МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Искусственный интеллект в информационной безопасности

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (в сфере связи, информационных и коммуникационных технологий)

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 4196
Подписал: заведующий кафедрой Желенков Борис Владимирович
Дата: 02.06.2026

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины являются:

- формирование компетенций по основным разделам теоретических и практических основ применения искусственного интеллекта при решении задач информационной безопасности;

- изучение методов построения систем информационной безопасности с использованием сильного интеллекта с учетом законодательных и нормативно-правовых требований.

Задачами дисциплины являются:

- изучение особенностей практического применения методов и систем искусственного интеллекта в задачах информационной безопасности;

- ознакомление с особенностями работы и проектирования современных интеллектуальных решений в рамках СКУД;

- изучение особенностей практического применения средств и систем информационной безопасности, использующих интеллектуальные решения;

- изучение интеллектуальных технологий обнаружения вирусов в современных системах антивирусной защиты;

- изучение интеллектуальных технологий в задачах управления доступом

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-3 - Способен на основании совокупности математических методов, физических законов и моделей разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

ОПК-6 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

ПК-5 - Способность формализовывать задачи управления безопасностью и анализировать риски функционирования компьютерных систем.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- основные математические методы, физические законы и модели для разработки, обоснования и реализации процедур решения задач профессиональной деятельности;

- основные методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

- способы формализации задач управления безопасностью и анализа рисков функционирования компьютерных систем.

Уметь:

- применять на практике основные математические методы, физические законы и модели для разработки, обоснования и реализации процедур решения задач профессиональной деятельности;

- применять на практике основные методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

- применять на практике способы формализации задач управления безопасностью и анализа рисков функционирования компьютерных систем

Владеть:

- навыками применения на практике основных математических методов, физические законов и моделей для разработки, обоснования и реализации процедур решения задач профессиональной деятельности;

- навыками применения на практике основных методов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

- навыками применения на практике способов формализации задач управления безопасностью и анализа рисков функционирования компьютерных систем

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов

	Всего	Семестр №10
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 80 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Основные направления применения ИИ в ИБ Рассматриваемые вопросы: - Обнаружение и предотвращение угроз; - Анализ кода и безопасная разработка - Анализ уязвимостей; - Автоматизация реагирования на инциденты; - Поведенческий анализ и прогнозирование атак; - Упракление доступом и идентификацией; - Анализ защищенности компании.
2	Технологии, используемые в ИБ с ИИ Рассматриваемые вопросы: - Машинное обучение - Глубокое обучение - Обработка естественного языка (NLP) - Генеративные модели - Реализация ИИ в системах с ИИ (SIEM, WAF, DLP, IDPS, ИИ-ассистенты)
3	Преимущества использования ИИ в ИБ Рассматриваемые вопросы: - Повышение эффективности обнаружения угроз - Автоматизация рутинных задач

№ п/п	Тематика лекционных занятий / краткое содержание
	- Адаптивная защита и обучение - Прогнозирование и предотвращение атак; - Анализ больших данных
4	Ограничения и риски применения ИИ в ИБ Рассматриваемые вопросы: - Зависимость от качества применяемых обучающих выборок и алгоритмов - Уязвимость к состязательным атакам - Этические и правовые проблемы - Фактор времени и динамичность угроз - Необходимость человеческого контроля
5	Регуляторные аспекты применения ИИ в ИБ Рассматриваемые вопросы: - Национальная стратегия развития искусственного интеллекта до 2030 года; - Приказ ФСТЭК России №117 от 11.04.2025 - Методика анализа защищенности информационных систем ФСТЭК от 25.11.2025
6	Регуляторные аспекты применения ИИ в ИБ (продолжение) Рассматриваемые вопросы: - Методика оценки угроз безопасности информационных систем ФСТЭК от 05.02.2021 - Раздел БДУ ФСТЭК по угрозам ИИ (атаки на ML-модели, атаки на RAG-системы, DoS через ИИ, API-атаки)
7	Применение ИИ для анализа уязвимостей Рассматриваемые вопросы: - Машинное обучение и машинное обучение с подкреплением - Глубокие нейронные сети - Обработка естественного языка (NLP) - Обнаружение аномалий - Инструменты и технологии: Solar appScreener (Ростелеком-Солар), VulnGPT, SentinelAI, DeepExploit, ZeroDay Sentinel
8	Анализ кода с помощью ИИ Рассматриваемые вопросы: - Выявление потенциальных уязвимостей - Статический анализ безопасности приложений (SAST) - Динамический анализ безопасности приложений (DAST) - Анализ сложности и дублирования кода - Сравнение с отраслевыми стандартами
9	Безопасная разработка с использованием ИИ Рассматриваемые вопросы: - Разработка руководящих принципов безопасного кодирования - Автоматическое создание патчей - Моделирование угроз и оценка рисков - Индивидуальные протоколы безопасности - Обнаружение аномалий в разработке - Проверка конфигурации и соответствия
10	Поведенческий анализ с использованием ИИ Рассматриваемые вопросы: - User and Entity Behavior Analytics (UEBA) - Машинное обучение и глубокое обучение (LSTM, графовые нейросети GNN) - Статистический анализ и машинное обучение
11	Прогнозирование атак с использованием ИИ Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- Классификационные модели (Decision Trees, Random Forest, SVM) - Нейросетевые архитектуры (RNN, LSTM) - Вероятностные методы (байесовские сети, марковские цепи) - Гибридные модели
12	Применение ИИ в СКУД Рассматриваемые вопросы: - Биометрическая идентификация и распознавание лиц - Поведенческий анализ и предиктивная аналитика - Адаптивное обучение - Интеграция с другими системами безопасности - Анализ и отчетность
13	Стандартизация при использовании ИИ Рассматриваемые вопросы: - ГОСТ Р 71476-2024 (ИСО/МЭК 22989:2022) - ГОСТ Р 71671-2024 - ГОСТ Р 71533-2024 - ГОСТ Р 71657-2024
14	Стандартизация при использовании ИИ (продолжение) Рассматриваемые вопросы: - ISO/IEC 22989:2022 - ISO/IEC 23053:2022 - ISO/IEC 42001:2023
15	Стандартизация при использовании биометрии Рассматриваемые вопросы: - ГОСТ Р 58624.5.2-2026 - ГОСТ Р 58230.1-2026 - ГОСТ Р 72502.1-2026 - ГОСТ Р 72502.4-2026 - ГОСТ Р 71414.1-2024 (ИСО/МЭК 19795-1:2021)
16	Стандартизация при использовании биометрии (продолжение) Рассматриваемые вопросы: - ГОСТ Р 58668.3-2021 - ГОСТ Р 71414.1-2024 - ISO/IEC 24713-1 - ISO/IEC 2382-37

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Технологии, используемые в ИБ с ИИ В результате выполнения практического задания студент получает навыки в выборе и оценке технологий ИИ на базе машинного и глубокого обучения, используемых в ИБ.
2	Технологии, используемые в ИБ с ИИ В результате выполнения практического задания студент получает навыки в выборе и оценке технологий ИИ, используемых в системах с ИИ (SIEM, WAF, DLP, IDPS, ИИ-ассистенты)
3	Преимущества использования ИИ в ИБ В результате выполнения практического задания студент получает навыки в выборе и оценке

№ п/п	Тематика практических занятий/краткое содержание
	технологий ИИ при автоматизации рутинных задач, адаптивной защите и обучении, прогнозировании и предотвращение атак.
4	Ограничения и риски применения ИИ в ИБ В результате выполнения практического задания студент получает навыки в оценке ограничений и рисков при применении технологий ИИ в ИБ.
5	Регуляторные аспекты применения ИИ в ИБ В результате выполнения практического задания студент получает навыки в практическом применении требований Приказа ФСТЭК России №117 от 11.04.2025 и методики анализа защищенности информационных систем ФСТЭК от 25.11.2025
6	Регуляторные аспекты применения ИИ в ИБ В результате выполнения практического задания студент получает навыки в практическом применении требований методики оценки угроз безопасности информационных систем ФСТЭК от 05.02.2021, раздела БДУ ФСТЭК по угрозам ИИ (атаки на ML-модели, атаки на RAG-системы, DoS через ИИ, API-атаки)
7	Применение ИИ для анализа уязвимостей В результате выполнения практического задания студент получает навыки в применении для анализа уязвимостей машинного обучения и машинное обучение с подкреплением, глубоких нейронных сетей, обнаружения аномалий.
8	Анализ кода с помощью ИИ В результате выполнения практического задания студент получает навыки в применении ИИ для анализа кода ПО при выявлении потенциальных уязвимостей, статическом анализе безопасности приложений (SAST), динамическом анализе безопасности приложений (DAST), анализе сложности и дублирования кода.
9	Безопасная разработка с использованием ИИ В результате выполнения практического задания студент получает навыки в применении ИИ при автоматическом создании патчей, моделировании угроз и оценке рисков, обнаружении аномалий в разработке.
10	Поведенческий анализ с использованием ИИ В результате выполнения практического задания студент получает навыки в поведенческом анализе с использованием ИИ (UEBA, машинное обучение и глубокое обучение (LSTM, GNN)
11	Прогнозирование атак с использованием ИИ В результате выполнения практического задания студент получает навыки в прогнозировании атак с использованием ИИ (классификационные модели, нейросетевые архитектуры, вероятностные методы)
12	Применение ИИ в СКУД В результате выполнения практического задания студент получает навыки в биометрической идентификации и распознавании лиц в системах ИБ с использованием ИИ
13	Применение ИИ в СКУД В результате выполнения практического задания студент получает навыки в поведенческом анализе и предиктивной аналитике в системах ИБ с использованием ИИ
14	Применение ИИ в СКУД В результате выполнения практического задания студент получает навыки в адаптивном обучении систем ИБ с использованием ИИ.
15	Стандартизация при использовании ИИ В результате выполнения практического задания студент получает навыки в подборе стандартов, регулирующих применение ИИ в системах ИБ

№ п/п	Тематика практических занятий/краткое содержание
16	Стандартизация при использовании биометрии В результате выполнения практического задания студент получает навыки в подборе стандартов, регулирующих применение биометрии в системах ИБ

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к практическим занятиям
2	Работа с лекционным материалом
3	Изучение вопросов для самостоятельной дополнительной проработки
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Диогенес Ю., Озкайя Э. Кибербезопасность. Стратегия атак и обороны. Издательство "ДМК Пресс", 2020 - 326с. – ISBN 978-5-97060-709-1	https://e.lanbook.com/book/131717 (дата обращения: 28.05.2026).- Текст электронный.
2	Мосолов А. С., Акинин Н. И. Компьютерные технологии и методы проектирования в сфере безопасности. Издательство "Лань", 2021 - 444с. – ISBN 978-5-8114-8034-0	https://e.lanbook.com/book/183115 (дата обращения: 28.05.2026)- Текст электронный.
3	Баланов А. Н. Защита информационных систем. Кибербезопасность: Учебное пособие для вузов. Издательство "Лань", 2025 - 280с. – ISBN 978-5-507-50467-1	https://e.lanbook.com/book/438971 (дата обращения: 28.05.2026)- Текст электронный.
4	Краковский Ю. М. Методы защиты информации. Издательство "Лань", 2021 - 236с. – ISBN 978-5-8114-5632-1	https://e.lanbook.com/book/156401 (дата обращения: 28.05.2026)- Текст электронный.
5	Тумбинская М.В., Петровский М.В. Защита информации на предприятии: учебное пособие. Издательство "Лань", 2020 - 184с. – ISBN 978-5-8114-4291-1	https://e.lanbook.com/book/130184 (дата обращения: 28.05.2026).- Текст электронный.
6	Прохорова О. В. Информационная безопасность и защита информации. Издательство "Лань", 2022 - 124с. – ISBN 978-5-8114-8924-4	https://e.lanbook.com/book/185333 (дата обращения: 28.05.2026).- Текст электронный.

7	Никифоров С. Н. Методы защиты информации. Защищенные сети, 2021 - 96с. – ISBN 978-5-8114-7907-8	https://e.lanbook.com/book/167186 (дата обращения: 28.05.2026).- Текст электронный.
8	Ермакова А.Ю. Методы и средства защиты компьютерной информации: учебное пособие. МИРЭА - Российский технологический университет, 2020.-223с	https://e.lanbook.com/book/163844
9	Леонтьев А. С. Защита информации: учебное пособие. МИРЭА - Российский технологический университет 2021.-79с	https://e.lanbook.com/book/18249 (дата обращения: 28.05.2026).- Текст электронный.

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

- Форум специалистов по информационным технологиям http://citforum.ru/
- Интернет-университет информационных технологий http://www.intuit.ru/
- Тематический форум по информационным технологиям http://habrahabr.ru/
- ЭБС "Лань" https://e.lanbook.com/book/

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

- Microsoft Windows
- Microsoft Office

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, лабораторных работ):

- компьютер преподавателя, рабочие станции студентов, мультимедийное оборудование, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Зачет в 10 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, доцент, к.н. кафедры
«Вычислительные системы и
квантовые коммуникации» С.В. Малинский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова