ОК 01, ОК 02 ОК 03, ОК 09

	5. Применение средств криптографической защиты информации (СКЗИ) 6. Разработка внутренних документов по защите информации		
	В том числе практических занятий	2	
	Практическое занятие «Применение средств криптографической защиты информации (СКЗИ)»	2	
Раздел 3. Безопасность компьютерных сетей и систем		14	ОК 01, ОК 02, ОК 03, ОК 09
Тема 3.1. Сетевые угрозы и методы обеспечения безопасности сетей	Содержание учебного материала 1. Основные угрозы безопасности компьютерных сетей: перехват данных, анализ трафика, подмена узлов, атаки типа «отказ в обслуживании» (DoS/DDoS). 2. Межсетевые экраны (Firewalls): принципы работы, типы (фильтрующие, прокси-серверы, stateful inspection). 3. VPN (Virtual Private Network): протоколы, назначение, схемы построения защищенных каналов связи. 4. Системы обнаружения и предотвращения вторжений (IDS/IPS).	4	ОК 01, ОК 03, ОК 09
	В том числе практических занятий	2	
	Практическое занятие «Конфигурирование межсетевого экрана для защиты периметра сети»	2	
	Самостоятельная работа «Организация защищенного канала связи с использованием VPN»	2	
Тема 3.2. Безопасность беспроводных сетей и мобильных устройств	Содержание учебного материала	4	ОК 01, ОК 09
	1. Особенности обеспечения безопасности в сетях Wi-Fi. Протоколы защиты: WEP, WPA/WPA2/WPA3. Угрозы для беспроводных сетей. 2. Основные угрозы для мобильных устройств и платформ. Вредоносное ПО для мобильных устройств. 3. Правила безопасной работы в публичных сетях Wi-Fi. Меры защиты мобильных устройств.		
	В том числе практических занятий		
	Практическое занятие «Аудит безопасности беспроводной сети»		
Тема 3.3.	Содержание учебного материала	4	

Безопасность приложений и веб-ресурсов	1. Основные уязвимости веб-приложений (OWASP Top 10): инъекции SQL, межсайтовый скриптинг (XSS), небезопасная аутентификация и др. 2. Безопасность баз данных. Защита от SQL-инъекций. 3. Безопасность облачных вычислений и хранения данных. Модели разделения ответственности.		OK 02, OK 03, OK 09
	В том числе практических занятий	2	
	Практическое занятие «Выявление и анализ уязвимостей веб-приложений»	2	
Раздел 4. Управление информационной безопасностью и защита систем ИИ		16	OK 01, OK 02, OK 03, OK 09
Тема 4.1. Управление рисками информационной безопасности	Содержание учебного материала 1. Понятие и основные этапы управления рисками ИБ: идентификация, оценка, обработка рисков. 2. Методы оценки рисков (качественные и количественные). Шкалы ущерба и вероятности. 3. Выбор мер по обработке рисков (снижение, принятие, избегание, передача). Остаточный риск. 4. Документирование процедур оценки рисков.	4	OK 03
	В том числе практических занятий	2	
	Практическое занятие Проведение качественной оценки и обработки рисков информационной безопасности»	2	
Тема 4.2. Организация режима информационной безопасности на предприятии	Содержание учебного материала 1. Политика информационной безопасности как основной документ. Структура и содержание политики ИБ. 2. Стандарты и методологии в области ИБ (ISO/IEC 27000, ГОСТ Р ИСО/МЭК 27001). 3. Реагирование на инциденты ИБ. План действий в случае нарушения безопасности. Компьютерная криминалистика (форензика).	4	OK 02, OK 03
	В том числе практических занятий	2	
	Практическое занятие «Разработка регламентов реагирования на инциденты информационной безопасности»	2	
	Самостоятельная работа «Обеспечение непрерывности бизнеса и восстановление после сбоев».	2	
Тема 4.3.	Содержание учебного материала	6	

Специфика защиты систем искусственного интеллекта	1.Классификация уязвимостей систем ИИ: атаки на этапе обучения (отравление данных), атаки на этапе эксплуатации (сопоставительные примеры), атаки, направленные на кражу модели. 2. Методы защиты: валидация и очистка данных, сопоставительное обучение, дифференциальная приватность. 3. Этические аспекты применения ИИ. Прозрачность и объяснимость моделей ИИ. Правовое регулирование в сфере ИИ.		ОК 01, ОК 02, ОК 09
	В том числе практических занятий	4	
	1.Практическое занятие «Анализ уязвимостей модели машинного обучения (на примере готового датасета).»	2	
	2. Практическое занятие «Искажение входных данных (сопоставительный шум).»	2	
Раздел 5. Специальные вопросы обеспечения информационной безопасности		24	ОК 01, ОК 02, ОК 03, ОК 09
Тема 5.1. Вредоносное программное обеспечение и методы защиты	Содержание учебного материала 1.Классификация вредоносного ПО: вирусы, черви, трояны, программы-шпионы, программы-вымогатели (шифровальщики). 2. Современные угрозы: АРТ-атаки (целевые атаки), полиморфизм, стелс-технологии. 3. Признаки заражения компьютерных систем. Анализ поведения программ. 4. Методы и средства антивирусной защиты: сигнатурный и эвристический анализ, проактивная защита. Политика использования антивирусных средств.	4	ОК 01, ОК 02, ОК 09
	В том числе практических занятий	2	
	1.Практическое занятие «Анализ вредоносного ПО и методов защиты»	2	
Тема 5.2. Резервное копирование и восстановление данных	Содержание учебного материала 1. Цели и задачи резервного копирования как элемента обеспечения доступности и целостности информации. 2. Типы резервного копирования: полное, инкрементальное, дифференциальное. 3. Схемы ротации носителей. 4. Программно-аппаратные средства резервного копирования. Хранение резервных копий (on-premise, облако). 5.Политика резервного копирования и восстановления. План Disaster Recovery (DRP)	4	ОК 01, ОК 02
	В том числе практических занятий	2	
	1.Практическое занятие «Разработка политики резервного копирования»	2	

Тема 5.3. Терминологическая база и стандартизация в области ИБ	Содержание учебного материала 1. Основные термины и определения в области информационной безопасности. Работа с профессиональным тезаурусом. 2. Анализ разночтений в терминологии различных нормативных документов (ГОСТ, ФСТЭК, международные стандарты). 3. Обзор действующих стандартов в области ИБ: серии ГОСТ Р ИСО/МЭК 27000, ГОСТ Р 56545, ГОСТ Р 56546.	14	ОК 01, ОК 02, ОК 03
	В том числе практических занятий	10	
	1. Практическое занятие «Анализ угроз облачных технологий»	2	
	2. Практическое занятие «Анализ угроз мобильных технологий»	2	
	3. Практическое занятие «Анализ специализированных векторов атак и методов защиты»	2	
	4. Практическое занятие «Изучение сложных технических атак и методов защиты»	2	
	5. Практическое занятие «Анализ реальных кибератак и прогнозирование будущих угроз»	2	
	Самостоятельная работа «Специализированные атаки и методы противодействия»	2	
	Промежуточная аттестации в форме дифференцированного зачета	-	
Всего:		74	ОК 01, ОК 02, ОК 03, ОК 09

3. Условия реализации дисциплины

3.1. Материально-техническое обеспечение

Для реализации программы дисциплины предусмотрены следующее специальное помещение:

- учебная аудитория для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, а также проведения текущего контроля, промежуточной аттестации и государственной итоговой аттестации, оснащенная оборудованием, техническими средствами обучения

(Кабинет общепрофессиональных дисциплин и профессиональных модулей)

Специализированная мебель:

Стол студенческий (двухместный) – 15 шт.

Стол одно-тумбовый (учительский) – 1 шт.

Стул – 30 шт.

Стул для преподавателя – 1 шт.

Шкаф для хранения учебной и методической литературы – 1 шт.

Кафедра – 1 шт.

Доска меловая – 1 шт.

Технические средства обучения:

Компьютер в сборе – 1 шт.

Мультимедийный проектор – 1 шт.

Помещение для самостоятельной работы (Библиотека, читальный зал с выходом в интернет)

Специализированная мебель:

Стол – 20 шт.

Стул – 40 шт.

Столы для автоматизированных рабочих мест (двухместные) – 6 шт.

Шкаф для книг – 4 шт.

Стеллаж книжный – 13 шт.

Стеллаж выставочный – 4 шт.

Каталожный шкаф – 1 шт.

Технические средства обучения:

Компьютер в сборе – 6 шт.

Телевизор – 1 шт.

Подключение к сети «Интернет» и обеспечение доступа в электронную информационно-образовательную среду Финансового университета

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд Владикавказского филиала Финуниверситета имеет печатные и электронные образовательные и информационные ресурсы для использования в образовательном процессе:

3.2.1. Основные печатные и электронные издания:

1. Щербаков А.В. Информационная безопасность: учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. URL: <https://urait.ru/bcode/588374> — Режим доступа: Электронно-библиотечная система Юрайт. — Текст: электронный.

2. Раченко, Т. А. Информационная безопасность: учебно-методическое пособие / Т. А. Раченко. — Тольятти: ТГУ, 2024. — 135 с. — ISBN 978-5-8259-1612-5. — URL: <https://e.lanbook.com/book/427130> — Режим доступа: Электронно-библиотечная система Лань. — Текст: электронный.

3.2.2. Дополнительная литература:

1. 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. — URL: <https://e.lanbook.com/book/463001> — Режим доступа: Электронно-библиотечная система Лань. — Текст: электронный.

2. Ищейнов, В. Я. Информационная безопасность и защита информации: словарь терминов и понятий: словарь / В. Я. Ищейнов. — Москва: Русайнс, 2026. — 226 с. — ISBN 978-5-466-10276-5. — URL: <https://book.ru/book/959878> — Режим доступа: Электронно-библиотечная система Book.ru. — Текст: электронный.

4. Контроль и оценка результатов освоения дисциплины

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, выполнения студентами индивидуальных заданий, а также в ходе проведения промежуточной аттестации.

Код и наименование общих и профессиональных компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
–распознавать базовые угрозы ИБ в профессиональном контексте; выделять этапы анализа угроз и составлять план действий; –анализировать архитектуру системы на предмет уязвимостей; Составлять модель угроз для ИС с элементами ИИ; –проводить качественную оценку рисков; выбирать меры обработки рисков (снижение, принятие, передача); –разрабатывать регламенты реагирования на инциденты; планировать действия по ликвидации последствий сбоев; –находить и анализировать нормативные акты в области защиты информации; оформлять результаты правового анализа; –применять сетевые сканеры и анализаторы трафика; настраивать правила межсетевого экрана и VPN; –выявлять уязвимости по методике OWASP Top 10 –работать с профессиональными тезаурусами и базами стандартов; –использовать специализированные инструменты тестирования; –сравнивать требования ГОСТ, ФСТЭК, ISO –применять современную научную профессиональную терминологию; –определять актуальность нормативной базы для конкретной организации; –выявлять достоинства и недостатки коммерческой идеи; –презентовать идеи по улучшению системы защиты информации; –составлять различные правовые документы; –находить интересные проектные идеи, грамотно их формулировать и документировать; –оценивать жизнеспособность проектной идеи, составлять план проекта в области ИБ	«Отлично» - теоретическое содержание темы (дисциплины) освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание темы (дисциплины) освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание темы (дисциплины) освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения	Текущий контроль: - устный опрос; – выполнения практических заданий; – компьютерного тестирования по темам, – оценки самостоятельной и творческой работы. Промежуточная аттестация – дифференцированный зачет

– читать и понимать техническую документацию на СКЗИ (в т.ч. на английском); кратко обосновывать выбор криптоалгоритма; – участвовать в обсуждении настроек сетевого оборудования на профессиональном языке; писать простые отчёты по результатам аудита безопасности; – анализировать отчёты об инцидентах и угрозах (в т.ч. международные источники) – строить связные сообщения о методах защиты от вредоносного ПО.	учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание темы (дисциплины) не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	
--	--	--