МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет компьютерных технологий и прикладной математики

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
подпись
« 29 » августа 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1. В.02 Основы информационной безопасности

Направление подготовки 01.03.02 Прикладная математика и информатика

Профиль Современные методы машинного обучения и компьютерного зрения

Форма обучения очная

Квалификация бакалавр

Краснодар 2025

Рабочая программа дисциплины «Основы информационной безопасности» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.03.02 Прикладная математика и информатика.

Программу составили:
В.И. Шиян, ст. преп. КВТ
И.О. Фамилия, должность, ученая степень, ученое звание
подпись

Т.А. Приходько, доц. КВТ, к.т.н., доц.
И.О. Фамилия, должность, ученая степень, ученое звание
подпись

Рабочая программа дисциплины «Кроссплатформные десктоп приложения» утверждена на заседании кафедры вычислительных технологий
протокол №1 от 26 августа 2025 г.
И.о. заведующего кафедрой (разработчика)
Т. А. Приходько
подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики
протокол №1 от 28 августа 2025 г.
Председатель УМК факультета
А. В. Коваленко
подпись

Рецензенты:

Мостовой Евгений Викторович, генеральный директор ООО «Портал-Юг», e-mail: mostovoy@portal-yug.ru

Луценко Евгений Вениаминович, д.э.н., к.т.н., профессор кафедры компьютерных технологий и систем ФГБОУ ВО «КубГАУ им. И.Т. Трубилина», e-mail: prof.lutsenko@gmail.com

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины

Цель дисциплины – сформировать у обучающихся системное понимание принципов информационной безопасности (ИБ) и практических методов защиты современных информационных систем, включая ИИ-системы, чат-боты, большие языковые модели (LLM) и Retrieval-Augmented Generation (RAG), на базе стандартов, фреймворков и лучших практик.

1.2 Задачи дисциплины

1. Изучение основ ИБ: свойства безопасности, угрозы и уязвимости, модели нарушителя, управление рисками, политика безопасности.
2. Освоение средств защиты: криптография, контроль доступа, аутентификация/авторизация, сетевые экраны, IDS/IPS, SIEM.
3. Безопасность программного обеспечения и Secure SDLC (SAST/DAST, управление зависимостями/секретами), DevSecOps.
4. Безопасность облачных и контейнерных сред (IAM, политика сети, реестр образов, сканирование уязвимостей).
5. Специальный модуль: безопасность ИИ-систем и LLM/RAG: угрозы (prompt-injection, jailbreak, model/RAG poisoning, model-DoS, insecure output handling), защиты (guardrails, проверка источников, контент-фильтрация, аудит и трассировка, верификация цитат), соответствие OWASP LLM Top-10 и фреймворкам NIST AI RMF 1.0, ISO/IEC 23894:2023.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к базовой части Б1.В.02.

Дисциплина в значительной степени **взаимодействует для формирования компетенций** с дисциплинами:

1. Мультиагентные системы
2. Операционные системы
3. Нейросетевые технологии

Требованием к «входным» знаниям является понимание основ сетей и операционных систем, навыки программирования на Python, знание базовой веб-архитектуры и облачных технологий.

1.4 Профессиональные роли в структуре образовательной программы

Роль 1: **Data Engineer (Инженер по данным)**
Задачи:

- Проектирование и построение ETL-процессов
- Создание и оптимизация хранилищ данных
- Обеспечение качества и доступности данных
- Настройка инфраструктуры для обработки больших данных
- Интеграция разрозненных источников данных
- Работа с данными в области природопользования, медицины, связи и телекоммуникаций

Роль 2: **ML Engineer (Инженер МО)**
Задачи:

- Реализация ML-моделей в продуктивных системах

- Оптимизация производительности и масштабирование моделей
- Разработка ML-пайплайнов и автоматизация процессов
- Мониторинг качества моделей в продуктиве
- Интеграция ML-решений с бизнес-приложениями

Роль 3: **MLOps (Специалист по эксплуатации ИИ)**
Задачи:

- Автоматизация процессов обучения и развертывания моделей
- Мониторинг производительности ML-систем
- Управление версиями моделей и данных
- Обеспечение CI/CD для ML-проектов
- Оптимизация вычислительных ресурсов

1.5 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

УК-3	***Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде***
УК-3.1	Понимает основные аспекты межличностных и групповых коммуникаций; соблюдает нормы и установленные правила поведения в организации Знает подходы к лидерству/делегированию. Умеет управлять командой в инцидент-сценариях. Владеет публичной защитой с технико-рисковым обоснованием.
ПК-4	***Способен планировать необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции***
ПК-4.1	Использует современные инструментальные средства разработки баз данных, прикладного программного обеспечения и систем различного функционального назначения Знает основы DevSecOps-подхода при выборе инструментальных средств. Умеет интегрировать инструменты статического и динамического анализа в процесс разработки. Владеет настройкой автоматизированных пайплайнов для обеспечения безопасности и качества ПО.
ПК-4.2	Применяет современные приемы работы с инструментальными средствами, поддерживающими создание программных продуктов и программных комплексов на базе языков программирования, баз данных и пакетов прикладных программ Знает тонкости криптоконфигов TLS/SSH и supply-chain риски. Умеет писать собственные правила Semgrep/IDS. Владеет построением «красной линии» в CI с SLA на исправления.
ПК-4.3	Способен использовать методы эффективного управления командой при разработке, внедрении и сопровождении программных продуктов Знает практики policy-as-code. Умеет внедрять риск-ориентированное планирование релизов. Владеет настройкой security-gates и KPI процесса.
SS-1	***Способен осуществлять свою трудовую деятельность с учетом определения корректной роли ИИ в различных процессах, критического анализа последствий применения ИИ-технологий, этических принципов***
SS-1.1	Определяет ценностные предпосылки, когнитивные искажения, культурно-

	обусловленные предвзятости в данных, алгоритмах, постановке задач для ИИ. Самостоятельно анализирует обучающую выборку на предмет репрезентативности, возможных искажений, скрытых предвзятостей. Соотносит технические характеристики модели с потенциальными рисками её применения (например, низкая устойчивость к шуму — риск в медицинской диагностике).
SS-3	***Способен осуществлять свою трудовую функцию с учетом неопределенности как сущностной черты функционирования искусственного интеллекта***
SS-3.1	Учитывает в работе когнитивные искажения человека и выявляет предвзятости систем ИИ, аргументированно оценивает надежность данных и выдачи ИИ Осуществляет регулярную рефлексию своих мыслительных практик и практики работы с ИИ; анализирует множественные уровни последствий внедрения ИИ (технологический, организационный, нормативный, этический); формулирует сценарии влияния ИИ в своей области и за её пределами.
LC-1 Б	***Способен проводить анализ бизнес-проблем с оценкой перспективности применения ИИ для их решения, осуществлять постановку задачи машинного обучения, формулировать требования к системе ИИ***
LC-1.3	Готовит и ведет документы для реализации проектов в области ИИ Оценивает технические требования на основе формализованной постановки
ML-5 П	***Способен разрабатывать и (или) применять методы повышения устойчивости, надежности, безопасности алгоритмов МО***
ML-5.1	Обосновывает способы и варианты применения методов повышения устойчивости, надежности, безопасности алгоритмов МО задачах ИИ, включая их преобразование и адаптацию к специфике задачи Обосновывает выбор и применение методов повышения устойчивости и надежности моделей с учётом специфики задачи, включая адаптацию моделей и использование подходов объяснимого ИИ и доверенного ИИ. Учитывает риски атак и методы их противодействия.
ML-5.2	Применяет методы повышения устойчивости, надежности, безопасности алгоритмов МО для проверки разведочных гипотез и подготовки данных к применению современных методов ИИ Использует продвинутые методы дообучения моделей при подготовке данных, применяет методы повышения устойчивости моделей к атакам и искажениям данных
ML-5.3	Оценивает результативность применения методов повышения устойчивости, надежности, безопасности алгоритмов МО в задачах ИИ на основе сопоставления с аналогами Проводит комплексный анализ результативности с учётом объяснимости моделей, устойчивости к атакам, использует методы доверенного ИИ для оценки.
AI S-1 Б	***Способен управлять рисками в разработке систем ИИ, выстраивать управление безопасностью ИИ в компании с учетом этики ИИ***
AI S-1.1	Выявляет и моделирует угрозы на всём жизненном цикле ИИ-систем, оценивает и приоритизирует риски Понимает основные категории рисков и атак на ИИ (data poisoning, model stealing, evasion). Применяет типовые методики (STRIDE, MITRE ATLAS) по готовым шаблонам. Следует в работе ГОСТ Р ISO/IEC 27005-2010; ПНСТ 836-2023 «ИИ. Функциональная безопасность»; методики ФСТЭК по оценке угроз (2024); Знает международные фреймворки и стандарты NIST AI RMF 1.0; ISO/IEC 27005 (risk); MITRE ATLAS; STRIDE/PASTA.

AI S-1.2 Обеспечивает соответствие нормативным требованиям и принципам доверенного/этичного ИИ
Знаком с Кодексом этики в сфере ИИ РФ (2021) , базовых принципах Responsible AI, законом 152-ФЗ «О перс. данных» и основами GDPR. Может описать процесс Data Impact Assessment.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 часов), их распределение по видам работ представлено в таблице

Вид учебной работы		Всего часов	Семестры (часы)					
			8					
Контактная работа, в том числе:		**46,3**	**46,3**					
Аудиторные занятия (всего):		**42**	**42**					
Занятия лекционного типа		**28**	28					
Лабораторные занятия		**14**	14					
Занятия семинарского типа (семинары, практические занятия)								
Иная контактная работа:		**4,3**	**4,3**					
Контроль самостоятельной работы (КСР)		**4**	4					
Промежуточная аттестация (ИКР)		**0,3**	0,3					
Самостоятельная работа, в том числе:		**8**	**8**					
Курсовая работа								
Выполнение индивидуальных заданий		**8**	8					
Реферат								
Подготовка к текущему контролю								
Контроль:		**53,7**	**53,7**					
Подготовка к экзамену		**53,7**	53,7					
Общая трудоемкость	**час.**	**108**	**108**					
	в том числе контактная работа	**46,3**	**46,3**					
	зач. ед.	**3**	**3**					

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) дисциплины, изучаемые в 8 семестре

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Основы ИБ и управление рисками	15	9		4	2
2.	Безопасность ПО, инфраструктуры и облака	17	9		5	3
3.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	18	10		5	3
ИТОГО по разделам дисциплины		**50**	**28**		**14**	**8**

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
Контроль самостоятельной работы (КСР)		4				
Промежуточная аттестация (ИКР)		0,3				
Подготовка к текущему контролю		53,7				
Общая трудоемкость по дисциплине		**108**				

Примечание: Л – лекции, ПЗ – практические занятия/семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1	2	3	4
1.	Основы ИБ и управление рисками	Введение в ИБ: цели, задачи, угрозы, стандарты и риск-ориентированный подход.	ЛР
2.	Основы ИБ и управление рисками	Криптография для инженера: хеш-функции, подписи, симметричное/асимметричное шифрование, TLS.	ЛР
3.	Основы ИБ и управление рисками	Идентификация и аутентификация. Контроль доступа. Политики безопасности.	ЛР
4.	Безопасность ПО, инфраструктуры и облака	Архитектура безопасных сетей, сегментация, IDS/IPS, журналирование и мониторинг.	ЛР
5.	Безопасность ПО, инфраструктуры и облака	Безопасная разработка ПО: Secure SDLC, SAST/DAST, анализ зависимостей, секретов.	ЛР
6.	Безопасность ПО, инфраструктуры и облака	Облачная/контейнерная безопасность и DevSecOps: IAM, политика образов и кластера.	ЛР
7.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	Угрозы LLM и чат-ботов: jailbreak, prompt-injection, insecure output handling. Обзор OWASP LLM Top-10.	ЛР
8.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	RAG: архитектура и угрозы – poisoning, джамминг, утечки; защита источников и векторных БД; верификация цитат.	ЛР
9.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	Моделирование угроз для ИИ-сервисов: STRIDE/LINDDUN, регламенты ответов, запрет опасных действий.	ЛР
10.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	Фреймворки управления рисками ИИ: NIST AI RMF 1.0, ISO/IEC 23894, соответствие и аудит.	ЛР
11.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	Социальные и этические аспекты ИИ-безопасности: предвзятости, защита	ЛР

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1	2	3	4
		прав и свобод, приватность.	
12.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	Практика реагирования и расследований инцидентов (в т.ч. для ИИ-сервисов): журналы, трассировка, воспроизводимость, отчётность.	ЛР

Примечание: ЛР – отчет/защита лабораторной работы, КП – выполнение курсового проекта, КР – курсовой работы, РГЗ – расчетно-графического задания, Р – написание реферата, Э – эссе, К – коллоквиум, Т – тестирование, РЗ – решение задач.

2.3.2 Занятия семинарского типа

Не предусмотрены.

2.3.3 Лабораторные занятия

№	Наименование раздела (темы)	Наименование лабораторных работ	Форма текущего контроля
1	2	3	4
1.	Основы ИБ и управление рисками	Политика безопасности организации: модель угроз, базовые меры, реестр рисков.	ЛР
2.	Основы ИБ и управление рисками	Криптопримитивы: хеш/подпись/шифрование, TLS-конфиг сервера, анализ сертификата.	ЛР
3.	Основы ИБ и управление рисками	Аутентификация и контроль доступа: проект RBAC/ABAC, MFA, секреты.	ЛР
4.	Основы ИБ и управление рисками	Логи и мониторинг: настройка журналов, разбор артефактов инцидентов.	ЛР
5.	Безопасность ПО, инфраструктуры и облака	Настройка межсетевого экрана и IDS (Suricata/Zeek): базовые сигнатуры и алерты.	ЛР
6.	Безопасность ПО, инфраструктуры и облака	SAST/DAST: настройка ZAP/Semgrep/Trivy, анализ уязвимостей веб-приложения.	ЛР
7.	Безопасность ПО, инфраструктуры и облака	Контейнерная безопасность: политика образов, сканирование, секреты, PSA/PSP.	ЛР
8.	Безопасность ПО, инфраструктуры и облака	Облачная безопасность: IAM-политики, сегментация, базовая KMS/шифрование.	ЛР
9.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	OWASP LLM Top-10 (LLM01–LLM04): моделирование и фиксация эффектов, разработка контрмер.	ЛР
10.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	Prompt-injection и jailbreak: постановка экспериментов, метрики успеха атаки, канареечные проверки.	ЛР
11.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	RAG-poisoning и джамминг: атаки на индекс/векторную БД; фильтрация и проверка источников.	ЛР
12.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	Structured/guarded prompting и «неисполняемые» инструменты: защита от completion-атак.	ЛР

№	Наименование раздела (темы)	Наименование лабораторных работ	Форма текущего контроля
1	2	3	4
13.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	LLM в безопасном окружении: аудит, трассировка, ограничения токенов, контроль стоимости и model-DoS.	ЛР
14.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	Threat-modeling для ИИ-сервиса: STRIDE/LINDDUN; угрозы/контрмеры; чек-лист соответствия NIST AI RMF 1.0.	ЛР
15.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	SOC-практикум: правила корреляции, алерты, инцидент-репорт по LLM-боту.	ЛР
16.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	Итоговая ЛР/мини-проект: защищённый RAG-чат-бот с фильтрацией контента, верификацией цитат и журналированием.	ЛР

Примечание: ЛР – отчет/защита лабораторной работы, КП – выполнение курсового проекта, КР – курсовой работы, РГЗ – расчетно-графического задания, Р – написание реферата, Э – эссе, К – коллоквиум, Т – тестирование, РЗ – решение задач.

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовая работа не предусмотрена. В качестве проекта на экзамен студенты выполняют проект по информационной безопасности по кейсу индустриального партнёра.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Изучение теоретического материала	Методические указания по организации самостоятельной работы студентов, утвержденные кафедрой вычислительных технологий, протокол №7 от 07.05.2025
2	Решение задач	Методические указания по организации самостоятельной работы студентов, утвержденные кафедрой вычислительных технологий, протокол №7 от 07.05.2025

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

– в форме аудиофайла,

– в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

– в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

В соответствии с требованиями ФГОС в программа дисциплины предусматривает использование в учебном процессе следующих образовательные технологии: чтение лекций с использованием мультимедийных технологий; метод малых групп, разбор практических задач и кейсов.

При обучении используются следующие образовательные технологии:

1 Технология коммуникативного обучения – направлена на формирование коммуникативной компетентности студентов, которая является базовой, необходимой для адаптации к современным условиям межкультурной коммуникации.

2 Технология разноуровневого (дифференцированного) обучения – предполагает осуществление познавательной деятельности студентов с учётом их индивидуальных способностей, возможностей и интересов, поощряя их реализовывать свой творческий потенциал. Создание и использование диагностических тестов является неотъемлемой частью данной технологии.

3 Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.

4 Информационно-коммуникационные технологии (ИКТ) – расширяют рамки образовательного процесса, повышая его практическую направленность, способствуют интенсификации самостоятельной работы учащихся и повышению познавательной активности. В рамках ИКТ выделяются 2 вида технологий:

5 Технология использования компьютерных программ – позволяет эффективно дополнить процесс обучения языку на всех уровнях.

6 Интернет-технологии – предоставляют широкие возможности для поиска информации, разработки научных проектов, ведения научных исследований.

7 Технология индивидуализации обучения – помогает реализовывать личностно-ориентированный подход, учитывая индивидуальные особенности и потребности учащихся.

8 Проектная технология – ориентирована на моделирование социального взаимодействия учащихся с целью решения задачи, которая определяется в рамках профессиональной подготовки, выделяя ту или иную предметную область.

9 Технология обучения в сотрудничестве – реализует идею взаимного обучения, осуществляя как индивидуальную, так и коллективную ответственность за решение учебных задач.

10 Игровая технология – позволяет развивать навыки рассмотрения ряда возможных способов решения проблем, активизируя мышление студентов и раскрывая личностный потенциал каждого учащегося.

11 Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.

Комплексное использование в учебном процессе всех вышеназванных технологий стимулируют личностную, интеллектуальную активность, развивают познавательные процессы, способствуют формированию компетенций, которыми должен обладать будущий специалист.

Основные виды интерактивных образовательных технологий включают в себя:

12 работа в малых группах (команде) – совместная деятельность студентов в группе под руководством лидера, направленная на решение общей задачи путём творческого

сложения результатов индивидуальной работы членов команды с делением полномочий и ответственности;

13 проектная технология – индивидуальная или коллективная деятельность по отбору, распределению и систематизации материала по определенной теме, в результате которой составляется проект;

14 анализ конкретных ситуаций – анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений;

15 развитие критического мышления – образовательная деятельность, направленная на развитие у студентов разумного, рефлексивного мышления, способного выдвинуть новые идеи и увидеть новые возможности.

Подход разбора конкретных задач и ситуаций широко используется как преподавателем, так и студентами во время лекций, лабораторных занятий и анализа результатов самостоятельной работы. Это обусловлено тем, что при исследовании и решении каждой конкретной задачи имеется, как правило, несколько методов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

Семестр	Вид занятия	Используемые интерактивные образовательные технологии	количество интерактивных часов
4	ЛР	Практические занятия в режимах взаимодействия «преподаватель – студент» и «студент – студент»	14
4	Л	Лекционные занятия	28
Итого			**42**

Примечание: Л – лекции, ПЗ – практические занятия/семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

Темы, задания и вопросы для самостоятельной работы призваны сформировать навыки поиска информации, умения самостоятельно расширять и углублять знания, полученные в ходе лекционных и практических занятий.

Подход разбора конкретных ситуаций широко используется как преподавателем, так и студентами при проведении анализа результатов самостоятельной работы.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4. Оценочные и методические материалы

Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «название дисциплины».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме оценки лабораторных работ к проекта к **экзамену**.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Контролируемые разделы (темы) дисциплины*	Код контролируемой компетенции (или ее части)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1.	Основы ИБ и управление рисками	AI S-1.1; LC-1.3; SS-1.1; УК-3.1	*ЛР 1. Политика безопасности: модель угроз, базовые меры, реестр рисков. (отчёт+защита)*	–
2.	Основы ИБ и управление рисками	ПК-4.1; ПК-4.2	*ЛР 2. Криптопримитивы: хеш/подпись/шифрование; TLS-конфиг; анализ*	–

			сертификата. (отчёт+защита)	
3.	Основы ИБ и управление рисками	ПК-4.1; ПК-4.2; AI S-1.1	*ЛР 3. Аутентификация и доступ: проект RBAC/ABAC, MFA, хранение секретов. (отчёт+защита)*	–
4.	Основы ИБ и управление рисками	ПК-4.1; ПК-4.2; LC-1.3	*ЛР 4. Логи и мониторинг: настройка журналов, разбор артефактов инцидента. (отчёт+защита)*	–
5.	Безопасность ПО, инфраструктуры и облака	ПК-4.1; ПК-4.2; AI S-1.1	*ЛР 5. Межсетевой экран и IDS (Suricata/Zeek): базовые сигнатуры и алерты. (отчёт+защита)*	–
6.	Безопасность ПО, инфраструктуры и облака	ПК-4.1; ПК-4.2; AI S-1.2; LC-1.3	*ЛР 6. SAST/DAST: ZAP/Semgrep/Trivy ; анализ уязвимостей веб-приложения. (отчёт+защита)*	–
7.	Безопасность ПО, инфраструктуры и облака	ПК-4.1; ПК-4.2; AI S-1.2	*ЛР 7. Контейнерная безопасность: политика образов, сканирование, секреты, PSA/PSP. (отчёт+защита)*	–
8.	Безопасность ПО, инфраструктуры и облака	ПК-4.1; ПК-4.2; AI S-1.2	*ЛР 8. Облако: IAM-политики, сегментация, базовая KMS/шифрование. (отчёт+защита)*	–
9.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	ML-5.1; AI S-1.1; SS-3.1	*ЛР 9. OWASP LLM Top-10 (LLM01–LLM04): моделирование эффектов, контрмеры. (отчёт+защита)*	–
10.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	ML-5.1; ML-5.2; AI S-1.1	*ЛР 10. Prompt-injection и jailbreak: эксперименты, метрики,*	–

			канареечные проверки. (отчёт+защита)	
11.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	ML-5.1; ML-5.2; AI S-1.2	*ЛР 11. RAG-poisoning/джамминг: атаки на индекс/векторную БД; фильтрация источников. (отчёт+защита)*	–
12.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	ML-5.1; ML-5.3	*ЛР 12. Guarded/structured prompting и «неисполняемые» инструменты. (отчёт+защита)*	–
13.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	ML-5.3; AI S-1.2; LC-1.3	*ЛР 13. Безопасное окружение LLM: аудит, трассировка, лимиты; защита от model-DoS. (отчёт+защита)*	–
14.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	AI S-1.1; AI S-1.2; LC-1.3	*ЛР 14. Threat-modeling для ИИ-сервиса: STRIDE/LINDDUN; чек-лист NIST AI RMF 1.0. (отчёт+защита)*	–
15.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	ПК-4.1; ПК-4.2; ML-5.3; AI S-1.1	*ЛР 15. SOC-практикум: корреляция событий, алерты, инцидент-репорт по LLM-боту. (отчёт+инцидент-репорт)*	–
16.	Безопасность ИИ-систем, чат-ботов, LLM и RAG	ML-5.1; ML-5.2; ML-5.3; AI S-1.1; AI S-1.2; ПК-4.3; УК-3.1	*ЛР 16. Итоговая мини-ЛР/мини-проект: защищённый RAG-чат-бот (фильтрация, верификация цитат, журналирование). (демо+защита)*	*Экзамен: письменная часть + защита мини-проекта (ЛР-16)*

Показатели, критерии и шкала оценки сформированных компетенций

Соответствие **<u>пороговому уровню</u>** освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **удовлетворительно/зачтено**):

УК-3 ***Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде***

	Понимает основные аспекты межличностных и групповых коммуникаций; соблюдает нормы и установленные правила поведения в организации Знает роли и правила коммуникаций. Умеет выполнять роль в подгруппе. Владеет базовыми правилами протоколирования договорённостей.
ПК-4	***Способен планировать необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции*** Использует современные инструментальные средства разработки баз данных, прикладного программного обеспечения и систем различного функционального назначения Применяет современные приемы работы с инструментальными средствами, поддерживающими создание программных продуктов и программных комплексов на базе языков программирования, баз данных и пакетов прикладных программ Знает основы Secure SDLC; типы уязвимостей; что такое SAST/DAST и анализ зависимостей/секретов. Умеет запустить типовой SAST/DAST, прочитать отчёт на уровне «критично/высоко/ниже». Владеет минимальной настройкой проверки безопасности в CI. Способен использовать методы эффективного управления командой при разработке, внедрении и сопровождении программных продуктов Знает роли в DevSecOps, артефакты релиза. Умеет составить чек-лист безопасного релиза. Владеет ведением простого риск-реестра.
SS-1	***Способен осуществлять свою трудовую деятельность с учетом определения корректной роли ИИ в различных процессах, критического анализа последствий применения ИИ-технологий, этических принципов*** Понимает, что качество обучающей выборки существенно определяет этико-социальные аспекты функционирования ИИ. Может выявить очевидные несоответствия между задачей для ИИ и обучающей выборкой. Знает основные виды предвзятостей и рисков контента. Умеет описать риски PII и «небезопасных» ответов LLM. Владеет базовой процедурой эскалации сомнительных случаев.
SS-3	***Способен осуществлять свою трудовую функцию с учетом неопределенности как сущностной черты функционирования искусственного интеллекта*** Распознаёт очевидные когнитивные искажения в работе человека (например, подтверждение своей точки зрения, слепое доверие алгоритму) обращает внимание на возможную предвзятость ИИ; воспринимает необходимость критически относиться к данным и результатам ИИ. Знает основные виды предвзятостей и рисков контента. Умеет описать риски PII и «небезопасных» ответов LLM. Владеет базовой процедурой эскалации сомнительных случаев.
LC-1	***Способен проводить анализ бизнес-проблем с оценкой перспективности применения ИИ для их решения, осуществлять постановку задачи машинного обучения, формулировать требования к системе ИИ*** Оценивает технические требования на основе формализованной постановки

Знает состав мини-набора документов безопасности.
Умеет оформить краткую политику ИБ/LLM-use.
Владеет шаблонами отчёта ЛР/инцидента.

ML-5 ***Способен разрабатывать и (или) применять методы повышения устойчивости, надежности, безопасности алгоритмов МО***

Обосновывает выбор и применение методов повышения устойчивости и надежности моделей с учётом специфики задачи, включая адаптацию моделей и использование подходов объяснимого ИИ и доверенного ИИ.
Учитывает риски атак и методы их противодействия.
Использует продвинутые методы дообучения моделей при подготовке данных, применяет методы повышения устойчивости моделей к атакам и искажениям данных
Проводит комплексный анализ результативности с учётом объяснимости моделей, устойчивости к атакам, использует методы доверенного ИИ для оценки.
Знает базовые угрозы LLM/RAG (prompt-inj., poisoning, model-DoS).
Умеет воспроизвести простую атаку и зафиксировать эффект.
Владеет элементарными мерами снижения риска (чёрные списки, базовые guardrails).

AI S-1 ***Способен управлять рисками в разработке систем ИИ, выстраивать управление безопасностью ИИ в компании с учетом этики ИИ***

Знает структуру NIST AI RMF и ISO/IEC 23894.
Умеет набросать минимальный threat-model (STRIDE-карточки).
Владеет сопоставлением рисков и простых контрмер.

Соответствие **базовому уровню** освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **хорошо/зачтено**)

УК-3 ***Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде***

Понимает основные аспекты межличностных и групповых коммуникаций; соблюдает нормы и установленные правила поведения в организации
Знает фасилитацию и способы разрешения конфликтов.
Умеет распределять роли и синхронизацию в команде 2–3 чел.
Владеет командной защитой ЛР/проекта.

ПК-4 ***Способен планировать необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции***

Использует современные инструментальные средства разработки баз данных, прикладного программного обеспечения и систем различного функционального назначения
Применяет современные приемы работы с инструментальными средствами, поддерживающими создание программных продуктов и программных комплексов на базе языков программирования, баз данных и пакетов прикладных программ
Знает OWASP Top-10 и OWASP LLM Top-10; модели доступа RBAC/ABAC.
Умеет настраивать Semgrep/ZAP/Trivy с исключениями и порогами; анализировать зависимости/секреты.
Владеет интеграцией проверок в CI/CD с артефактами и порогами «fail the build».
Способен использовать методы эффективного управления командой при

	разработке, внедрении и сопровождении программных продуктов Знает метрики процесса (coverage, MTTR). Умеет спланировать релиз с контрольными точками ИБ. Владеет ретроспективами по инцидентам (lessons learned).
SS-1	***Способен осуществлять свою трудовую деятельность с учетом определения корректной роли ИИ в различных процессах, критического анализа последствий применения ИИ-технологий, этических принципов*** Понимает, что качество обучающей выборки существенно определяет этико-социальные аспекты функционирования ИИ. Может выявить очевидные несоответствия между задачей для ИИ и обучающей выборкой. Знает privacy-by-design, минимизацию данных. Умеет выявлять проявления предвзятостей и предлагать смягчения. Владеет контент-политиками и ручной валидацией.
SS-3	***Способен осуществлять свою трудовую функцию с учетом неопределенности как сущностной черты функционирования искусственного интеллекта*** Распознаёт очевидные когнитивные искажения в работе человека (например, подтверждение своей точки зрения, слепое доверие алгоритму) обращает внимание на возможную предвзятость ИИ; воспринимает необходимость критически относиться к данным и результатам ИИ. Знает privacy-by-design, минимизацию данных. Умеет выявлять проявления предвзятостей и предлагать смягчения. Владеет контент-политиками и ручной валидацией.
LC-1	***Способен проводить анализ бизнес-проблем с оценкой перспективности применения ИИ для их решения, осуществлять постановку задачи машинного обучения, формулировать требования к системе ИИ*** Оценивает технические требования на основе формализованной постановки Знает структуру регламентов/инструкций. Умеет готовить разделы ТЗ/регламентов по ИБ. Владеет ведением живой документации (ADR, risk register).
ML-5	***Способен разрабатывать и (или) применять методы повышения устойчивости, надежности, безопасности алгоритмов МО*** Обосновывает выбор и применение методов повышения устойчивости и надежности моделей с учётом специфики задачи, включая адаптацию моделей и использование подходов объяснимого ИИ и доверенного ИИ. Учитывает риски атак и методы их противодействия. Использует продвинутые методы дообучения моделей при подготовке данных, применяет методы повышения устойчивости моделей к атакам и искажениям данных Проводит комплексный анализ результативности с учётом объяснимости моделей, устойчивости к атакам, использует методы доверенного ИИ для оценки. Знает защиты RAG (фильтрация источников, верификация цитат). Умеет проектировать канареечные проверки и метрики устойчивости. Владеет guarded/structured prompting и «неисполняемыми» инструментами.
AI S-1	***Способен управлять рисками в разработке систем ИИ, выстраивать управление безопасностью ИИ в компании с учетом этики ИИ*** Знает приоритизацию рисков (impact×likelihood).

Умеет формировать матрицу рисков и карту соответствия RMF/ISO.
Владеет аудит-трейлом решений LLM.

Соответствие **продвинутому уровню** освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **отлично/зачтено**):

УК-3 ***Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде***
Понимает основные аспекты межличностных и групповых коммуникаций; соблюдает нормы и установленные правила поведения в организации
Знает подходы к лидерству/делегированию.
Умеет управлять командой в инцидент-сценариях.
Владеет публичной защитой с технико-рисковым обоснованием.

ПК-4 ***Способен планировать необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции***
Использует современные инструментальные средства разработки баз данных, прикладного программного обеспечения и систем различного функционального назначения
Применяет современные приемы работы с инструментальными средствами, поддерживающими создание программных продуктов и программных комплексов на базе языков программирования, баз данных и пакетов прикладных программ
Знает тонкости криптоконфигов TLS/SSH и supply-chain риски.
Умеет писать собственные правила Semgrep/IDS.
Владеет построением «красной линии» в CI с SLA на исправления.
Способен использовать методы эффективного управления командой при разработке, внедрении и сопровождении программных продуктов
Знает практики policy-as-code.
Умеет внедрять риск-ориентированное планирование релизов.
Владеет настройкой security-gates и KPI процесса.

SS-1 ***Способен осуществлять свою трудовую деятельность с учетом определения корректной роли ИИ в различных процессах, критического анализа последствий применения ИИ-технологий, этических принципов***
Понимает, что качество обучающей выборки существенно определяет этико-социальные аспекты функционирования ИИ.
Может выявить очевидные несоответствия между задачей для ИИ и обучающей выборкой.
Знает сложные случаи предвзятостей и их влияние на безопасность.
Умеет организовывать HUM-in-the-loop контроль LLM.
Владеет комбинированными смягчениями (политики, модерация, верификация).

SS-3 ***Способен осуществлять свою трудовую функцию с учетом неопределенности как сущностной черты функционирования искусственного интеллекта***
Распознаёт очевидные когнитивные искажения в работе человека (например, подтверждение своей точки зрения, слепое доверие алгоритму) обращает внимание на возможную предвзятость ИИ; воспринимает необходимость критически относиться к данным и результатам ИИ.
Знает сложные случаи предвзятостей и их влияние на безопасность.

Умеет организовывать HUM-in-the-loop контроль LLM.
Владеет комбинированными смягчениями (политики, модерация, верификация).

LC-1 ***Способен проводить анализ бизнес-проблем с оценкой перспективности применения ИИ для их решения, осуществлять постановку задачи машинного обучения, формулировать требования к системе ИИ***

Оценивает технические требования на основе формализованной постановки
Знает требования к полноте/проверяемости документации.
Умеет интегрировать документацию в CI (doc-as-code).
Владеет сборкой комплекта для передачи в эксплуатацию/аудит.

ML-5 ***Способен разрабатывать и (или) применять методы повышения устойчивости, надежности, безопасности алгоритмов МО***

Обосновывает выбор и применение методов повышения устойчивости и надежности моделей с учётом специфики задачи, включая адаптацию моделей и использование подходов объяснимого ИИ и доверенного ИИ.
Учитывает риски атак и методы их противодействия.
Использует продвинутые методы дообучения моделей при подготовке данных, применяет методы повышения устойчивости моделей к атакам и искажениям данных
Проводит комплексный анализ результативности с учётом объяснимости моделей, устойчивости к атакам, использует методы доверенного ИИ для оценки.
Знает продвинутые техники защиты LLM/RAG (retrieval-policy, tool isolation).
Умеет подтверждать устойчивость к poisoning/jamming экспериментально.
Владеет прототипом защищённого LLM-сервиса с трассировкой и верификацией цитат.

AI S-1 ***Способен управлять рисками в разработке систем ИИ, выстраивать управление безопасностью ИИ в компании с учетом этики ИИ***

Знает требования регуляторов/стандартов и методики аудита.
Умеет выстраивать программу соответствия (governance) по RMF/ISO.
Владеет убедительными отчётами для внешнего аудита/партнёров.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Практические задания для лабораторных работ

ЛР-1. Политика безопасности: модель угроз, базовые меры, реестр рисков
Задание. Выбрать учебный сервис (веб-приложение или LLM-бот), провести инвентаризацию активов и DFD, описать модель нарушителя, составить реестр рисков (вероятность/ущерб/уровень), предложить базовые меры (пароли/MFA/RBAC/журналы).
Сдать. Политика ИБ (1–2 стр.), DFD-схема, реестр рисков (таблица), чек-лист базовых мер.
Компетенции. AI S-1.1; LC-1.3; SS-1.1; УК-3.1.

ЛР-2. Криптопримитивы и TLS-конфигурация: хеш/подпись/шифрование, сертификаты
Задание. Сгенерировать ключи (RSA/ECDSA), подписать и проверить файл; настроить TLS для тестового сервера (self-signed), проверить цепочку и набор шифров, зафиксировать рукопожатие.
Сдать. Набор ключей/сертификат, конфиг сервера, команды проверки (openssl), скриншоты рукопожатия, краткий отчёт.
Компетенции. ПК-4.1; ПК-4.2.

ЛР-3. Аутентификация и доступ: RBAC/ABAC, MFA, управление секретами
Задание. Спроектировать простую RBAC/ABAC-политику для учебного сервиса; подключить TOTP-MFA; организовать хранение секретов (варианты: env-файл/хранилище секретов) и ротацию.
Сдать. Политика доступа, демонстрация MFA (скрин), артефакты настройки секретов, отчёт.
Компетенции. ПК-4.1; ПК-4.2; AI S-1.1.

ЛР-4. Логи и мониторинг: журналы и артефакты инцидентов
Задание. Включить структурированное логирование (JSON), настроить уровни/форматы; собрать образцы журналов при норме/ошибках; выделить артефакты инцидента и составить таймлайн.
Сдать. Конфиг логирования, примеры логов, таймлайн инцидента, отчёт.
Компетенции. ПК-4.1; ПК-4.2; LC-1.3.

ЛР-5. Межсетевой экран и IDS (Suricata/Zeek): сигнатуры и алерты
Задание. Настроить базовые правила фильтрации (fw); развернуть Suricata/Zeek, создать ≥2 кастомные сигнатуры, сгенерировать трафик и зафиксировать алерты.
Сдать. Конфиги, правила, pcap/логи, отчёт.
Компетенции. ПК-4.1; ПК-4.2; AI S-1.1.

ЛР-6. Secure SDLC: SAST/DAST/SCA (ZAP, Semgrep, Trivy)
Задание. Прогнать Semgrep по учебному репозиторию, OWASP ZAP Baseline по стенду, Trivy по образу; сформировать план исправлений с приоритизацией.
Сдать. Отчёты инструментов, сводная таблица уязвимостей, план ремедиации.
Компетенции. ПК-4.1; ПК-4.2; AI S-1.2; LC-1.3.

ЛР-7. Контейнерная безопасность: образы, сканирование, секреты, Pod Security
Задание. Собрать минимальный образ (non-root, drop caps), просканировать его; продемонстрировать хранение секретов; настроить Pod Security (PSA) манифест.
Сдать. Dockerfile/манифесты, отчёт сканирования, описание секретов.
Компетенции. ПК-4.1; ПК-4.2; AI S-1.2.

ЛР-8. Облачная безопасность: IAM-политики, сегментация, KMS/шифрование
Задание. Создать принцип минимальных прав (IAM), настроить сегментацию сети/SG, включить шифрование объекта/тома (KMS) и проверить доступ.
Сдать. Политики/скриншоты настроек, отчёт о проверке.
Компетенции. ПК-4.1; ПК-4.2; AI S-1.2.

ЛР-9. OWASP LLM Top-10 (LLM01–LLM04): эксперименты и контрмеры
Задание. Составить чек-лист тестов под LLM01–LLM04, выполнить атаки на учебный LLM-бот, зафиксировать эффекты, предложить и проверить контрмеры.
Сдать. Тест-план, логи/примеры, таблица «атака→эффект→контрмера».
Компетенции. ML-5.1; AI S-1.1; SS-3.1.

ЛР-10. Prompt-injection и jailbreak: метрики атаки и канарейки
Задание. Спроектировать и провести серию prompt-injection/jailbreak-атак; ввести метрики успеха; реализовать «канареечные» проверки и сравнить до/после.
Сдать. Набор промптов, метрики и результаты, отчёт.
Компетенции. ML-5.1; ML-5.2; AI S-1.1.

ЛР-11. RAG-poisoning и джамминг: атаки на индекс/векторную БД
Задание. Подготовить малый корпус, внедрить «ядовитые» документы, оценить искажение ответа; реализовать фильтрацию источников/входной модерации.
Сдать. Корпус/индекс, отчёт с примерами и показателями.
Компетенции. ML-5.1; ML-5.2; AI S-1.2.

ЛР-12. Guardrails и structured prompting: защита от completion-атак
Задание. Настроить правила/шаблоны структурированного ответа, добавить пост-фильтры выдачи и проверки ссылок; измерить влияние на точность/безопасность.
Сдать. Конфигурации/политики, отчёт с метриками.
Компетенции. ML-5.1; ML-5.3.

ЛР-13. Аудит и трассировка LLM: логи, лимиты токенов, защита от model-DoS
Задание. Централизовать логи запросов/ответов, ввести квоты и rate-limit, оценить стоимость/токены, смоделировать model-DoS и показать защиту.
Сдать. Конфиги, примеры логов/дашбордов, отчёт.
Компетенции. ML-5.3; AI S-1.2; LC-1.3.

ЛР-14. Threat-modeling для ИИ-сервиса: STRIDE/LINDDUN, NIST AI RMF
Задание. Построить DFD, провести STRIDE или LINDDUN, сформировать матрицу рисков и чек-лист соответствия NIST AI RMF 1.0.
Сдать. DFD, таблицы угроз/рисков, чек-лист соответствия.
Компетенции. AI S-1.1; AI S-1.2; LC-1.3.

ЛР-15. SOC-практикум: корреляция событий и инцидент-репорт по LLM-боту
Задание. Сформулировать правила корреляции для типовых событий ИИ-сервиса, сымитировать инцидент и подготовить отчёт по стандартной структуре.
Сдать. Правила/запросы, отчёт об инциденте.
Компетенции. ПК-4.1; ПК-4.2; ML-5.3; AI S-1.1.

ЛР-16. Итоговый мини-проект: защищённый RAG-чат-бот
Задание. Реализовать прототип RAG-бота с фильтрацией контента, верификацией цитат, журналированием и базовыми guardrails; провести демонстрацию и самоаудит.
Сдать. Код/манифесты, демо-видео (до 3 мин), отчёт по безопасности.
Компетенции. ML-5.1; ML-5.2; ML-5.3; AI S-1.1; AI S-1.2; ПК-4.3; УК-3.1.

Пример лабораторной работы

Лабораторная работа № 2: «Криптопримитивы и TLS-конфиг: хеш/подпись/шифрование, сертификаты»

Тема. Практика базовых криптопримитивов и настройка защищённого канала связи (TLS) для учебного сервиса.

Цель

Освоить хеширование/подпись/шифрование на прикладных примерах и корректно настроить TLS-соединение (ключи, сертификаты, шифросuites, проверка).

Оборудование и ПО

ПК (Windows/Linux), OpenSSL, любой локальный веб-сервер (nginx/Apache) или простое приложение на Python/Node.js, Wireshark (по желанию).

Исходные данные

Текстовый файл (≥1 КБ) для демонстрации хеша/подписи; локальный DNS-алиас/localhost для тестового сервера.

Задание

1. Хеш-функции. Вычислить SHA-256/512 от исходного файла; показать устойчивость к малым изменениям (бит-флип).
2. Цифровая подпись. Сгенерировать пару ключей (RSA или ECDSA), подписать файл и проверить подпись. Объяснить разницу «подпись vs. хеш vs. HMAC».
3. Симметричное шифрование. Зашифровать файл алгоритмом AES-256-GCM, корректно сохранить/передать IV и тег аутентичности; расшифровать и сверить.
4. TLS-сертификат. Выпустить self-signed сертификат (или через локальный CA), настроить TLS на учебном сервере.
5. Проверка соединения. С помощью openssl s_client проверить цепочку, версию протокола, набор шифров; продемонстрировать отказ от слабых шифров и TLS < 1.2.
6. Наблюдение рукопожатия (опционально). Снять pcap и отметить ClientHello/ServerHello, выбор шифра, обмен ключами.
7. Безопасная конфигурация. Кратко обосновать выбранные кривые/шифросuites, параметры session resumption/OCSP stapling (если применимо).

Порядок выполнения

1. Подготовка среды и ключевых материалов.
2. Операции хеш/подпись/шифрование.
3. Выпуск сертификата и включение TLS.
4. Проверка и фиксация артефактов.

5. Итоги и рекомендации.

Контрольные вопросы

1. Чем отличаются SHA-256, HMAC-SHA-256 и цифровая подпись?
2. Как обеспечивается PFS в TLS 1.2/1.3 и почему это важно?
3. Что входит в проверку сертификата (CN/SAN, срок, цепочка, доверие)?
4. Почему небезопасны устаревшие шифросuites (RC4/3DES), и как их запретить?
5. Где хранить приватные ключи и как организовать их ротацию?

Отчёт

1. Цель/среда.
2. Команды/скрипты с комментариями.
3. Артефакты (хеш-значения, подписи, шифротекст/IV/tags, сертификат/конфиг, вывод s_client, pcap-фрагменты).
4. Итоги и рекомендации по hardening.

Критерии приёма

Зачтено. Выполнены все пункты задания; TLS настроен и проверен; представлены ключевые артефакты и корректно интерпретированы; отчёт структурирован.

Не зачтено. Отсутствует любой обязательный шаг (напр., верификация подписи или проверка TLS), ошибки в конфигурации, нет отчёта или артефактов.

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен)

Примеры вопросов для подготовки к экзамену

1. Триада CIA и риск-ориентированный подход: активы, нарушители, матрица impact×likelihood.
2. Криптопримитивы для инженера: хеш, HMAC, цифровая подпись; отличие «подпись vs. хеш vs. HMAC».
3. TLS 1.2/1.3: рукопожатие, PFS, выбор шифросьютов; почему отключают устаревшие алгоритмы.
4. Аутентификация и доступ: RBAC vs. ABAC, MFA/TOTP; принципы хранения и ротации секретов.
5. Secure SDLC / DevSecOps: SAST/DAST/SCA, секрет-скан; «красная линия» в CI/CD и пороги «fail the build».
6. Сетевой периметр и мониторинг: сегментация, WAF/IDS (Suricata/Zeek), журналирование и трассировка.
7. Контейнерная и облачная безопасность: минимальные образы, non-root, политика образов; IAM least privilege, сегментация сети, KMS-шифрование.
8. OWASP LLM Top-10: LLM01–LLM04 (prompt-injection/jailbreak, insecure output handling) и базовые guardrails.
9. RAG-угрозы: poisoning/джамминг, защита индекса/векторной БД, верификация цитат.
10. NIST AI RMF 1.0, ISO/IEC 23894: назначение, артефакты соответствия, связь с аудитом.
11. Инцидент-менеджмент: обязательные события логирования, корреляция, структура инцидент-репорта.
12. Threat modeling для ИИ-сервиса: STRIDE/LINDDUN, приоритизация мер.

Перечень компетенций (части компетенции), проверяемых оценочным средством:
УК-3.1; ПК-4.1; ПК-4.2; ПК-4.3; SS-1.1; SS-3.1; LC-1.3; ML-5.1; ML-5.2; ML-5.3; AI S-1.1; AI S-1.2.

В рамках подготовки к экзамену студенты выполняют в командах от 2 до 3 человек проект, составленный на примере задач индустриальных партнёров
1. Проект 1. DevSecOps-пайплайн с «красной линией» безопасности: SAST/DAST/SCA, secret-scan, пороги critical/high ⇒ fail, отчёт и план ремедиации.
2. Проект 2. Облачная/контейнерная безопасность учебного сервиса: IAM least privilege, сегментация сети, KMS-шифрование, политика образов, проверка журналирования/алертов.
3. Проект 3. Защита LLM/RAG-бота: guardrails, канареечные проверки, метрики успеха атак до/после, аудит и верификация цитат.

Реальные варианты тем индустриальных партнёров

1. **ПАО «Сбербанк» – «Security-gate для CI/CD учебного веб-сервиса»**: Semgrep (SAST), OWASP ZAP Baseline (DAST), Trivy/Grype (SCA/SBOM), secret-scan; артефакты и пороги «fail the build».

2. **ООО «АВА ЛАБ» – «LLM/RAG-бот: guardrails, канарейки и верификация цитат»**: чек-лист по OWASP LLM Top-10, канареечные запросы, снижение доли небезопасных ответов.

3. **ООО «СвязьРесурс-Кубань» – «Облако и сеть: IAM, сегментация и базовый SOC»**: IAM least privilege, VPC/SG/ACL, включение KMS-шифрования, базовые правила IDS и инцидент-репорт.

4.2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Методические рекомендации, определяющие процедуры оценивания на экзамене:

Процедура промежуточной аттестации проходит в соответствии с Положением о текущем контроле и промежуточной аттестации обучающихся ФГБОУ ВО «КубГУ».

Итоговой формой контроля сформированности компетенций у обучающихся по дисциплине является экзамен. Студенты обязаны сдать экзамен в соответствии с расписанием и учебным планом.

ФОС промежуточной аттестации состоит из заданий и результатов текущего контроля.

Форма проведения экзамена: письменно.

Преподавателю предоставляется право задавать студентам дополнительные вопросы по всей учебной программе дисциплины.

Результат сдачи экзамена заносится преподавателем в экзаменационную ведомость и зачетную книжку.

Оценивание уровня освоения дисциплины основывается на качестве выполнения студентом заданий текущего контроля и проекта.

Критерии оценки:

Оценивание уровня освоения дисциплины основывается на качестве выполнения студентом заданий текущего контроля и проекта, а также на результатах письменного экзамена. Применяется бально-рейтинговая система в логике РПД Жука (50 баллов за семестр: посещаемость лекций – до 5 б.; посещаемость лабораторных – до 5 б.; защита ЛР – до 32 б.; midterm-аттестация – до 8 б.). В середине семестра проходит аттестация;

студент аттестован, если написал письменную работу на оценку «3» и выше и набрал ≥15 б. к моменту аттестации. Механизм допуска к экзамену: к концу зачётной недели студент должен иметь аттестацию «3» и выше и ≥30 б. за работу в семестре. Перевод баллов: 35 б. → «3», 40 б. → «4», 45 б. → «5». Эта оценка учитывается на экзамене как одна из четырёх/пяти составляющих.

Итого на экзамене студент получает: (1) оценку за работу в семестре (по рейтингу), (2) оценку за проект (защита кейса), (3) оценку за аттестацию (midterm), (4) письменный билет: два ответа, учитываемые как две отдельные оценки. Вычисляется среднее арифметическое, округление – по правилам кафедры. Возможна дополнительная беседа/доп. задания по дисциплине для повышения оценки.

Методические рекомендации, определяющие процедуры оценивания лабораторных работ:

Процедура оценивания лабораторных работ проходит в соответствии с Положением о текущем контроле и промежуточной аттестации обучающихся ФГБОУ ВО «КубГУ».

По каждой лабораторной работе оформляется отчет. Отчеты сдаются на проверку руководителю в течение курса по мере их выполнения, и защищаются студентами в установленном порядке.

При защите отчета студенту могут быть заданы вопросы и дополнительные задания по сути лабораторной работы, в том числе из списка контрольных вопросов к данной лабораторной работе. При неудовлетворительной оценке знаний студента по теме данного отчета, студент возвращается к повторному изучению соответствующих материалов, после чего допускается к повторной защите. Неудовлетворительно выполненный отчет также возвращается на доработку.

Отчет должен содержать заголовок, тему лабораторной работы, цель, задание, индивидуальную тему, описание хода выполнения работы, необходимые прикладные материалы (схемы, макеты документов и т.п.), в соответствии с требованиями к содержанию, и выводы по работе.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4.3. Методические указания по организации вычислительной инфраструктуры

Условия применения:

- Курс рассчитан на студентов 4 курса.
- Наличие персональных компьютеров или ноутбуков с установленной операционной системой Linux (рекомендуется Ubuntu 22.04+) либо Windows с поддержкой виртуализации.
- Наличие установленного интерпретатора Python версии 3.9+ и базовых инструментов разработки.
- Доступ к средствам виртуализации и контейнеризации (Docker, Docker Compose), а также к тестовым облачным ресурсам (Yandex Cloud, иные учебные аккаунты).
- Возможность использования удалённых вычислительных ресурсов и виртуальных машин, предоставляемых индустриальными партнёрами, в том числе для выполнения лабораторных работ по сетевой, облачной и ИИ-безопасности.

Цели, задачи и ожидаемые результаты:

Цели:

- Обеспечить единообразную и контролируемую учебную инфраструктуру для выполнения лабораторных работ по безопасности информационных систем.
- Сформировать у обучающихся практические навыки работы с инструментами защиты, анализа уязвимостей, мониторинга и аудита.

Задачи преподавателя:

- Подготовка методических рекомендаций по развертыванию учебных стендов (локальных, виртуальных и облачных).
- Настройка базовых шаблонов лабораторных окружений для работ по криптографии, сетевой безопасности, Secure SDLC, контейнерной и облачной безопасности.
- Формирование типовых конфигураций для воспроизводимых экспериментов в области ИБ и безопасности ИИ-систем.

Ожидаемые результаты студентов:

- Умение самостоятельно разворачивать и настраивать учебный стенд для задач информационной безопасности.
- Навыки работы с инструментами журналирования, сканирования уязвимостей, контроля доступа и анализа инцидентов.
- Понимание принципов построения защищённой вычислительной инфраструктуры и безопасного вычислительного процесса.

Порядок реализации:

Настройка окружения:

- Для локальной работы: использование Linux-системы с установленными Docker, OpenSSL, Git, Python, а также средствами анализа безопасности (Semgrep, Trivy, OWASP ZAP в учебном режиме).
- Для удалённой и облачной работы: подключение к виртуальным машинам с преднастроенной сетевой изоляцией, IAM-ролями и журналированием.
- Для задач по безопасности ИИ-систем: использование тестовых LLM-сервисов и RAG-стендов с включённым логированием и ограничениями доступа.

Шаблоны работ:

Типовая структура лабораторного стенда:

1. Описание учебного сервиса или сценария
2. Модель угроз и активов
3. Конфигурация инфраструктуры
4. Настройка средств защиты
5. Проведение экспериментов (атаки/проверки)
6. Анализ результатов и выводы

Порядок проверки корректности:

Чек-лист работоспособности окружения:

- Доступность виртуальной машины или контейнерного окружения
- Корректная работа сетевых интерфейсов и сервисов
- Наличие журналов и артефактов безопасности
- Отсутствие критических ошибок при выполнении базовых сценариев защиты и тестирования

4.4. Методические указания по организации лабораторных работ

Условия применения:

- Наличие у обучающихся настроенного учебного стенда или доступа к облачным ресурсам.
- Доступ к методическим материалам, сценариям лабораторных работ и шаблонам отчётов.
- Использование системы контроля версий (Git) для фиксации конфигураций и результатов.

Цели, задачи и ожидаемые результаты:

Цели:

- Закрепить теоретические положения дисциплины «Безопасность информационных систем» на практических примерах.
- Сформировать навыки анализа угроз, настройки средств защиты и оценки рисков.

Задачи преподавателя:

- Разработка лабораторных работ, отражающих ключевые разделы дисциплины: ИБ, Secure SDLC, облачная и ИИ-безопасность.
- Подготовка учебных кейсов, приближённых к реальным сценариям эксплуатации ИС.
- Организация процедуры проверки отчётов и защиты лабораторных работ.

Ожидаемые результаты студентов:

- Умение применять средства защиты и анализа безопасности на практике.
- Навыки интерпретации результатов сканирования, журналирования и тестирования.
- Способность оформлять отчёты и аргументировать принятые решения по ИБ.

Порядок реализации:

План лабораторных работ:

ЛР1: Политика безопасности и модель угроз

ЛР2: Криптографические примитивы и TLS

ЛР3: Аутентификация, контроль доступа и секреты
ЛР4: Журналирование и мониторинг инцидентов
ЛР5: Сетевая безопасность и IDS
ЛР6: Secure SDLC и анализ уязвимостей
ЛР7: Контейнерная безопасность
ЛР8: Облачная безопасность и IAM
ЛР9–15: Безопасность ИИ-систем, LLM и RAG
ЛР16: Итоговый мини-проект по защите ИС или ИИ-сервиса

Пример индивидуального задания (ЛР4):

Задача: Настроить журналирование учебного сервиса, выявить и проанализировать признаки инцидента безопасности

Критерии оценки: полнота логирования, корректность анализа, обоснованность выводов

Контрольные вопросы:
- Назначение журналирования в ИБ
- Типы событий безопасности
- Роль логов при расследовании инцидентов

Критерии оценки:
Зачтено: все этапы выполнены корректно, выводы аргументированы.
Не зачтено: допущены принципиальные ошибки или отсутствует понимание механизмов защиты.

4.5. Методические указания по организации проектной деятельности студентов

Условия применения:
- Курс рассчитан на студентов 4 курса.
- Трудоёмкость проектной работы - 10–15 часов на команду.
- Наличие базовых навыков администрирования, программирования и понимания основ ИБ.

Цели, задачи и ожидаемые результаты:
Цели:
- Применить знания по безопасности информационных систем для решения комплексного практического кейса.
- Сформировать навыки командной работы и риск-ориентированного подхода.

Задачи преподавателя:
- Формирование тем проектов, соответствующих разделам дисциплины и уровню обучающихся.
- Подготовка технических заданий с чёткими критериями безопасности.
- Организация промежуточного и итогового контроля.

Ожидаемые результаты студентов:
- Опыт проектирования и анализа защищённой информационной системы.
- Умение презентовать результаты аудита и предложенные меры защиты.
- Навыки командной работы над ИБ-проектом.

Порядок реализации:
Примеры проектов:

- DevSecOps-пайплайн с контролем уязвимостей
- Защищённая облачная инфраструктура учебного сервиса
- Анализ угроз и защита LLM-чат-бота
- Проектирование системы журналирования и реагирования на инциденты

Пример ТЗ для проекта «Защищённый LLM-бот»:

- Описать архитектуру сервиса
- Выполнить моделирование угроз
- Реализовать базовые меры защиты
- Подготовить отчёт по соответствию требованиям ИБ
- Представить результаты в виде презентации

Критерии оценки:
Зачтено: проект соответствует ТЗ, продемонстрировано понимание принципов ИБ, выводы обоснованы.
Не зачтено: проект не соответствует требованиям или отсутствует понимание применённых мер безопасности.

Порядок проверки корректности:

- Соответствие проекта техническому заданию
- Обоснованность архитектурных и защитных решений
- Качество отчётных материалов и презентации

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

5.1 Основная литература:

1. Сидак, А. А.; Василенко, В. В.; Рыженко, С. В. Информационная безопасность. Физические основы технических каналов утечки информации: учебное пособие. — Москва: Директ-Медиа, 2022. — 128 с. — DOI: 10.23681/694670. — ISBN 978-5-4499-3327-0. — URL: https://biblioclub.ru/index.php?id=694670&page=book (дата обращения: 25.08.2025).
2. Грициенко, Н. В.; Чефранова, А. О.; Уривский, А. В.; Алабина, Ю. Ф. Система защиты информации ViPNet: учебное пособие. 2-е изд.; под ред. А. О. Чефрановой. — Москва: ДМК Пресс, 2023. — 385 с. — ISBN 978-5-89818-458-2. — URL: https://biblioclub.ru/index.php?id=703655&page=book_red&razdel=10487 (дата обращения: 25.08.2025).
3. Зайцев, А. П.; Мещеряков, Р. В.; Шелупанов, А. А. Технические средства и методы защиты информации: учебник. — Москва: Горячая линия – Телеком, 2021. — URL: https://biblioclub.ru/index.php?id=713902&page=book_red (дата обращения: 25.08.2025).
4. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — URL: https:// urait.ru/ bcode/512268.
5. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — URL: https://urait.ru/bcode/511998.

5.2 Дополнительная литература:

1. Webb, G. I.; Hyde, R.; Cao, H.; Nguyen, H. L.; Petitjean, F. Understanding Concept Drift [Электронный ресурс]. — arXiv:1704.00362, 2017. — URL: https://arxiv.org/pdf/1704.00362 (дата обращения: 25.08.2025).
2. Machine learning-based detection of concept drift in business processes [Электронный ресурс]. — SpringerLink, 2025. — DOI: 10.1007/s44311-025-00012-w. — URL: https://link.springer.com/article/10.1007/s44311-025-00012-w (дата обращения: 25.08.2025).
3. Adversarial machine learning: a review of methods, tools, and critical industry sectors [Электронный ресурс]. — SpringerLink, 2025. — DOI: 10.1007/s10462-025-11147-4. — URL: https://link.springer.com/article/10.1007/s10462-025-11147-4 (дата обращения: 25.08.2025).
4. A Comprehensive Guide to Explainable AI: From Classical Models to LLMs [Электронный ресурс]. — arXiv:2412.00800, 2024. — URL: https://arxiv.org/pdf/2412.00800 (дата обращения: 25.08.2025).
5. AI Development Life Cycle: A Comprehensive Guide [Электронный ресурс] // SmartDev. — URL: https://smartdev.com/ai-development-life-cycle-a-comprehensive-guide/ (дата обращения: 25.08.2025).
6. ATLAS — Adversarial Threat Landscape for Artificial-Intelligence Systems [Электронный ресурс] // MITRE. — URL: https://atlas.mitre.org/ (дата обращения: 25.08.2025).

5.3. Периодические издания:

1. IEEE Transactions on Big Data – научные статьи по обработке больших данных.
2. Journal of Big Data (SpringerOpen) – открытый журнал с исследованиями в области Big Data.
3. Big Data Research (Elsevier) – публикации по анализу, управлению и визуализации данных.
4. Data Science Journal (CODATA) – междисциплинарные исследования данных.
5. ACM Transactions on Knowledge Discovery from Data (TKDD) – методы извлечения знаний из больших данных.
6. https://openreview.net/forum?id=FMMF1a9ifL
7. https://openreview.net/forum?id=ElUrNM9U8c#discussion
8. https://openreview.net/forum?id=JoO6mtCLHD
9. https://aclanthology.org/2024.findings-emnlp.760/
10. https://aclanthology.org/2020.coling-main.588/
11. https://link.springer.com/chapter/10.1007/978-3-030-72113-8_30
12. https://link.springer.com/chapter/10.1007/978-3-031-42448-9_10
13. https://aclanthology.org/2024.findings-naacl.288/

5.4. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» http://www.biblioclub.ru/
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных

1. Scopus http://www.scopus.com/
2. ScienceDirect https://www.sciencedirect.com/
3. Журналы издательства Wiley https://onlinelibrary.wiley.com/
4. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/

5. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
6. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
7. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
8. База данных CSD Кембриджского центра кристаллографических данных (CCDC) https://www.ccdc.cam.ac.uk/structures/
9. Springer Journals: https://link.springer.com/
10. Springer Journals Archive: https://link.springer.com/
11. Nature Journals: https://www.nature.com/
12. Springer Nature Protocols and Methods: https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials: http://materials.springer.com/
14. Nano Database: https://nano.nature.com/
15. Springer eBooks (i.e. 2020 eBook collections): https://link.springer.com/
16. "Лекториум ТВ" http://www.lektorium.tv/
17. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Бесплатные образовательные ресурсы

1. Jupyter Notebook – интерактивные вычисления
2. Visual Studio Code – редактор кода с поддержкой Python
3. Google Scholar/arXiv – доступ к научным публикациям

Ресурсы свободного доступа

1. КиберЛенинка http://cyberleninka.ru/;
2. Американская патентная база данных http://www.uspto.gov/patft/
3. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
4. Федеральный портал "Российское образование" http://www.edu.ru/;
5. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
6. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
7. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
8. Справочно-информационный портал "Русский язык" http://gramota.ru/;
9. Служба тематических толковых словарей http://www.glossary.ru/;
10. Словари и энциклопедии http://dic.academic.ru/;
11. Образовательный портал "Учеба" http://www.ucheba.com/;
12. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ

1. Электронный каталог Научной библиотеки КубГУ http://megapro.kubsu.ru/MegaPro/Web
2. Электронная библиотека трудов ученых КубГУ http://megapro.kubsu.ru/MegaPro/UserEntry?Action=ToDb&idb=6
3. Среда модульного динамического обучения http://moodle.kubsu.ru
4. База учебных планов, учебно-методических комплексов, публикаций и конференций http://infoneeds.kubsu.ru/
5. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;

6. Электронный архив документов КубГУ http://docspace.kubsu.ru/
7. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

5.5 Публикации конференций A*

1. Tim Menzies, Oussama Elrawas, Jairus Hihn, Martin Feather, Ray Madachy, and Barry Boehm. 2007. The business case for automated software engineering. In Proceedings of the 22nd IEEE/ACM International Conference on Automated Software Engineering (ASE '07). Association for Computing Machinery, New York, NY, USA, 303–312. https://doi.org/10.1145/1321631.1321676

2. Farzana Ahamed Bhuiyan and Akond Rahman. 2021. Characterizing co-located insecure coding patterns in infrastructure as code scripts. In Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering (ASE '20). Association for Computing Machinery, New York, NY, USA, 27–32. https://doi.org/10.1145/3417113.3422154

3. Michael Hilton, Timothy Tunnell, Kai Huang, Darko Marinov, and Danny Dig. 2016. Usage, costs, and benefits of continuous integration in open-source projects. In Proceedings of the 31st IEEE/ACM International Conference on Automated Software Engineering (ASE '16). Association for Computing Machinery, New York, NY, USA, 426–437. https://doi.org/10.1145/2970276.2970358

6. Методические указания для обучающихся по освоению дисциплины (модуля)

В рамках курса предусмотрено проведение лекционных занятий, на которых излагается систематизированный материал по разработке кроссплатформенных десктопных приложений. На лекциях рассматриваются основные концепции, современные подходы и инструменты, используемые для создания приложений, работающих на различных операционных системах. После каждой лекции рекомендуется выполнение практических заданий для закрепления изученного материала и освоения ключевых технологий.

Лабораторные занятия направлены на практическое освоение методов и инструментов разработки кроссплатформенных десктопных приложений. В ходе лабораторных работ студенты реализуют основные компоненты пользовательских интерфейсов, обеспечивают взаимодействие с файловой системой, используют средства для работы с сетью и базами данных. Для выполнения заданий используются популярные фреймворки и среды разработки, такие как Qt, Electron или аналогичные.

В самостоятельной работе студентам рекомендуется изучать официальную документацию к выбранным фреймворкам и инструментам, а также дополнительную литературу по проектированию и оптимизации десктопных приложений.

Важной частью курса является самостоятельная проектная работа, в рамках которой студент разрабатывает завершённое кроссплатформенное десктопное приложение для решения конкретной задачи (кейса), предложенной индустриальными партнёрами или преподавателем. Допускается выполнение проектов индивидуально или в командах до 3-х человек.

Кейс №1 (АВА ЛАБ – Fastboard desktop-клиент):
Задание: кроссплатформенный desktop-клиент (**Qt/PyQt/GTK**) для естественно-языковых запросов к Fastboard; визуализация отчётов (таблицы/графики); экспорт PDF/PNG; локализация; релизы под 2 ОС; пайплайн CI.

Минимум к зачёту: UI + визуализация + локализация + пакеты Win/Linux + артефакты CI.

Кейс №2 (СвязьРесурс-Кубань – desktop-генератор документов):
Задание: приложение (**Tkinter/PyQt**) с параметрической формой, предпросмотр DOCX/PDF, логирование; локализация; релизы 2 ОС; CI-сборка.
Минимум к зачёту: работоспособный предпросмотр и экспорт; две сборки; CI + инструкция пользователя.

Для студентов с ограниченными возможностями здоровья предусмотрены дополнительные индивидуальные консультации, на которых преподаватель подробно разъясняет сложные аспекты дисциплины, помогает адаптировать практические задания и обеспечивает специальные условия для освоения методов работы с системами искусственного интеллекта. Индивидуальный подход позволяет таким студентам полноценно участвовать в учебном процессе и достигать требуемых результатов обучения.

7. Материально-техническое обеспечение по дисциплине (модулю)

Виртуальные машины, кластер Managed Kubernetes и ресурсы GPU в облаке предоставляется индустриальным партнером ПАО «Сбербанк»:

№	Продукт	Параметры продукта	Кол-во	Кол-во конфигураций	Ед. изм.
1	Виртуальная машина	Виртуальная машина 10% vCPU 2 vCPU 4 RAM	1	60	Шт
		ОС Ubuntu 22.04	1		Шт
		Системный диск SSD	1		Шт
			10		Гб
		Аренда публичного IP	1		Шт
2	Виртуальная машина с GPU	Виртуальная машина с GPU NVIDIA® Tesla® V100 2 GPU 8 vCPU 128 ГБ RAM	1	1	Шт
		ОС Ubuntu_24.04	1		Шт
		Системный диск SSD	1		Шт
			2000		Гб
		Диск SSD	1		Шт
			4096		Гб
		Диск SSD	1		Шт
			4096		Гб
		Аренда публичного IP	1		Шт
3	K8S	Master node 8 vCPU 16 RAM	1	1	Шт

		Worker node 10% доля 4 vCPU 32 RAM	5		Шт
		Worker node SSD-NVME	64		Гб
		Аренда публичного IP	1		Шт
4	ML Inference Instance Type GPU	Время работы в месяц	40	1	Ч
		Инстанс 8 x NVIDIA® H100 NVLink PCIe 160 vCPU 1520 GB RAM	1		Шт
		Количество запросов к ML-моделям	1		Млн. Шт
		Кэш ML-моделей	160		Гб
5	LLM	Токены GigaChat 2 Max	50		Млн. Шт
		Токены Embeddings	400		Млн. Шт

Дополнительные облачные ресурсы предоставляются технологическим партнером Yandex Cloud.

№	Вид работ	Наименование учебной аудитории, ее оснащенность оборудованием и техническими средствами обучения
1.	Лекционные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения
2.	Лабораторные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, проектором, программным обеспечением
3.	Практические занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения
4.	Групповые (индивидуальные) консультации	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
5.	Текущий контроль, промежуточная аттестация	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
6.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

Примечание: Конкретизация аудиторий и их оснащение определяется ОПОП.