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
«02» июня 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.36 «Безопасность информационных систем»

Направление подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем

Направленность Искусственный интеллект и аналитика данных

Форма обучения очная

Квалификация бакалавр

Краснодар 2026

Рабочая программа дисциплины Безопасность информационных систем составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем

Программу составила:
В.И. Грищенко, ст. преподаватель КАДИИ
И.О. Фамилия, должность, ученая степень, ученое звание _____ подпись

Рабочая программа дисциплины утверждена на заседании центра искусственного интеллекта
протокол № 10 «14» мая 2026 г.
Заведующий кафедрой (разработчика)
А. В. Коваленко
_____
подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол № 3 от «15» мая 2026 г.
Председатель УМК факультета
Н. Ю. Добровольская
_____
подпись

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

Луценко Евгений Вениаминович, доктор экономических наук, кандидат технических наук, профессор кафедры компьютерных технологий и систем Федерального государственного бюджетное образовательное учреждение высшего образования «Кубанский государственный аграрный университет имени И.Т. Трубилина», e-mail: prof.lutsenko@gmail.com

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины

Цели определены государственным образовательным стандартом высшего образования и соотнесены с общими целями ООП ВО по направлению подготовки «Математическое обеспечение и администрирование информационных систем», в рамках которой преподается дисциплина.

Цель: Формирование у студентов навыков разработки требований к безопасности информационных систем с использованием основных алгоритмов криптографии и различных криптосистем шифрования.

1.2 Задачи дисциплины

- Изучить использование в своей практической деятельности различные алгоритмы шифрования;
- Освоение возможностей компьютерными технологиями в области персональной и сетевой безопасности;
- Приобретение навыков самостоятельного изучения специальной литературы по информационной безопасности;

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Безопасность информационных систем» относится к обязательной части учебного плана.

Данная дисциплина тесно связана с дисциплинами: «Алгебра и геометрия», «Основы программирования», «Параллельное и низкоуровневое программирование».

Материал курса является связкой между математикой, программированием и прикладными задачами, связанными с безопасностью информационных систем на предприятии. Знания, полученные в данной дисциплине, используются в ходе изучения курсов «Правовые основы оценки проектных решений», «Математические модели защиты информации» и др.

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

Роль 1: Data Analyst (Аналитик данных)

Задачи:

1. Статистический анализ, визуализация данных, предварительная обработка.
2. Создание прогнозных моделей
3. Построение аналитических моделей для поддержки бизнес-решений.

Роль 2: MLOps (Специалист по эксплуатации ИИ)

Задачи:

1. DevOps для ML.
2. Автоматизация, мониторинг ML-систем.
3. Операционное управление жизненным циклом ML-моделей.

Роль 3: AI PM (Менеджер проектов ИИ)

Задачи:

1. Управление ИИ-проектами от идеи до внедрения
2. Анализ бизнес-требований и постановка задач
3. Оценка эффективности и ROI ИИ-решений

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

Код и наименование индикатора*	Результаты обучения по дисциплине
УК 1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	
УК-1.2 Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	Знает методы и стратегии эффективного поиска информации. Умеет формулировать цели поиска и подбирать оптимальные источники информации. Анализировать и критически оценивать найденные данные. Владеет навыками использования цифровых ресурсов и специализированного программного обеспечения для поиска и обработки информации.
ОПК 4 Способен участвовать в разработке технической документации программных продуктов и программных комплексов	
ОПК 4.1 Обладает знаниями об основных стандартах, нормах и правил разработки технической документации программных продуктов и программных комплексов	Знает основные элементы технической документации (описания архитектуры, руководства пользователей, спецификации интерфейсов, инструкции по установке и развертыванию). Умеет создавать техническую документацию, соответствующую стандартам и требованиям заказчика. Владеет программами и сервисами для подготовки качественной технической документации (Word, LaTeX, Dia, PlantUML).
ОПК 4.2 Способен применять стандарты, нормы и правила при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла программных продуктов и программных комплексов	Знать международные и российские стандарты оформления технической документации (ISO, ГОСТ Р, отраслевые регламенты). Уметь применять стандарты и регламенты для эффективного сопровождения всех стадий разработки программных продуктов. Владеть практическим опытом работы с системами управления версиями и хранения документации (GitHub, Confluence, Jira Docs).
ОПК 6 Способен использовать в педагогической деятельности научные основы знаний в сфере информационно-коммуникационных технологий	
ОПК 6.2 Обосновывает выбор конкретной ИКТ-технологии для решения педагогической задачи	Знает особенности и возможности различных информационно-коммуникационных технологий (ИКТ), используемых в образовательном процессе. Умеет аргументированно обосновывать выбор технологии исходя из поставленных учебных целей и потребностей учащихся. Владеет техническими умениями работы с современными технологиями обучения (интерактивные доски, онлайн-платформы, виртуальная реальность и др.).
ML-5 Способен разрабатывать и (или) применять методы повышения устойчивости надежности безопасности алгоритмов машинного обучения	
ML-5.1 Обосновывает способы и варианты применения методов повышения устойчивости, надежности, безопасности алгоритмов машинного обучения задачах искусственного интеллекта, 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.
AI S-1.1 Выявляет и моделирует угрозы на всём жизненном цикле ИИ-систем, оценивает и приоритизирует риски	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.
AI S-1.2 Обеспечивает соответствие нормативным требованиям и принципам доверенного/этичного ИИ.	Выполняет базовые тесты устойчивости (noise, simple adversarial examples) в песочнице. Участвует в подготовке сценариев red-team-тестов по готовым шаблонам. Знает международные стандарты и фреймворки MITRE ATLAS; OWASP ML Sec Top 10; гайд «AI Red Teaming Regulations»
SS-1.1 Определяет ценностные предпосылки, когнитивные искажения, культурно-обусловленные предвзятости в данных, алгоритмах, постановке задач для ИИ	Понимает, что качество обучающей выборки существенно определяет этико-социальные аспекты функционирования ИИ.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

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

Вид учебной работы		Всего часов	Семестры (часы)
			7
Контактная работа, в том числе:		**54,3**	**54,3**
Аудиторные занятия (всего):		**50**	**50**
Занятия лекционного типа		**16**	16
Лабораторные занятия		**34**	34
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:		**18**	**18**
Проработка учебного (теоретического) материала		**12**	12
Выполнение индивидуальных заданий (типовой расчет)		**6**	6
Подготовка к текущему контролю			
Контроль:		**35,7**	**35,7**
Подготовка к экзамену		**35,7**	35,7
Общая трудоемкость	**час.**	**108**	**108**
	в том числе контактная работа	**54,3**	**54,3**
	зач. ед	**3**	**3**

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) дисциплины, изучаемые в 7 семестре

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Основы информационной безопасности	8	2		4	2
2.	Методы криптографической защиты данных	10	2		6	2
3.	Средства защиты персональных данных и конфиденциальной информации	8	2		4	2
4.	Обеспечение безопасности приложений и веб-сервисов	8	2		4	2
5.	Мониторинг и аудит безопасности информационных систем	14	4		6	4
6.	Организационные меры и регламенты обеспечения безопасности	8	2		4	4
7.	Практикум по защите ИИ-моделей и аналитических платформ	10	2		6	2
ИТОГО по разделам дисциплины		**68**	**16**		**34**	**18**
Контроль самостоятельной работы (КСР)		4				
Промежуточная аттестация (ИКР)		0,3				
Подготовка к текущему контролю		35,7				
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 информационной безопасности	Основы концепции защиты информации, модели угроз и уязвимости ИС, принципы построения защищенных информационных систем.	Вопросы к экзамену 1-5
2	Методы криптографической защиты данных	Алгоритмы шифрования и хеширования, асимметричные и симметричные методы шифрования, управление ключами, цифровая подпись и электронная идентификация.	Вопросы к экзамену 6-10
3	Средства защиты персональных данных и конфиденциальной информации	Законодательные основы защиты персональных данных, стандарты обработки конфиденциальной информации, механизмы анонимизации и деперсонализации данных.	Вопросы к экзамену 11-15
4	Обеспечение безопасности приложений и веб-сервисов	Типичные атаки на приложения и сервисы (SQL-injection, XSS, CSRF), средства и методики защиты серверных и клиентских частей ПО.	Вопросы к экзамену 16-20
5	Мониторинг и аудит безопасности информационных систем	Инструменты мониторинга сетевых атак и аномалий, системы обнаружения вторжений IDS / IPS, проведение аудитов безопасности, составление отчетов по инцидентам.	Вопросы к экзамену 21-25
6	Организационные меры и регламенты обеспечения безопасности	Политики безопасности организаций, внутренние процедуры управления рисками, сертификация и аттестация ИС согласно требованиям ГОСТ Р и ISO/IEC 27001.	Вопросы к экзамену 26-28
7	Практикум по защите ИИ-моделей и аналитических платформ	Особенности безопасности моделей машинного обучения и алгоритмов аналитики данных, методы противодействия атакам на AI-системы, организация защиты хранилищ данных и облачных сервисов.	Вопросы к экзамену 29-30

2.3.2 Занятия семинарского типа / лабораторные занятия

№	**Наименование раздела (темы)**	**Наименование лабораторных работ**	**Форма текущего контроля**
1	**2**	**3**	**4**
1	Основы информационной безопасности	1. Изучение основных принципов классификации угроз и уязвимостей информационных систем. 2. Проведение анализа рисков информационной безопасности предприятия с использованием методик SWOT-анализа и матрицы рисков.	Проверка домашнего задания
2	Методы криптографической защиты данных	3. Реализация простых симметричных алгоритмов шифрования и дешифровки сообщений (например, AES, DES).	Проверка домашнего задания

№	Наименование раздела (темы)	Наименование лабораторных работ	Форма текущего контроля
1	2	3	4
		4. Применение асимметричного метода RSA для реализации цифровой подписи и проверки подлинности документа.	
3	Средства защиты персональных данных и конфиденциальной информации	5. Создание и настройка механизма ограничения доступа к персональным данным на уровне реляционной СУБД (PostgreSQL, MySQL). 6. Моделирование процессов деперсонализации данных с применением техник анонимизации и псевдонимации.	Проверка домашнего задания
4	Обеспечение безопасности приложений и веб-сервисов	7. Исследование типичных атак SQL Injection и разработка мер противодействия (на примере PHP-приложения). 8. Моделирующая атака типа Cross-Site Scripting (XSS) и реализация защитных механизмов на стороне клиента и сервера.	Проверка домашнего задания
5	Мониторинг и аудит безопасности информационных систем	9. Настройка системы обнаружения вторжений Snort и анализ журналов подозрительных действий. 10. Использование инструмента Wireshark для перехвата пакетов сети и выявления возможных попыток несанкционированного доступа.	Проверка домашнего задания
6	Организационные меры и регламенты обеспечения безопасности	11. Разработка внутренней политики безопасности предприятия и создание плана реагирования на инциденты. 12. Аудит соответствия корпоративной ИТ-инфраструктуры стандартам информационной безопасности (ISO/IEC 27001, ФЗ-152).	Проверка домашнего задания
7	Практикум по защите ИИ-моделей и аналитических платформ	13. Исследование методов и технологий защиты ML-модель от атаки типа Adversarial Attacks. 14. Обнаружение и защита от утечек данных при обработке больших массивов аналитической информации (Data Leakage Detection and Prevention).	Проверка домашнего задания

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) – не предусмотрено

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	Проработка и повторение лекционного материала, материала учебной и научной литературы,	Методические указания для подготовки к лекционным и семинарским занятиям, утвержденные на заседании кафедры анализа данных и искусственного интеллекта факультета компьютерных технологий и

	подготовка к семинарским занятиям	прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 22.03.2023 г
2	Подготовка к текущему контролю	Методические указания для подготовки к лекционным и семинарским занятиям, утвержденные на заседании кафедры анализа данных и искусственного интеллекта факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 22.03.2023 г

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, применяемые при освоении дисциплины (модуля)

В соответствии с требованиями ФГОС программа дисциплины предусматривает использование в учебном процессе следующих образовательные технологии: чтение лекций с использованием мультимедийных технологий; лабораторные занятия.

С точки зрения применяемых методов используются как традиционные информационно-объяснительные лекции, так и интерактивная подача материала с мультимедийной системой. Компьютерные технологии в данном случае обеспечивают возможность разнопланового отображения алгоритмов и демонстрационного материала. Такое сочетание позволяет оптимально использовать отведенное время и раскрывать логику и содержание дисциплины.

Лабораторное занятие позволяет научить студента применять теоретические знания при решении и исследовании конкретных задач. Лабораторные занятия проводятся в компьютерных классах. Подход разбора конкретных ситуаций широко используется как преподавателем, так и студентами при проведении анализа результатов самостоятельной работы. Это обусловлено тем, что в процессе исследования часто встречаются задачи, для которых единых подходов не существует. Каждая конкретная задача при своем исследовании имеет множество подходов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

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

– 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:

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

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

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

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

– 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 решении каждой конкретной задачи имеется, как правило, несколько методов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

4. Оценочные и методические материалы

4.1 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

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

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме тестовых заданий, разноуровневых заданий, типовых расчетов и **промежуточной аттестации** в форме вопросов и заданий 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	Изучение основных принципов классификации угроз и уязвимостей информационных систем.	ОПК 6.2	ЛР№1	Отчёт по практике

2	Проведение анализа рисков информационной безопасности предприятия с использованием методик SWOT-анализа и матрицы рисков.	AI S-1.1	ЛР№2	Отчёт по практике
3	Реализация простых симметричных алгоритмов шифрования и дешифровки сообщений (например, AES, DES).	ML-5.1	ЛР№3	Отчёт по практике
4	Применение асимметричного метода RSA для реализации цифровой подписи и проверки подлинности документа.	ОПК 4.1	ЛР№4	Отчёт по практике
5	Создание и настройка механизма ограничения доступа к персональным данным на уровне реляционной СУБД (PostgreSQL, MySQL).	AI S-1.2	ЛР№5	Отчёт по практике
6	Моделирование процессов деперсонализации данных с применением техник анонимизации и псевдонимации.	AI S-1.2	ЛР№6	Отчёт по практике
7	Исследование типичных атак SQL Injection и разработка мер противодействия (на примере PHP-приложения).	ML-5.1	ЛР№7	Отчёт по практике
8	Моделирующая атака типа Cross-Site Scripting (XSS) и реализация защитных механизмов на стороне клиента и сервера.	ML-5.1	ЛР№8	Отчёт по практике
9	Настройка системы обнаружения вторжений Snort и анализ журналов подозрительных действий.	AI S-1.1	ЛР№9	Отчёт по практике
10	Использование инструмента Wireshark для перехвата пакетов сети и выявления возможных попыток несанкционированного доступа.	AI S-1.1	ЛР№10	Отчёт по практике
11	Разработка внутренней политики безопасности предприятия и создание плана реагирования на инциденты.	ОПК-4.1	ЛР№11	Отчёт по практике
12	Аудит соответствия корпоративной ИТ-инфраструктуры стандартам информационной безопасности (ISO/IEC 27001, ФЗ-152).	ОПК-4.2	ЛР№12	Отчёт по практике
13	Исследование методов и технологий защиты ML-модель от атаки типа Adversarial Attacks.	SS-1.1	ЛР№13	Отчёт по практике
14	Обнаружение и защита от утечек данных при обработке больших массивов аналитической информации	УК 1.2	ЛР№14	Отчёт по практике

	(Data Leakage Detection and Prevention).			

Показатели, критерии и шкала оценки сформированных компетенций

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **удовлетворительно /зачтено**)				
на пороговом уровне:				
1.	УК-1.2 Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	студент показывает начальные навыки анализа и поиска информации	ЛР	Вопрос к экзамену 1
2.	ОПК 4.1 Обладает знаниями об основных стандартах, нормах и правил разработки технической документации программных продуктов и программных комплексов	проявляется интерес к участию в дискуссиях	ЛР	Вопрос к экзамену 26
3.	ОПК 4.2 Способен применять стандарты, нормы и правила при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла программных продуктов и программных комплексов	знает основные стандарты, нормы и правила	ЛР	Вопрос к экзамену 15
4.	ОПК 6.2 Обосновывает выбор конкретной ИКТ-технологии для решения педагогической задачи	знает основные ИКТ-технологии для решения педагогической задачи	ЛР	Вопрос к экзамену 27
5.	ML-5.1 Обосновывает способы и варианты применения методов повышения устойчивости, надежности, безопасности алгоритмов машинного обучения задачах искусственного интеллекта, включая их преобразование и адаптацию к специфике задачи	знание и понимание базовых концепций	ЛР	Вопрос к экзамену 6
6.	AI S-1.1 Выявляет и моделирует угрозы на всём жизненном цикле ИИ-систем, оценивает и приоритизирует риски	поверхностное представление о рисках	ЛР	Вопрос к экзамену 9
7.	AI S-1.2 Обеспечивает соответствие нормативным требованиям и принципам доверенного/этичного ИИ.	ознакомлен с основными нормами	ЛР	Вопрос к экзамену 14
8.	SS-1.1 Определяет ценностные предпосылки, когнитивные искажения, культурно-обусловленные предвзятости в данных, алгоритмах, постановке задач для ИИ	осознаёт наличие предвзятости	ЛР	Вопрос к экзамену 16

Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **хорошо /зачтено**)				
на базовом уровне:				
1.	УК-1.2 Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	уверенно демонстрирует поиск и обработку информации	ЛР	Вопрос к экзамену 2
2.	ОПК 4.1 Обладает знаниями об основных стандартах, нормах и правил разработки технической документации программных продуктов и программных комплексов	уверенно оценивает нормах и правил разработки технической документации программных продуктов	ЛР	Вопрос к экзамену 18
3.	ОПК 4.2 Способен применять стандарты, нормы и правила при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла программных продуктов и программных комплексов	может применить знание стандарты, нормы и правила при оформлении технической документации на различных стадиях проектирования	ЛР	Вопрос к экзамену 14
4.	ОПК 6.2 Обосновывает выбор конкретной ИКТ-технологии для решения педагогической задачи	уверенно ориентируется в ИКТ-технологиях	ЛР	Вопрос к экзамену 11
5.	ML-5.1 Обосновывает способы и варианты применения методов повышения устойчивости, надежности, безопасности алгоритмов машинного обучения задачах искусственного интеллекта, включая их преобразование и адаптацию к специфике задачи	уверенное использование стандартных методов	ЛР	Вопрос к экзамену 7
6.	AI S-1.1 Выявляет и моделирует угрозы на всём жизненном цикле ИИ-систем, оценивает и приоритизирует риски	распознавание и оценка большинства рисков	ЛР	Вопрос к экзамену 10
7.	AI S-1.2 Обеспечивает соответствие нормативным требованиям и принципам доверенного/этичного ИИ.	последовательное соблюдение требований	ЛР	Вопрос к экзамену 15
8.	SS-1.1 Определяет ценностные предпосылки, когнитивные искажения, культурно-обусловленные предвзятости в данных, алгоритмах, постановке задач для ИИ	систематически выявляет и устраняет предвзятость	ЛР	Вопрос к экзамену 17
Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **отлично /зачтено**)				
на продвинутом уровне:				
1.	УК-1.2 Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	мастерски осуществляет глубокий анализ и интерпретацию информации	ЛР	Вопрос к экзамену 3
2.	ОПК 4.1 Обладает знаниями об основных стандартах, нормах и правил разработки технической документации программных	глубоко оценивает важность стандартов, норм и правил разработки технической документации программных	ЛР	Вопрос к экзамену 25

	продуктов и программных комплексов	продуктов и программных комплексов		
3.	ОПК 4.2 Способен применять стандарты, нормы и правила при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла программных продуктов и программных комплексов	мастерски знает основные нормы и правила при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла программных продуктов и программных комплексов	ЛР	Вопрос к экзамену 2
4.	ОПК 6.2 Обосновывает выбор конкретной ИКТ-технологии для решения педагогической задачи	мастерски обосновывает выбор конкретной ИКТ-технологии	ЛР	Вопрос к экзамену 4
5.	ML-5.1 Обосновывает способы и варианты применения методов повышения устойчивости, надежности, безопасности алгоритмов машинного обучения задачах искусственного интеллекта, включая их преобразование и адаптацию к специфике задачи	внедрение инновационных решений и глубокая экспертиза	ЛР	Вопрос к экзамену 8
6.	AI S-1.1 Выявляет и моделирует угрозы на всём жизненном цикле ИИ-систем, оценивает и приоритизирует риски	глубокое понимание и детальное прогнозирование потенциальных угроз инициативу	ЛР	Вопрос к экзамену 10
7.	AI S-1.2 Обеспечивает соответствие нормативным требованиям и принципам доверенного/этичного ИИ.	активный вклад в разработку и улучшение этических стандартов	ЛР	Вопрос к экзамену 30
8.	SS-1.1 Определяет ценностные предпосылки, когнитивные искажения, культурно-обусловленные предвзятости в данных, алгоритмах, постановке задач для ИИ	создаёт рекомендации и развивает подходы для снижения предвзятости	ЛР	Вопрос к экзамену 18

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

Зачетно-экзаменационные материалы для промежуточной аттестации

Примерный перечень вопросов для экзамена

Вопросы экзамена	Перечень компетенций (части компетенции
1. Дайте определение понятия «угроза информационной безопасности». Приведите классификацию угроз.	AI S-1.1
2. Какие основные категории объектов информационной безопасности существуют?	ОПК 4.2
3. Перечислите уровни иерархии информационной безопасности и поясните их взаимосвязь.	AI S-1.1
4. Что такое «управление рисками» в области информационной безопасности?	ОПК 6.2

5. Какова роль стандартов ISO/IEC 27001 и ГОСТ Р в обеспечении информационной безопасности?	AI S-1.2
6. Опишите различия между симметричными и асимметричными методами шифрования.	ML-5.1
7. Назовите известные вам симметричные алгоритмы шифрования и укажите область их применения.	ML-5.1
8. Чем отличается алгоритм RSA от эллиптических кривых в криптографии?	ML-5.1
9. Что такое цифровая подпись и зачем она применяется?	ML-5.1
10. Объясните принцип работы схемы электронной идентификации на основе открытого ключа.	ML-5.1
11. Расскажите о мерах по обеспечению конфиденциальности персональных данных.	ОПК 4.1
12. Что понимается под термином «деперсонализация данных»? Приведите пример.	AI S-1.2
13. Какие угрозы возникают при хранении и передаче конфиденциальной информации?	AI S-1.1
14. Какие правовые нормы регулируют защиту персональных данных в России?	ОПК 4.2
15. Почему важно соблюдать политику хранения и обработки данных сотрудников внутри компании?	ОПК-4.1
16. Какие типы атак возможны на веб-приложения и каким образом их предотвратить?	ML-5.1
17. Как защитить приложение от SQL инъекций?	ML-5.1
18. Для чего нужны cookies и сессии, и как обеспечить безопасность сессионных данных?	ОПК 4.2
19. Какой механизм обеспечивает предотвращение межсайтового скриптинга (XSS)?	ML-5.1
20. Охарактеризуйте технологию SSL/TLS и ее роль в защите передачи данных.	ML-5.1
21. Какие виды аудита информационной безопасности выделяют?	AI S-1.1
22. По какому принципу работают системы обнаружения вторжений (IDS)? Примеры таких систем.	AI S-1.1
23. Какое значение имеет мониторинг активности пользователей и ведение логов событий?	AI S-1.1
24. Назовите распространенные инструменты для сбора и анализа сетевого трафика.	AI S-1.1
25. Зачем проводить регулярный внутренний аудит системы безопасности?	ОПК 4.1
26. Как организовать процесс управления доступом к ресурсам предприятия?	ОПК-4.2
27. Что входит в состав документации по информационной безопасности?	ОПК 6.2
28. Раскройте понятие «репутационный риск» и способы минимизации такого риска.	AI S-1.2
29. В чем заключается ответственность персонала за нарушение требований информационной безопасности?	УК-1.2
30. Какие меры предусмотрены российским законодательством за нарушения правил обращения с персональными данными?	AI S-1.2

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

Методические рекомендации, определяющие процедуры оценивания лабораторных работ:

Оценка зависит от:

- **Качества реализации** (работоспособность кода, эффективность)
- **Анализа результатов** (интерпретация, сравнение методов)
- **Оформления и отчетности** (четкость, соответствие стандартам)

Уровень	Требования
Теоретическая подготовка (20%)	
Пороговый (3/5)	Приведены базовые формулы, но без глубокого объяснения.

Базовый (4/5)	Дано обоснование выбранных методов, ссылки на источники.
Продвинутый (5/5)	Сравнение альтернативных подходов, критика ограничений.
Практическая реализация (40%)	
Пороговый (3/5)	Код работает, но без обработки ошибок и оптимизации.
Базовый (4/5)	Чистый код с комментариями, тестами и визуализацией.
Продвинутый (5/5)	Использование векторных операций, сравнение нескольких методов.
Анализ результатов (30%)	
Пороговый (3/5)	Простые графики без интерпретации.
Базовый (4/5)	Сравнение с теоретическими ожиданиями (например, сходимость градиентного спуска).
Продвинутый (5/5)	Анализ влияния гиперпараметров, статистические выводы.
Оформление отчета (10%)	
Пороговый (3/5)	Есть введение, код и выводы.
Базовый (4/5)	Структурированный отчет с графиками и таблицами.
Продвинутый (5/5)	LaTeX-документ или Jupyter Notebook с интерактивными визуализациями.

4.3 Методические указания по организации лабораторных работ по дисциплине «Безопасность информационных систем»

---

1. Общие сведения

Образовательная программа: «Искусственный интеллект и аналитика данных»

Дисциплина: «Безопасность информационных систем»

Вид обеспечения: Проведение лабораторных работ

Условия применения:

Для успешного выполнения лабораторных работ необходимо обеспечить:

Программное обеспечение:

Средства виртуализации и эмуляции сетей:

- VirtualBox или VMware Workstation.
- Kali Linux (для выполнения специальных задач по кибербезопасности).

Среда разработки Python:

1) Python версии 3.x.
2) PyCharm Community Edition или Visual Studio Code с установленными модулями cryptography, OpenSSL, requests и др.

Антивирусные и защитные программы:

3) Antivirus (Kaspersky, Dr.Web, ESET NOD32 и аналогичные продукты).
4) Firewall (брандмауэр операционной системы или стороннее решение).

Утилиты и инструменты безопасности:

5) Wireshark (анализатор сетевого трафика).
6) Metasploit Framework (фреймворк для проведения тестов на проникновение).
7) John the Ripper (утилита для взлома паролей).
8) Burp Suite (средство для тестирования безопасности веб-приложений).

Аппаратное обеспечение:

- Компьютеры с ОС Windows/Linux, поддерживающие Python, доступ к высокоскоростному широкополосному интернету (желательно скорость загрузки от 10 Мбит/с и выше).
- Свободное пространство на жестком диске не менее 50 Гб.
- USB-накопители (для резервного копирования и переноса данных).
- Достаточные вычислительные ресурсы (CPU/GPU) для работы с нейросетевыми моделями

2. Цели, задачи и ожидаемые результаты выполнения лабораторных работ

2.1. Обоснование необходимости лабораторных работ

Лабораторные работы в данной дисциплине необходимы, поскольку:

a) **Практическая направленность:** Лабораторные работы направлены на приобретение студентами практических навыков, необходимых инженерам-разработчикам и администраторам информационных систем. Они помогают закрепить теорию и подготовиться к реальной производственной деятельности, поскольку безопасность информационных систем играет ключевую роль в современной экономике и управлении организациями.

b) **Формирование инженерного мышления:** Выполнение лабораторных работ способствует формированию инженерного подхода к решению задач. Студенты учатся ставить цели, планировать мероприятия по обеспечению безопасности, анализировать последствия ошибок и принимать эффективные решения. Этот опыт важен для дальнейшего развития профессионализма и успешной карьеры.

c) **Подготовка к реальным проектам:** Опыт, полученный в ходе лабораторных работ, позволит студентам успешно интегрироваться в рабочие группы предприятий и организаций, занимающихся разработкой и поддержкой информационных систем. Лаборатории формируют готовность к профессиональным вызовам, связанным с обеспечением информационной безопасности в сложных технологических системах.

2.2. Задачи лабораторных работ

1. **Освоение инструментов:**

Студенты должны научиться правильно настраивать и использовать современное программное обеспечение и инструменты для защиты информации, включая антивирусные программы, системы обнаружения и предотвращения вторжений, анализаторы сетевого трафика и инструменты криптографии.

2. **Применение математических методов:**

Необходимо освоить базовые криптографические алгоритмы и математические методы, обеспечивающие надёжность и целостность передаваемых данных. Будущие специалисты должны понимать принципы шифрования, хэширования и цифровую подпись, а также уметь реализовывать эти методы на практике.

3. **Интеграция методов:**

Одной из важнейших задач является интеграция различных методов и инструментов защиты информации в единый рабочий процесс. Студенты должны научиться объединять различные элементы защиты (сетевую безопасность, аутентификацию, шифрование) в единую стратегию обеспечения информационной безопасности предприятия.

2.3. Ожидаемые результаты

После выполнения лабораторных работ студенты смогут:

- грамотно организовывать процессы обеспечения информационной безопасности на предприятиях различного масштаба.
- повысить уровень осознанности относительно роли инженера в проектировании защищенных информационных систем.
- понимать механизмы и последствия угроз, атак и уязвимостей, встречающихся в реальных проектах.
- быть готовыми к дальнейшему профессиональному развитию и продолжению образования в области кибербезопасности.

2.4. Что необходимо для реализации лабораторных работ?

1) **Методические материалы:**

- Пошаговые инструкции по каждой теме.
- Примеры кода (Python).

2) **Техническая поддержка:**
- Настройка ПО на компьютерах.
- Доступ к облачным ресурсам (при необходимости).

3) **Контроль выполнения:**
- Отчеты по каждой работе.

Лабораторные работы в данной дисциплине позволяют студентам **перейти от теории к практике**, освоив ключевые инструменты информационной безопасности. Это формирует **навыки, необходимые для работы в области ИИ**.

Формат:
- Каждая работа включает **теоретическую справку, пошаговое руководство и задания для самостоятельного выполнения**.
- Рекомендуется **сочетание индивидуальной и групповой работы** (особенно в задачах оптимизации и гибридного моделирования).

Таким образом, предложенный план лабораторных работ обеспечит **системный подход к обучению** и подготовит студентов к решению реальных задач в области информационной безопасности.

3. Порядок реализации лабораторных работ

3.1. Задача №4: Разработка схемы динамического пароля. Электронная цифровая подпись

Цель: Научиться создавать ЭЦП.

Тема 4: Применение асимметричного метода RSA для реализации цифровой подписи и проверки подлинности документа

Пошаговая инструкция:

1. **Знакомство с методами:**
- Методы модификации схемы простых паролей
- Метод «запрос-ответ»
- Функциональные методы
2. **Базовые операции:**

Задания:

1. С использованием функциональных методов составить функцию

$$У=(X \bmod 100)*D+W,$$

***где X* – собственная дата рождения**,

записать их в отчет. Отчет (документ Microsoft Word), сохранить с вводом пароля из трех знаков.
2. Запрограммировать программу, предназначенную для демонстрации порядка постановки и проверки электронной цифровой подписи.
3. Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования набирается непосредственно в окне программы. Зашифровать исходное сообщение и подписать его на секретном ключе отправителя. Переслать зашифрованное и подписанное сообщение получателю.
4. Выполнить проверку правильности ЭЦП и восстановить исходный текст сообщения.
5. Сохранить в отчете экранные формы, демонстрирующие процесс генерации и распространения ключей; процесс шифрования исходного документа и постановки ЭЦП.

Итоговая структура каждой лабораторной работы:

1. **Теоретическая часть** (краткое описание методов).
2. **Пошаговые инструкции** (код + пояснения).
3. **Индивидуальные задания** (3–5 задач на самостоятельное выполнение).
4. **Контрольные вопросы** (например, *"В чем преимущество различных методов?"*).

Такой подход обеспечит **постепенное усложнение задач** и **интеграцию знаний** из разных тем.

Соответствие лабораторных работ и индикаторов компетенций

В таблице ниже представлено, как каждая лабораторная работа способствует формированию заявленных компетенций.

Компетенция	Соответствующие лабораторные работы	Обоснование
УК-1.2 Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	Л.Р. 2 Проведение анализа рисков информационной безопасности предприятия с использованием методик SWOT-анализа и матрицы рисков.	Задача анализа рисков включает сбор и систематизацию информации, а также выработку рекомендаций на основе проведенных исследований, что укрепляет навыки осуществления поиска необходимой информации и ее последующего анализа.
ОПК 4.1 Обладает знаниями об основных стандартах, нормах и правил разработки технической документации программных продуктов и программных комплексов	Л.Р. 9 Исследование типичных атак SQL Injection и разработка мер противодействия (на примере PHP-приложения).	В ходе лабораторной работы студенты создают технический отчёт, содержащий детальное описание проведённых исследований, найденных уязвимостей и предложенных мер противодействия. Эта деятельность соответствует процессу разработки технической документации, регламентированному международными и отечественными стандартами (ISO, ГОСТ Р, методология Agile и Scrum).
ОПК 4.2 Способен применять стандарты, нормы и правила при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла программных продуктов и программных комплексов	Л.Р. 11 Разработка внутренней политики безопасности предприятия и создание плана реагирования на инциденты.	Данная лабораторная работа требует создания внутренних нормативных документов, включая политику безопасности и планы реагирования на инциденты, что соответствует требованиям международного стандарта ISO/IEC 27001, посвящённого управлению информационной безопасностью.
ОПК 6.2 Обосновывает выбор конкретной ИКТ-технологии для решения педагогической задачи	Л.Р. 11 Настройка системы обнаружения вторжений Snort и анализ журналов подозрительных действий.	В данном лабораторном занятии используется система обнаружения вторжений Snort, специально предназначенная для отслеживания несанкционированных действий в компьютерных сетях. Выбор именно этой технологии обусловлен её популярностью среди профессионалов и наличием обширной базы примеров, что идеально подходит для учебного процесса.
ML-5.1 Обосновывает способы и варианты применения методов повышения устойчивости, надежности, безопасности алгоритмов машинного обучения задачах искусственного интеллекта, включая их преобразование и адаптацию к специфике задачи	Л.Р. 3 Реализация простых симметричных алгоритмов шифрования и дешифровки сообщений (AES, DES).	Внедрение и настройку алгоритмов шифрования студенты осуществляют, основываясь на знаниях и понимании принципов криптографии, что способствует овладению методами повышения устойчивости и надежности алгоритмов машинного обучения.
AI S-1.1 Выявляет и моделирует угрозы на всём жизненном цикле ИИ-	Л.Р. 7 Исследование типичных атак SQL Injection и разработка мер противодействия (PHP-приложение).	Атаки типа SQL инъекции представляют собой угрозу для информационных систем, и умение выявлять подобные атаки и строить меры защиты являются

Компетенция	Соответствующие лабораторные работы	Обоснование
систем, оценивает и приоритизирует риски		частью компетенции по выявлению и моделированию угроз.
AI S-1.2 Обеспечивает соответствие нормативным требованиям и принципам доверенного/этичного ИИ.	Л.Р. 12 Аудит соответствия корпоративной ИТ-инфраструктуры стандартам информационной безопасности (ISO/IEC 27001, ФЗ-152).	Проведение аудита и обеспечение соответствия установленным стандартам укрепляет навыки обеспечения нормативных требований и поддержания этичного поведения при использовании ИИ
SS-1.1 Определяет ценностные предпосылки, когнитивные искажения, культурно-обусловленные предвзятости в данных, алгоритмах, постановке задач для ИИ	Л.Р. 14 Обнаружение и защита от утечек данных при обработке больших массивов аналитической информации (Data Leakage Detection and Prevention).	Решение проблемы утечки данных помогает выявлять когнитивные искажения и предвзятости в алгоритмах, оказывая прямое воздействие на формирование компетенции в определении влияющих факторов и ценностных предпосылок в аналитических процессах.

Чек-лист для проверки выполнения лабораторных работ

Этот чек-лист поможет преподавателю и студентам убедиться, что все этапы работ выполнены корректно.

Общий чек-лист для всех лабораторных работ

1) Подготовка к работе

- Установлено необходимое ПО (Python с библиотеками).
- Проверена работоспособность среды (запуск примеров из документации).
- Изучены методические указания и теоретическая часть.

2) Выполнение заданий

- Код написан без синтаксических ошибок.
- Результаты вычислений соответствуют ожидаемым (проверка на тестовых данных).
- Для символьных вычислений проведена аналитическая проверка (например, ручной расчет зашифрованного текста).

3) Отчетность

Отчет содержит:

- Цель работы.
- Листинги кода с комментариями.
- Результаты вычислений (графики, таблицы, выводы).
- Ответы на контрольные вопросы.

Оформление соответствует стандартам (титульный лист, нумерация страниц).

Чек-листы по темам

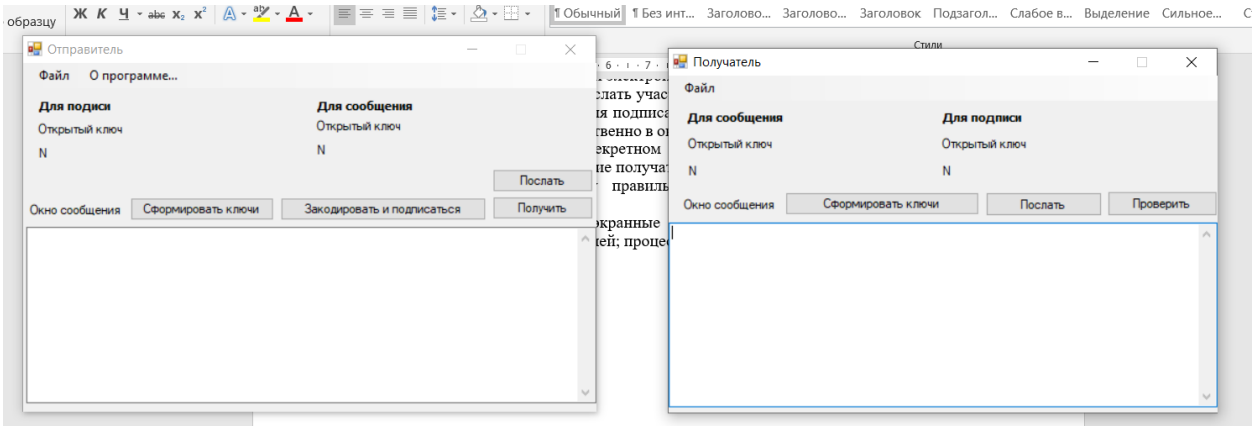
Тема 4: Применение асимметричного метода RSA для реализации цифровой подписи и проверки подлинности документа

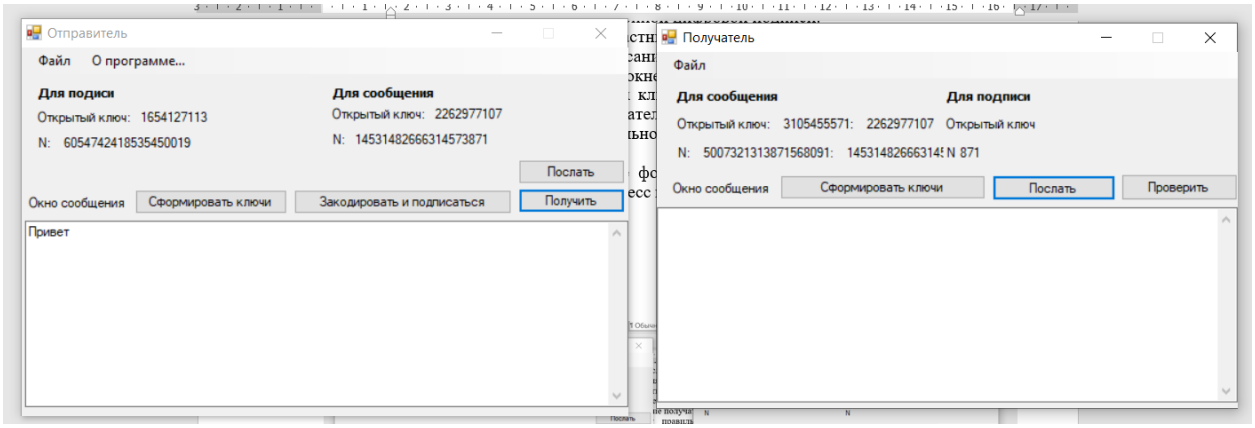
Критерии проверки:

- Переменные и функции заданы корректно.
- Упрощение выражений дает ожидаемый результат
- Программа реализована с помощью визуального интерфейса
- Все функции и кнопки интерфейса работают корректно

Пример проверки для задания 4:

Пример окон программы:





Итоговый контроль

- Все задания выполнены в срок.
- Отчет защищен (студент может объяснить любую часть кода).
- Результаты воспроизводимы (запуск на другом компьютере дает тот же вывод).

Преподаватель может использовать этот чек-лист при проверке работ, а также рекомендовать студентам применять его для самоконтроля. Этот подход минимизирует ошибки и обеспечит системное освоение компетенций.

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

5.1 Литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. - 2-е изд., перераб. и доп. - Москва : Юрайт, 2025. - 107 с. - URL: https://urait.ru/bcode/567915 (дата обращения: 05.03.2025). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-16388-9. - Текст : электронный. URL: http://212.192.134.46/MegaPro/UserEntry?Action=Link_FindDoc&id=281310&idb=0.
2. Чернова, Е. В. Информационная безопасность человека : учебник для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/566457 (дата обращения: 26.10.2025).
3. Илякова, И. Е. Коммерческая тайна : учебник для вузов / И. Е. Илякова. — Москва : Издательство Юрайт, 2025. — 139 с. — (Высшее образование). — ISBN 978-5-534-14712-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/568094 (дата обращения: 26.10.2025).
4. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567672 (дата обращения: 26.10.2025).
5. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный //

Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543351 (дата обращения: 26.10.2025).
6. Sun, X., Li, J., Kovalenko, A.V., Feng, W., Ou, Y. Integrating Reinforcement Learning and Learning From Demonstrations to Learn Nonprehensile Manipulation //IEEE Transactions on Automation Science and Engineering, 2023, 20(3), 1735–1744, DOI: 10.1109/TASE.2022.3185071, Q1
7. Petukhova, A.V.; Kovalenko, A.V.; Ovsyannikova, A.V. Algorithm for Optimization of Inverse Problem Modeling in Fuzzy Cognitive Maps. Mathematics 2022, 10, 3452. DOI: 10.3390/math10193452, Q1
8. Kirillova, E.; Kovalenko, A.; Urtenov, M. Study of the Current–Voltage Characteristics of Membrane Systems Using Neural Networks. AppliedMath 2025, 5, 10. https://doi.org/10.3390/appliedmath5010010
9. Polykovskiy, Daniil, et al. "Molecular sets (MOSES): a benchmarking platform for molecular generation models." Frontiers in pharmacology 11 (2020): 565644.
10. Khrabrov, Kuzma, et al. "$\nabla^ 2$ DFT: A Universal Quantum Chemistry Dataset of Drug-Like Molecules and a Benchmark for Neural Network Potentials." Advances in Neural Information Processing Systems 37 (2024): 36869-36889.

5.2. Периодические издания и конференции (A*):

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/

5.3. 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

Информационные справочные системы

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

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/

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

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал. В ходе лекционных занятий разбираются элементы теории и практики дискретной математики, приводятся примеры решения задач, проводится анализ наиболее распространенных ошибок. После прослушивания лекции рекомендуется выполнить упражнения, приводимые в аудитории для самостоятельной работы.

По курсу предусмотрено проведение лабораторных занятий, на которых дается прикладной систематизированный материал. В ходе занятий разбираются методы решений задач по темам. После занятия рекомендуется выполнить упражнения, приводимые для самостоятельной работы.

При самостоятельной работе студентов необходимо изучить литературу, приведенную в перечнях выше, для осмысления вводимых понятий, анализа предложенных

подходов и методов дискретной математики. При решении новой задачи студент должен уметь выбрать метод решения и его обоснование.

Важнейшим этапом курса является самостоятельная работа по дисциплине. В процессе самостоятельной работы студент приобретает навыки работы с дискретными объектами.

Используются активные, инновационные образовательные технологии, которые способствуют развитию общекультурных, общепрофессиональных компетенций и профессиональных компетенций обучающихся:

- проблемное обучение;
- разноуровневое обучение;
- проектные методы обучения;
- исследовательские методы в обучении;
- обучение в сотрудничестве (командная, групповая работа);
- информационно- коммуникационные технологии.

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

Учебно-методическим обеспечением курсовой работы студентов являются:

1. учебная литература;
2. нормативные документы ВУЗа;
3. методические разработки для студентов.

Самостоятельная работа студентов включает:

– оформление итогового отчета (пояснительной записки).
– анализ нормативно-методической базы организации;
– анализ научных публикации по заранее определённой теме;
– анализ и обработку информации;
– работу с научной, учебной и методической литературой,
– работа с конспектами лекций, ЭБС.

Для самостоятельной работы представляется аудитория с компьютером и доступом в Интернет, к электронной библиотеке вуза и к информационно-справочным системам.
Перечень учебно-методического обеспечения:

1. Основная образовательная программа высшего профессионального образования федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный университет» по направлению подготовки.
2. Положение о проведении текущего контроля успеваемости и промежуточной аттестации в федеральном государственном бюджетном образовательном учреждении высшего образования «Кубанский государственный университет».
3. Общие требования к построению, содержанию, оформлению и утверждению рабочей программы дисциплины Федерального государственного образовательного стандарта высшего профессионального образования.
4. Методические рекомендации по содержанию, оформлению и применению образовательных технологий и оценочных средств в учебном процессе, основанном на Федеральном государственном образовательном стандарте.
5. Учебный план основной образовательной программы по направлению подготовки.
6. Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

Важнейшим компонентом курса является самостоятельная проектная работа, в ходе которой студент разрабатывает законченное решение для решения задач (кейсов) индустриальных партнеров. Допускается выполнение проектов в командах.

Подход, определяющий установление соответствия кейсов ИП и УГТ (5-7), позволяет четко соотносить этапы развития технологии с вовлеченностью партнера и снижать риски при переходе от лабораторных испытаний к промышленному внедрению.

А. Применение безопасности информационных систем в кейсах ПАО «Сбербанк»

Кейс 1. Защита от SQL-инъекций в банковских приложениях

Описание: Разработчики Сбербанка сталкиваются с необходимостью защиты внутреннего банковского веб-приложения от атак SQL-инъекций, которые могут привести к хищению важных финансовых данных клиентов банка.

Цель: предотвратить атаку SQL-инъекции и повысить устойчивость приложения к подобным попыткам проникновения злоумышленников.

Технологии:

- Используются методы фильтрации вводимых данных и параметризованные запросы.
- Обзор используемого API и база данных для исключения потенциальных слабых мест.
- Современные инструменты статического анализа кода, такие как SonarQube.

Реализация6

- Команда разработчиков внедряет фильтры и валидаторы на стороне клиента и сервера.
- Оптимизация запросов с использованием подготовленных операторов.
- Интеграция автоматического тестирования на предмет уязвимостей к SQL-инъекциям.

Результат:

Количество успешных попыток SQL-инъекций сокращено практически до нуля. Улучшена общая безопасность приложения, повысился уровень доверия пользователей к банковской платформе.

Кейс 2. Организация централизованной системы обнаружения вторжений (Snort)

Описание: Банковская инфраструктура Сбербанка сталкивается с растущим числом попыток несанкционированного доступа и атак на внутренние системы.

Цель: Создать централизованную систему обнаружения вторжений (IDS), которая сможет оперативно реагировать на попытки взлома и минимизировать ущерб.

Технологии:

- Система Snort установлена на ключевых узлах инфраструктуры.
- Конфигурация правил для регистрации подозрительной активности.
- Централизованная консоль для просмотра и анализа инцидентов.

Реализация:

- Установка и настройка сенсоров Snort на границе периметра и внутреннем сегменте сети.
- Мониторинг и автоматическое оповещение службы безопасности о событиях.
- Периодический анализ журнала событий для выявления новых паттернов атак.

Результат

Система своевременно фиксирует около 95% случаев попыток вторжения, обеспечивая своевременное реагирование на угрозы и повышение общего уровня защиты банка.

Кейс 3. Защита персональных данных клиентов с помощью деперсонализации

Описание: Банк собирает большие объемы персональных данных клиентов, и необходим надежный механизм деперсонализации, чтобы исключить злоупотребления и уменьшить вероятность утечек данных.

Цель: Снизить риск нарушений приватности и соответствовать законодательству РФ о защите персональных данных.

Технологии:

- Введение строгих протоколов деперсонализации и псевдонимизации данных.

- Использование шифрованных каналов передачи данных.
- Хранение персональных данных раздельно от остальной бизнес-информации.

Реализация:

- Созданы процедуры деперсонализации на уровне реляционной СУБД (PostgreSQL).
- Постоянный контроль целостности и доступности зашифрованных данных.
- Регулярные аудиторские проверки для подтверждения правильности работы механизмов деперсонализации.

Результат:

Уровень защищённости персональных данных значительно повышен, количество инцидентов, связанных с нарушением конфиденциальности, сведено к минимуму.

Кейс 4. Противодействие атакам на основе кросс-сайт скриптов (XSS)

Описание: Клиенты банка сообщают о всплесках мошеннических действий через банковские онлайн-платформы, вызванных атаками типа XSS.

Цель: Повысить безопасность онлайн-банкинга путём усиления защиты против атак XSS.

Технологии:

- HTTP-заголовки Content Security Policy (CSP).
- Проверка ввода данных на стороне клиента и сервера.
- Обновление библиотек и компонентов, подверженных уязвимостям.

Реализация:

- Полноценная проверка веб-интерфейсов и мобильных приложений на наличие уязвимостей XSS.
- Добавлены заголовки CSP и активированы специальные фильтры.
- Разработаны инструкции для постоянного обновления и поддержки интерфейсов.

Результат:

Атаки XSS сократились почти на 90%, улучшилась стабильность и безопасность онлайн-сервиса, повысилась лояльность клиентов к банку.

Б. Применение безопасности информационных систем в кейсах компании AVA Lab

Кейсы для компании AVA Lab по разработке безопасности информационных систем

Кейс 1: Защита биометрических данных клиентов

Описание: Компания AVA Lab занимается обработкой большого объема биометрических данных пользователей (отпечатков пальцев, изображений лица), собираемых в рамках предоставляемых услуг по биометрии и верификации.

Цель: Обеспечить надежную защиту биометрических данных, исключив случаи несанкционированного доступа и возможного злоупотребления информацией.

Технологии:

- Асимметричное шифрование данных (RSA).
- Многократная проверка подлинности (multi-factor authentication).
- Хэширование и деперсонализация данных.

Реализация:

- Все данные хранятся в специально оборудованном закрытом контуре, отделённом от внешней сети.
- Биометрические записи защищены усиленными криптографическими системами.
- Данные пользователей деперсонализируются и дополнительно обрабатываются специальными сервисами для увеличения степени защиты.

Результат:

- Значительное снижение количества инцидентов с раскрытием биометрических данных.
- Высокая степень доверия среди клиентов благодаря гарантиям полной конфиденциальности и защищённости.

Кейс 2: Мониторинг и обнаружение аномальной активности в инфраструктуре

Описание: AVA Lab испытывает проблему с обнаружением скрытых угроз и нелегитимной активности в собственной инфраструктуре.

Цель: Раннее выявление аномального поведения и немедленное реагирование на инциденты, угрожающие безопасности данных.

Технологии

- Использование системы мониторинга ELK Stack (Elasticsearch, Logstash, Kibana).
- Анализ поведения с применением машинного обучения (anomaly detection).
- Интеграция системы мониторинга с защитой конечных точек (EDR).

Реализация

- Запущена централизованная система сбора и анализа логов (ELK Stack).
- Настроены правила поведенческого анализа для автоматической сигнализации о подозрительных действиях.
- Введён ежедневный отчёт о результатах мониторинга и реакция на тревожные события.

Результат

- Сокращение среднего времени реакции на инциденты безопасности примерно на 70%.
- Повышение общей осведомлённости сотрудников отдела безопасности и уменьшение числа ложных срабатываний.

Кейс 3: Защита инфраструктуры от DDoS-атак

Описание: Инфраструктура AVA Lab периодически подвергается мощным DDoS-атакам, приводящим к снижению производительности и недоступности сервиса.

Цель: Защитить инфраструктуру компании от массовых DDoS-атак и сохранить доступность критически важных сервисов.

Технологии

- Применение CDN (Content Delivery Network) с функцией фильтрации трафика.
- Балансировка нагрузки и динамическое масштабирование мощностей.
- Интеграция WAF (Web Application Firewall) для дополнительной защиты от атак.

Реализация

- Компания перешла на облачную инфраструктуру с балансировкой нагрузки и фильтрацией вредоносного трафика.
- Был введён многоуровневый фильтр для очистки входящих запросов.
- Регулярно проводится стресс-тестирование системы для оценки готовности к высоким нагрузкам.

Результат

- Время простоя вследствие DDoS-атак снизилось практически до нуля.
- Увеличенная производительность сервисов даже при значительных нагрузках позволила увеличить пропускную способность и поднять доверие клиентов.

Кейс 4: Защищённое хранение конфиденциальных медицинских данных

Описание: AVALab оказывает услуги по хранению и обработке медицинских данных пациентов, включая историю болезней и диагностические отчёты.

Цель: Обеспечить полную конфиденциальность и сохранность медицинской информации, соответствующую международному стандарту HIPAA и российскому закону о защите персональных данных.

Технологии

- Энд-то-энд шифрование (End-to-end encryption).
- Физическое разделение кластеров хранения данных.
- Двухфакторная аутентификация (2FA) и строгий контроль доступа.

Реализация:

- Медицинская информация хранится исключительно в зашифрованном виде.
- Права доступа строго контролируются и проверяются при каждом обращении к данным.

– Постоянный аудит процессов доступа и обработки данных, обеспечивается соответствие международным стандартам безопасности.

Результат:

– Ни одной зарегистрированной утечки медицинских данных.
– Полученный сертификат соответствия HIPAA подтверждает высокий уровень безопасности и соответствие мировым стандартам.

7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

7.1 Перечень информационно-коммуникационных технологий

1. Электронная почта mail.ru, yandex.ru
2. Yandex Browser
3. Система управления обучением Moodle – сдача работ

7.2 Перечень лицензионного и свободно распространяемого программного обеспечения

1. OpenOffice
2. GIT
3. Yandex Browser
4. Mozilla Firefox
5. Google Chrome
6. Python + Jupyter + Google Colab

8. Материально-техническое обеспечение по дисциплине (модулю)

№	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.	Групповые (индивидуальные) консультации	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
4.	Текущий контроль, промежуточная аттестация	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
5.	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.

№	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.

Примечание: Конкретизация аудиторий и их оснащение определяется ОПОП.