Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Брикс кафедра»

УТВЕРЖДЕНА:
на заседании кафедры
Протокол №15 от 18 марта 2025 г.

Рабочая программа дисциплины

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ / ARTIFICIAL INTELLIGENCE IN INFORMATION SECURITY»

Направление: 09.03.01 Информатика и вычислительная техника

Искусственный интеллект и компьютерные науки /Artificial Intelligence and Computer Science

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Усов Евгений Геннадьевич Дата подписания: 18.06.2025	Документ подписан простой электронной подписью Утвердил: Киреенко Анна Павловна Дата подписания: 19.06.2025	Документ подписан простой электронной подписью Согласовал: Афанасьев Александр Диомидович Дата подписания: 18.06.2025

Год набора – 2025

Иркутск, 2025 г.

1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Дисциплина «Искусственный интеллект в информационной безопасности / Artificial Intelligence in Information Security» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ДК-1 Способность осуществлять деятельность, находящуюся за пределами непосредственной профессиональной сферы	ДК-1.3

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ДК-1.3	Применяет технологии искусственного интеллекта в сфере информационной безопасности	**Знать** Основные концепции и методы искусственного интеллекта (ИИ), применяемые в информационной безопасности. Алгоритмы машинного обучения для обнаружения аномалий, классификации угроз и прогнозирования кибератак. Технологии обработки естественного языка (NLP) в анализе вредоносного ПО и фишинговых атак. Принципы работы нейросетевых моделей для защиты данных (например, генеративно-состязательные сети для создания и обнаружения deepfake). Этические и правовые аспекты применения ИИ в кибербезопасности, включая вопросы ответственности и приватности. **Уметь** Разрабатывать и настраивать модели машинного обучения для детектирования киберугроз (например, с использованием Python и библиотек Scikit-learn, TensorFlow). Применять ИИ-инструменты (например, SIEM с ИИ-аналитикой,

		платформы типа Darktrace) для мониторинга безопасности. Анализировать данные сетевого трафика и логи с помощью методов кластеризации и классификации. Оценивать эффективность ИИ-решений в защите информации (метрики точности, F1-score). Адаптировать готовые ИИ-модели под конкретные задачи ИБ (например, дообучение модели для распознавания новых типов вредоносного ПО). **Владеть** Навыками предобработки данных для ИИ-моделей (нормализация, feature engineering). Методами тестирования ИИ-систем на устойчивость к adversarial-атакам. Опытом интеграции ИИ-решений в существующие системы безопасности (например, связка IDS/IPS с ИИ-аналитикой). Умением интерпретировать результаты работы ИИ-моделей для принятия решений в ИБ. Способностью критически оценивать ограничения ИИ в кибербезопасности (риски ложных срабатываний, зависимость от качества данных).

2 Место дисциплины в структуре ООП

Изучение дисциплины «Искусственный интеллект в информационной безопасности / Artificial Intelligence in Information Security» базируется на результатах освоения следующих дисциплин/практик: «Защита информации / Information Security»

Дисциплина является предшествующей для дисциплин/практик: «Защита интеллектуальной собственности / Intellectual Property Protection»

3 Объем дисциплины

Объем дисциплины составляет – 3 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45

	минутам астрономического часа)	
	Всего	Семестр № 7
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	45	45
лекции	15	15
лабораторные работы	0	0
практические/семинарские занятия	30	30
Самостоятельная работа (в т.ч. курсовое проектирование)	63	63
Трудоемкость промежуточной аттестации	0	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет	Зачет

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 7

№ п/п	Наименование раздела и темы дисциплины	Виды контактной работы						СРС		Форма текущего контроля
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Введение в ИИ для кибербезопасности	1	3			1	6	1	10	Устный опрос
2	Машинное обучение для защиты данных	2	2			2	4	1	10	Устный опрос
3	Глубокое обучение в кибербезопасности	3	2			3	4	1	10	Устный опрос
4	NLP и анализ угроз	4	2			4	4	1	10	Устный опрос
5	Adversarial-атаки и защита от них	5	2			5	4	1	10	Устный опрос
6	ИИ для SOC и мониторинга	6	2			6	4	1	7	Устный опрос
7	Этические и правовые аспекты ИИ в ИБ	7	2			7	4	1	6	Устный опрос
	Промежуточная аттестация									Зачет
	Всего		15				30		63	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 7

№	Тема	Краткое содержание
1	Введение в ИИ для	Роль ИИ в современной информационной

	кибербезопасности	безопасности: преимущества и риски. Основные задачи ИИ в ИБ: обнаружение аномалий, прогнозирование атак, автоматизация SOC. Обзор технологий: машинное обучение (ML), глубокое обучение (DL), NLP. Кейсы: применение ИИ в антивирусах (Cylance), SIEM-системах (IBM QRadar).
2	Машинное обучение для защиты данных	Машинное обучение для защиты данных Алгоритмы ML в ИБ: Классификация (SVM, Random Forest) для детектирования угроз. Кластеризация (K-means) для выявления аномалий. Ансамбли моделей (XGBoost). Фичинг данных: выбор признаков для анализа сетевого трафика и логов. Проблема переобучения и методы её решения.
3	Глубокое обучение в кибербезопасности	Глубокое обучение в кибербезопасности Нейросети для ИБ: CNN (анализ вредоносного ПО), RNN (обработка последовательностей логов). GAN-атаки: генерация фейковых данных и защита от них. Autoencoders для обнаружения аномалий. Примеры: использование DeepInstinct для предотвращения zero-day угроз.
4	NLP и анализ угроз	NLP и анализ угроз Обработка текстов в ИБ: Анализ фишинговых писем (BERT, GPT). Классификация киберугроз по открытым источникам (OSINT). Токенизация и векторизация текста (Word2Vec,

		TF-IDF). Кейс: применение NLP в платформе Darktrace для анализа почтовых атак.
5	Adversarial-атаки и защита от них	Adversarial-атаки и защита от них Типы атак на ИИ-модели: FGSM, Poisoning, Evasion. Методы защиты: adversarial training, детекция аномальных входных данных. Устойчивость моделей к манипуляциям (Robust ML).
6	ИИ для SOC и мониторинга	Интеграция ИИ в Security Operations Center: Автоматизация инцидентов (SOAR). Анализ поведения пользователей (UEBA). Платформы: Splunk с ML, Microsoft Sentinel. Проблемы ложных срабатываний и их минимизация.
7	Этические и правовые аспекты ИИ в ИБ	Риски ИИ: дискриминация алгоритмов, утечки данных. Регулирование: GDPR, NIST AI RMF, этика использования ИИ. Будущие тренды: квантовый ИИ, объяснимый AI (XAI) для безопасности. Дебаты: можно ли полностью доверять ИИ в защите информации?

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 7

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Введение в ИИ для кибербезопасности	6
2	Машинное обучение для защиты данных	4
3	Глубокое обучение в кибербезопасности	4
4	NLP и анализ угроз	4
5	Adversarial-атаки и защита от них	4

6	ИИ для SOC и мониторинга	4
7	Этические и правовые аспекты ИИ в ИБ	4

4.5 Самостоятельная работа

Семестр № 7

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	63

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Дискуссия; Деловая игра; Кейс-метод; Лекция с ошибками; Мозговой штурм; Тренинг; Отдельные занятия по курсу могут проводиться в форме активного практического обучения: выездных занятий с посещением организаций и мероприятий для получения новых знаний и/или повторения материала на практике. При проведении таких занятий преподаватель выступает в качестве помощника и координатора процесса, передавая активную функцию обучения студентам. Он же регулирует процесс посредством подготовки специальных заданий, проведения консультаций, оценки знаний, умений и навыков, предоставления обратной связи. Помимо получения знаний активные практические занятия развивают коммуникативные навыки, учат студентов работать в команде, решать проблемы.

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по практическим занятиям

Практические занятия по данной дисциплине направлены на формирование у студентов навыков применения методов искусственного интеллекта для решения актуальных задач информационной безопасности. Основной формой контроля будет устный опрос, поэтому особое внимание следует уделять не только практическому выполнению заданий, но и умению аргументированно объяснять свои решения.

При подготовке к занятиям студентам рекомендуется внимательно изучить теоретические материалы по соответствующим темам, так как понимание принципов работы алгоритмов искусственного интеллекта является обязательным условием успешного выполнения практических задач. На каждом занятии будет проводиться краткое обсуждение ключевых концепций, после чего студенты приступят к решению практических задач.

Во время выполнения заданий важно не просто получить результат, но и понимать каждый этап работы: от предобработки данных до интерпретации результатов. Следует быть готовым объяснить, почему был выбран тот или иной алгоритм, какие параметры настраивались и как это повлияло на итоговую эффективность модели.

Особое внимание нужно уделять анализу возможных ограничений и уязвимостей применяемых методов. Студенты должны уметь критически оценивать полученные результаты, понимать риски ложных срабатываний и пропущенных угроз, а также возможные способы adversarial-атак на используемые модели.

При устном опросе будут оцениваться:

глубина понимания применяемых методов;

способность обосновать выбор конкретного подхода;

умение анализировать полученные результаты;

понимание ограничений и уязвимостей используемых технологий.

Рекомендуется вести конспект, в котором фиксировать ключевые моменты по каждой теме, возникающие вопросы и трудности при выполнении заданий. Это поможет при подготовке к устному опросу. Во время занятий следует активно участвовать в обсуждениях, задавать вопросы преподавателю и коллегам - это способствует более глубокому усвоению материала.

Важно помнить, что в области информационной безопасности недостаточно просто уметь применять инструменты - необходимо понимать их работу на концептуальном уровне, чтобы обеспечивать реальную защиту систем. Поэтому устный опрос будет направлен на проверку именно этого глубинного понимания, а не только практических навыков работы с конкретными реализациями алгоритмов.

5.1.2 Методические указания для обучающихся по самостоятельной работе:

Самостоятельная подготовка к практическим занятиям должна строиться на системном изучении теоретических основ и их последующем применении к решению практических задач. Начинайте с повторения ключевых концепций искусственного интеллекта, особое внимание уделяя тем разделам, которые непосредственно связаны с информационной безопасностью. Важно понимать не только как работают алгоритмы, но и почему они эффективны для конкретных задач защиты информации.

При подготовке к каждому занятию заранее ознакомьтесь с тематикой предстоящей работы. Проанализируйте рекомендуемую литературу, выделяя основные принципы и методы, которые будут использоваться на практике. Составляйте краткие конспекты с выделением ключевых терминов и понятий - это поможет вам увереннее чувствовать себя во время устного опроса.

Разработайте собственный глоссарий специальных терминов, включая как общепринятые понятия искусственного интеллекта, так и их специфическое применение в сфере информационной безопасности. Регулярно возвращайтесь к этому списку, проверяя и дополняя свои знания.

Для лучшего усвоения материала практикуйтесь в устном объяснении сложных концепций простыми словами. Попробуйте рассказать выученный материал воображаемой аудитории или записать свои объяснения на диктофон. Это развивает навыки четкого и логичного изложения мыслей, которые будут необходимы при устном опросе.

Обращайте особое внимание на взаимосвязь между различными методами искусственного интеллекта и конкретными задачами информационной безопасности. Анализируйте, почему определенные алгоритмы лучше подходят для обнаружения аномалий, классификации угроз или прогнозирования атак. Готовьтесь аргументированно отвечать на вопросы о преимуществах и ограничениях каждого подхода.

Разбирайте примеры реальных кейсов применения искусственного интеллекта в информационной безопасности. Анализируйте успешные реализации и случаи неудач, стараясь понять, какие факторы повлияли на результат. Это поможет вам развить критическое мышление и способность оценивать эффективность различных решений.

Практикуйтесь в решении типовых задач, которые могут быть предложены на занятиях. Старайтесь не просто получить правильный ответ, но и понять логику решения, чтобы суметь объяснить ее во время опроса. Обращайте внимание на типичные ошибки и сложные моменты, которые могут вызвать вопросы.

Развивайте навыки критического анализа, регулярно задавая себе вопросы: "Как это работает?", "Почему именно так?", "Какие есть альтернативы?". Такой подход поможет вам глубже понять материал и подготовиться к возможным уточняющим вопросам во время устного опроса.

Создавайте собственные схемы и ментальные карты, связывающие различные концепции искусственного интеллекта с задачами информационной безопасности. Визуализация поможет лучше запомнить сложные взаимосвязи и быстрее воспроизводить информацию при ответе.

Готовясь к занятиям, уделяйте равное внимание как теоретическим основам, так и их практическому применению. Помните, что на устном опросе вам может потребоваться не только воспроизвести изученный материал, но и продемонстрировать умение применять знания для решения нестандартных задач.

6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 7 | Устный опрос

Описание процедуры.

Устный опрос проводится с целью проверки глубины понимания студентами теоретических основ и их способности применять знания искусственного интеллекта к задачам информационной безопасности. Опрос проходит в форме диалога с преподавателем, где особое внимание уделяется не только воспроизведению изученного материала, но и умению анализировать, сравнивать и критически оценивать различные подходы.

При подготовке к опросу студентам следует сосредоточиться на понимании ключевых концепций, а не на механическом запоминании определений. Важно уметь объяснять принципы работы алгоритмов ИИ своими словами, приводить примеры их применения в сфере информационной безопасности, а также анализировать преимущества и ограничения каждого метода. Особую ценность представляет способность студента демонстрировать понимание взаимосвязей между различными технологиями ИИ и конкретными задачами защиты информации.

Во время опроса преподаватель может задавать как прямые вопросы по теории, так и предлагать решить практическую задачу "на бумаге", описав логику применения того или иного алгоритма. Студенту важно показать не только знание материала, но и способность

логически мыслить, выстраивать причинно-следственные связи, аргументированно отстаивать свою точку зрения.

Рекомендуется при ответе сначала кратко сформулировать основной тезис, затем привести необходимые пояснения и примеры, а в завершение сделать обобщающий вывод. Если вопрос вызывает затруднения, можно попросить уточняющие вопросы или время на обдумывание. Оценка выставляется с учетом полноты ответа, глубины понимания темы, логичности изложения и способности применять знания к практическим ситуациям.

Критерии оценивания.

Критерии оценки (дифференцированной):
оценка «отлично» выставляется студенту, если материал изложен грамотно, логически структурирован; работа содержательная и аргументированная; материал подкреплен знанием литературы и источников по теме вопроса; правильно использована юридическая терминология; присутствует четкое изложение дефиниций и классификаций, раскрытие основных признаков и характерных черт понятий, явлений, процессов; содержание работы в полной мере соответствует выбранной теме.
оценка «хорошо» выставляется при наличии незначительного нарушения логики изложения материала, допущено не более двух фактических или терминологических ошибок, присутствует неполнота или неточность в формулировках;
оценка «удовлетворительно» - существенное нарушение логики изложения материала, допущение более двух фактических или терминологических ошибок; содержание работы не в полной мере соответствует выбранной теме.
оценка «неудовлетворительно» - грубое нарушение логики изложения материала, допущение многочисленных фактических или терминологических ошибок; содержание работы не соответствует выбранной теме.

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	**Критерии оценивания**	**Средства (методы) оценивания промежуточной аттестации**
ДК-1.3	Для «знать»: точность воспроизведения теорий, способность объяснить работу алгоритмов. Для «уметь»: корректность реализации моделей, эффективность решения практических задач. Для «владеть»: глубина анализа результатов, адаптация технологий под реальные кейсы.	Опрос; Дискуссия; Доклады; Тестирование.

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 7, Типовые оценочные средства для проведения зачета по дисциплине

6.2.2.1.1 Описание процедуры

Недифференцированный зачет по данной дисциплине проводится в форме устного собеседования с целью проверки уровня освоения студентами теоретических основ искусственного интеллекта и их способности применять эти знания для решения практических задач информационной безопасности. Процедура предполагает подготовку студентом ответа на два вопроса билета: первый вопрос касается теоретических аспектов искусственного интеллекта, второй требует анализа практического кейса или решения прикладной задачи в области ИБ. Время на подготовку составляет 20-25 минут, в течение которых разрешается пользоваться своими конспектами лекций и семинарских занятий.

При ответе на теоретический вопрос студент должен продемонстрировать знание ключевых алгоритмов и методов искусственного интеллекта, их преимуществ и ограничений применительно к задачам информационной безопасности. Ответ должен содержать конкретные примеры применения технологий ИИ в различных областях ИБ, таких как обнаружение аномалий, классификация угроз, прогнозирование атак и автоматизация процессов безопасности. Особое внимание уделяется пониманию студентом современных тенденций и вызовов в области использования ИИ для защиты информации.

Практический вопрос требует от студента умения применять полученные знания к конкретным ситуациям. Необходимо проанализировать предложенный кейс кибератаки или задачи информационной безопасности, предложить решение с использованием методов искусственного интеллекта, обосновать выбор конкретных алгоритмов и спрогнозировать возможные результаты. Преподаватель может задавать уточняющие вопросы, направленные на проверку глубины понимания материала и способности студента адаптировать теоретические знания к практическим задачам.

Зачет считается пройденным, если студент продемонстрировал достаточный уровень знаний по обоим вопросам билета, смог аргументированно изложить свою позицию и показал способность применять теоретические знания к практическим ситуациям в области информационной безопасности. Результат зачета ("зачтено"/"не зачтено") объявляется сразу после завершения ответа. В случае получения оценки "не зачтено" студенту предоставляется возможность повторной сдачи в установленные учебным графиком сроки. Процедура зачета направлена на проверку не только знаний теоретического материала, но и способности студентов к профессиональной аргументации и решению актуальных задач информационной безопасности с использованием методов искусственного интеллекта.

Примерный перечень вопросов к зачету:

Дайте определение искусственного интеллекта в контексте информационной безопасности.

Назовите основные методы машинного обучения, применяемые в информационной безопасности.

В чем заключаются преимущества использования искусственного интеллекта для обнаружения киберугроз?

Опишите принципы работы нейронных сетей в задачах информационной безопасности.

Каковы основные этапы обработки данных для задач машинного обучения в ИБ?

Дайте определение adversarial-атак на модели машинного обучения.

Опишите методы защиты ИИ-систем от манипуляций входными данными.

Какие существуют подходы к обнаружению аномалий с использованием ИИ?

В чем особенности применения методов обработки естественного языка в информационной безопасности?

Опишите принципы работы систем автоматического реагирования на инциденты с использованием ИИ.

Каковы основные проблемы этического характера при использовании ИИ в ИБ?

Опишите примеры успешного применения ИИ для защиты от фишинговых атак.

В чем заключаются особенности использования глубокого обучения для анализа вредоносного ПО?

Каковы основные метрики оценки эффективности ИИ-моделей в информационной безопасности?

Опишите принципы работы рекомендательных систем в контексте ИБ.

Каковы современные тенденции развития ИИ в области информационной безопасности?

Опишите примеры использования ИИ для прогнозирования кибератак.

В чем заключаются особенности применения методов кластеризации в задачах ИБ?

Каковы основные требования к данным для обучения моделей ИИ в области безопасности?

Опишите принципы интеграции ИИ-решений в существующие системы безопасности.

Пример задания:

В чем заключаются особенности применения методов кластеризации в задачах ИБ?

Каковы основные требования к данным для обучения моделей ИИ в области безопасности?

6.2.2.1.2 Критерии оценивания

Зачтено	Не зачтено

Ответы на уровне минимальных требований Наличие существенных пробелов Затруднения с примерами	Серьезные пробелы в знаниях Неспособность ответить на основные вопросы Многочисленные ошибки

7 Основная учебная литература

1. Краковский, Ю. М. Методы и средства защиты информации : Учебное пособие для вузов / Ю. М. Краковский. – 1-е изд.. – Санкт-Петербург : Издательство ЛАНЬ, 2024. – 272 с. – EDN SWECXC.

8 Дополнительная учебная литература и справочная

1. Ерохин, В. В. Верификация информации и защита программного обеспечения в информационно-телекоммуникационных системах банка / В. В. Ерохин. – 2-е издание, переработанное и дополненное. – Москва : ООО Спутник+, 2025. – 183 с. – ISBN 5-277-01356-3. – EDN MYYDNF.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Свободно распространяемое программное обеспечение Microsoft Word

2. Свободно распространяемое программное обеспечение Power Point

12 Материально-техническое обеспечение дисциплины