**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ**



**УТВЕРЖДАЮ**

Директор/Декан
факультета цифровых технологий
Шлаев Дмитрий Валерьевич

_____

_____

«___» _____ 20___ г.

# Рабочая программа дисциплины

# Б1.В.ДВ.02.02 Поведенческий анализ и мониторинг защищенности с использованием ИИ

09.04.03 Прикладная информатика

Искусственный интеллект в кибербезопасности

магистр

очная

Ставрополь, 2026

**1. Цель дисциплины**

Целью освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» является формирование у обучающихся теоретических знаний и практических навыков в области поведенческого анализа, мониторинга защищенности информационных систем, выявления и предупреждения опасных действий и условий, а также применения методов искусственного интеллекта для решения задач кибербезопасности.

**2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы**

Процесс изучения дисциплины направлен на формирование следующих компетенций ОП ВО и овладение следующими результатами обучения по дисциплине:

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Перечень планируемых результатов обучения по дисциплине |
|---|---|---|
| ПК-3 Способен применять методы машинного обучения и искусственного интеллекта для решения задач кибербезопасности | ПК-3.1 Проводит анализ безопасности компьютерных систем с использованием методов машинного обучения для выявления уязвимостей и оценки рисков | **знает**<br>методы машинного обучения для анализа безопасности компьютерных систем, выявления уязвимостей и оценки рисков<br>**умеет**<br>применять методы машинного обучения для выявления уязвимостей и оценки рисков безопасности<br>**владеет навыками**<br>навыками анализа безопасности компьютерных систем с использованием методов машинного обучения |
| ПК-3 Способен применять методы машинного обучения и искусственного интеллекта для решения задач кибербезопасности | ПК-3.2 Применяет методы инструментального мониторинга защищённости, включая алгоритмы ИИ для обнаружения и классификации аномалий и атак | **знает**<br>методы инструментального мониторинга защищенности и алгоритмы ИИ для обнаружения аномалий и атак<br>**умеет**<br>применять инструменты мониторинга и алгоритмы ИИ для обнаружения и классификации аномалий и атак<br>**владеет навыками**<br>навыками инструментального мониторинга защищенности и анализа аномалий с использованием ИИ |
| ПК-4 Способен администрировать средства защиты информации и обеспечивать безопасность информационных систем | ПК-4.1 Администрирует средства защиты информации прикладного и системного программного обеспечения (ОС, СУБД, приложения), настраивая политики безопасности и контролируя их соблюдение | **знает**<br>средства защиты информации, политики безопасности и порядок контроля их соблюдения<br>**умеет**<br>настраивать политики безопасности и администрировать средства защиты информации<br>**владеет навыками**<br>навыками администрирования средств защиты информации и контроля соблюдения политик безопасности |
| ПК-5 Способен проводить | ПК-5.1 Проводит инструментальный | **знает** |

| | | |
|---|---|---|
| инструментальный анализ защищённости, тестирование на проникновение и расследование компьютерных инцидентов | анализ защищённости и тестирование на проникновение информационных систем | методы инструментального анализа защищенности и тестирования на проникновение информационных систем<br>**умеет**<br>проводить инструментальный анализ защищенности и тестирование на проникновение информационных систем<br>**владеет навыками**<br>навыками применения инструментов анализа защищенности и тестирования на проникновение информационных систем |
| ПК-5 Способен проводить инструментальный анализ защищённости, тестирование на проникновение и расследование компьютерных инцидентов | ПК-5.2 Проводит экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов, анализируя цифровые следы и составляя заключения | **знает**<br>методы расследования компьютерных инцидентов, анализа цифровых следов и подготовки экспертных заключений<br>**умеет**<br>анализировать цифровые следы и составлять заключения по результатам расследования компьютерных инцидентов<br>**владеет навыками**<br>навыками экспертизы цифровых следов и документирования результатов расследования инцидентов |

**3. Место дисциплины в структуре образовательной программы**

Дисциплина «Поведенческий анализ и мониторинг защищенности с использованием ИИ» является дисциплиной части, формируемой участниками образовательных отношений программы.

Изучение дисциплины осуществляется в 4семестре(-ах).

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» студенты используют знания, умения и навыки, сформированные в процессе изучения дисциплин:

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Администрирование безопасных информационных систем

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Администрирование защищенных сетей

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Управление информационной безопасностью

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Прикладные системы искусственного интеллекта

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Научно-исследовательская работа

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Современные интеллектуальные системы и технологии

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Безопасность облачных технологий

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Проектирование автономных ИИ-агентов

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Технологии расследования компьютерных преступлений и инцидентов

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Технологии разработки защищенного ПО

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Атаки на системы искусственного интеллекта

Для освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» обучающийся должен иметь знания, умения и навыки, сформированные при изучении дисциплин: «Администрирование безопасных информационных систем», «Администрирование защищенных сетей», «Управление информационной безопасностью», «Безопасность облачных технологий», «Современные интеллектуальные системы и технологии», «Машинное обучение в кибербезопасности», «Прикладные системы искусственного интеллекта», «Технологии расследования компьютерных преступлений и инцидентов».Машинное обучение в кибербезопасности

Освоение дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» является необходимой основой для последующего изучения следующих дисциплин:

Обнаружение и анализ вредоносного программного обеспечения

Технологии непрерывной разработки и безопасности

Инструментальный анализ защищённости и тестирование на проникновение

**4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся**

Общая трудоемкость дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» в соответствии с рабочим учебным планом и ее распределение по видам работ представлены ниже.

| Семестр | Трудоемкость час/з.е. | Контактная работа с преподавателем, час | | | Самостоятельная работа, час | Контроль, час | Форма промежуточной аттестации (форма контроля) |
|---|---|---|---|---|---|---|---|
| | | лекции | практические занятия | лабораторные занятия | | | |
| 4 | 108/3 | 12 | 24 | | 72 | | За |
| в т.ч. часов: в интерактивной форме | | 4 | 6 | | | | |
| практической подготовки | | 12 | 24 | | 72 | | |

| Семестр | Трудоемкость час/з.е. | Внеаудиторная контактная работа с преподавателем, час/чел | | | | | |
|---|---|---|---|---|---|---|---|
| | | Курсовая работа | Курсовой проект | Зачет | Дифференцированный зачет | Консультации перед экзаменом | Экзамен |
| 4 | 108/3 | | | 0.12 | | | |

**5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

| № | Наименование раздела/темы | Семестр | Количество часов | | | | | Формы текущего контроля успеваемости и промежуточной аттестации | Оценочное средство проверки результатов достижения индикаторов компетенций | Код индикаторов достижения компетенций |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | всего | Лекции | Семинарские занятия | | Самостоятельная работа | | | |
| | | | | | Практические | Лабораторные | | | | |
| 1. | 1 раздел. Поведенческий анализ и мониторинг защищенности с использованием ИИ | | | | | | | | | |
| 1.1. | Основы поведенческого анализа в кибербезопасности | 4 | 24 | 6 | 18 | | 12 | | Тест | ПК-3.1, ПК-3.2, ПК-4.1, ПК-5.1, ПК-5.2 |
| 1.2. | Мониторинг защищенности информационных систем | 4 | 4 | 2 | 2 | | 12 | КТ 1 | Тест | ПК-3.1, ПК-3.2, ПК-4.1, ПК-5.1, ПК-5.2 |
| 1.3. | Применение искусственного интеллекта для выявления аномалий и атак | 4 | 4 | 2 | 2 | | 24 | | Тест | ПК-3.1, ПК-3.2, ПК-4.1, ПК-5.1, ПК-5.2 |
| 1.4. | Анализ результатов мониторинга и реагирование на инциденты | 4 | 4 | 2 | 2 | | 24 | КТ 2 | Тест | ПК-3.1, ПК-3.2, ПК-4.1, ПК-5.1, ПК-5.2 |
| | Промежуточная аттестация | За | | | | | | | | |
| | Итого | | 108 | 12 | 24 | | 72 | | | |
| | Итого | | 108 | 12 | 24 | | 72 | | | |

**5.1. Лекционный курс с указанием видов интерактивной формы проведения занятий**

| Тема лекции (и/или наименование раздел) (вид интерактивной формы проведения занятий)/ (практическая подготовка) | Содержание темы (и/или раздела) | Всего, часов / часов интерактивных занятий/ практическая подготовка |
|---|---|---|
| Основы поведенческого анализа в кибербезопасности | Понятие поведенческого анализа. Поведенческие признаки угроз и аномалий в информационных системах. Роль поведенческого анализа в мониторинге защищенности. | 6/6 |
| Мониторинг защищенности | Методы и средства мониторинга защищенности | 2/- |

| | | |
|---|---|---|
| информационных систем | информационных систем. Источники данных для мониторинга. Журналы событий, сетевой трафик и показатели безопасности. | |
| Применение искусственного интеллекта для выявления аномалий и атак | Методы машинного обучения и искусственного интеллекта в задачах кибербезопасности. Обнаружение аномалий, классификация атак и оценка рисков. | 2/- |
| Анализ результатов мониторинга и реагирование на инциденты | Интерпретация результатов поведенческого анализа и мониторинга защищенности. Подготовка выводов по выявленным угрозам. Использование результатов анализа при реагировании на инциденты. | 2/- |
| Итого | | 12 |

**5.2.1. Семинарские (практические) занятия с указанием видов проведения занятий в интерактивной форме**

| Наименование раздела дисциплины | Формы проведения и темы занятий (вид интерактивной формы проведения занятий)/(практическая подготовка) | Всего, часов / часов интерактивных занятий/ практическая подготовка | |
|---|---|---|---|
| | | вид | часы |
| Основы поведенческого анализа в кибербезопасности | Анализ типовых моделей поведения пользователей и систем. Выявление отклонений от нормального поведения. Построение базовой модели поведенческого профиля. | Пр | 18/4/18 |
| Мониторинг защищенности информационных систем | Настройка мониторинга событий безопасности. Анализ журналов событий и сетевой активности. Выявление признаков атак и нарушений политики безопасности. | Пр | 2/-/2 |
| Применение искусственного интеллекта для выявления аномалий и атак | Применение алгоритмов машинного обучения для анализа событий безопасности. Классификация аномалий и атак. Оценка результатов работы моделей ИИ. | Пр | 2/-/2 |
| Анализ результатов мониторинга и реагирование на инциденты | Анализ результатов мониторинга защищенности. Подготовка отчета по выявленным аномалиям и инцидентам. Разработка рекомендаций по повышению защищенности информационной системы. | Пр | 2/-/2 |
| Итого | | | |

**5.3. Курсовой проект (работа) учебным планом не предусмотрен**

**5.4. Самостоятельная работа обучающегося**

| Темы и/или виды самостоятельной работы | Часы |
|---|---|

| | |
|---|---|
| Самостоятельные работы | 12 |
| Самостоятельные работы | 12 |
| Самостоятельные работы | 24 |
| Самостоятельные работы | 24 |

**6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

Учебно-методическое обеспечение для самостоятельной работы обучающегося по дисциплине «Поведенческий анализ и мониторинг защищенности с использованием ИИ» размещено в электронной информационно-образовательной сре-де Университета и доступно для обучающегося через его личный кабинет на сайте Университета. Учебно-методическое обеспечение включает:

1. Рабочую программу дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ».

2.Методические рекомендации для организации самостоятельной работы обучающегося по дисциплине «Поведенческий анализ и мониторинг защищенности с использованием ИИ».

3. Методические рекомендации по выполнению письменных работ () (при наличии).

4. Методические рекомендации по выполнению контрольной работы студентами заочной формы обучения (при наличии)

5. Методические указания по выполнению курсовой работы (проекта) (при наличии).

Для успешного освоения дисциплины, необходимо самостоятельно детально изучить представленные темы по рекомендуемым источникам информации:

| № п/п | Темы для самостоятельного изучения | Рекомендуемые источники информации (№ источника) | | |
|---|---|---|---|---|
| | | основная (из п.8 РПД) | дополнительная (из п.8 РПД) | метод. лит. (из п.8 РПД) |
| 1 | Основы поведенческого анализа в кибербезопасности. Самостоятельные работы | Л1.1 | Л2.1 | Л3.1, Л3.2 |
| 2 | Мониторинг защищенности информационных систем. Самостоятельные работы | Л1.1 | Л2.1 | Л3.1, Л3.2 |
| 3 | Применение искусственного интеллекта для выявления аномалий и атак. Самостоятельные работы | Л1.1 | Л2.1 | Л3.1, Л3.2 |
| 4 | Анализ результатов мониторинга и реагирование на инциденты. Самостоятельные работы | Л1.1 | Л2.1 | Л3.1, Л3.2 |

**7. Фонд оценочных средств (оценочных материалов) для проведения промежуточной аттестации обучающихся по дисциплине «Поведенческий анализ и мониторинг защищенности с использованием ИИ»**

**7.1. Перечень индикаторов компетенций с указанием этапов их формирования в процессе освоения образовательной программы**

| Индикатор компетенции (код и содержание) | Дисциплины/элементы программы (практики, ГИА), участвующие в формировании индикатора компетен-ции | |
|---|---|---|
| | | |

**7.2. Критерии и шкалы оценивания уровня усвоения индикатора компетенций, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности**

Оценка знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций по дисциплине «Поведенческий анализ и мониторинг защищенности с использованием ИИ» проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль проводится в течение семестра с целью определения уровня усвоения обучающимися знаний, формирования умений и навыков, своевременного выявления преподавателем недостатков в подготовке обучающихся и принятия необходимых мер по её корректировке, а также для совершенствования методики обучения, организации учебной работы и

оказания индивидуальной помощи обучающемуся.

Промежуточная аттестация по дисциплине «Поведенческий анализ и мониторинг защищенности с использованием ИИ» проводится в виде Зачет.

За знания, умения и навыки, приобретенные студентами в период их обучения, выставляются оценки «ЗАЧТЕНО», «НЕ ЗАЧТЕНО». (или «ОТЛИЧНО», «ХОРОШО», «УДОВЛЕТВОРИТЕЛЬНО», «НЕУДОВЛЕТВОРИТЕЛЬНО» для дифференцированного зачета/экзамена)

Для оценивания знаний, умений, навыков и (или) опыта деятельности в университете применяется балльно-рейтинговая система оценки качества освоения образовательной программы. Оценка проводится при проведении текущего контроля успеваемости и промежуточных аттестаций обучающихся. Рейтинговая оценка знаний является интегрированным показателем качества теоретиче-ских и практических знаний и навыков студентов по дисциплине.

**Состав балльно-рейтинговой оценки студентов очной формы обучения**

Для студентов очной формы обучения знания по осваиваемым компетенциям формируются на лекционных и практических занятиях, а также в процессе самостоятельной подготовки.

В соответствии с балльно-рейтинговой системой оценки, принятой в Университете студентам начисляются баллы по следующим видам работ:

| № контрольной точки | Оценочное средство результатов индикаторов достижения компетенций | Максимальное количество баллов |
|---|---|---|
| 4 семестр | | |
| КТ 1 | Тест | 15 |
| КТ 2 | Тест | 15 |
| **Сумма баллов по итогам текущего контроля** | | **30** |
| Посещение лекционных занятий | | 20 |
| Посещение практических/лабораторных занятий | | 20 |
| Результативность работы на практических/лабораторных занятиях | | 30 |
| Итого | | 100 |

| № контрольной точки | Оценочное средство результатов индикаторов достижений компетенций | Максимальное количество баллов | Критерии оценки знаний студентов |
|---|---|---|---|
| 4 семестр | | | |
| КТ 1 | Тест | 15 | 15 баллов выставляется обучающемуся, если тестовые задания выполнены на 85 % и выше; 12–14 баллов выставляется обучающемуся, если тестовые задания выполнены на 70–84 %; 9–11 баллов выставляется обучающемуся, если тестовые задания выполнены на 55–69 %; 6–8 баллов выставляется обучающемуся, если тестовые задания выполнены на 44–54 %; 0–5 баллов выставляется обучающемуся, если тестовые задания выполнены на 43 % и менее. |

| | | | |
|---|---|---|---|
| КТ 2 | Тест | 15 | 15 баллов выставляется обучающемуся, если тестовые задания выполнены на 85 % и выше; 12–14 баллов выставляется обучающемуся, если тестовые задания выполнены на 70–84 %; 9–11 баллов выставляется обучающемуся, если тестовые задания выполнены на 55–69 %; 6–8 баллов выставляется обучающемуся, если тестовые задания выполнены на 44–54 %; 0–5 баллов выставляется обучающемуся, если тестовые задания выполнены на 43 % и менее. |

**Критерии и шкалы оценивания результатов обучения на промежуточной аттестации**

При проведении итоговой аттестации «зачет» («дифференцированный зачет», «экзамен») преподавателю с согласия студента разрешается выставлять оценки («отлично», «хорошо», «удовлетворительно», «зачет») по результатам набранных баллов в ходе текущего контроля успеваемости в семестре по выше приведенной шкале.

В случае отказа – студент сдает зачет (дифференцированный зачет, экзамен) по приведенным выше вопросам и заданиям. Итоговая успеваемость (зачет, дифференцированный зачет, экзамен) не может оцениваться ниже суммы баллов, которую студент набрал по итогам текущей и промежуточной успеваемости.

При сдаче (зачета, дифференцированного зачета, экзамена) к заработанным в течение семестра студентом баллам прибавляются баллы, полученные на (зачете, дифференцированном зачете, экзамене) и сумма баллов переводится в оценку.

**Критерии и шкалы оценивания ответа на зачете**

По дисциплине «Поведенческий анализ и мониторинг защищенности с использованием ИИ» к зачету допускаются студенты, выполнившие и сдавшие практические работы по дисциплине, имеющие ежемесячную аттестацию и без привязке к набранным баллам. Студентам, набравшим более 65 баллов, зачет выставляется по результатам текущей успеваемости, студенты, не набравшие 65 баллов, сдают зачет по вопросам, предусмотренным РПД. Максимальная сумма баллов по промежуточной аттестации (зачету) устанавливается в 15 баллов

| Вопрос билета | Количество баллов |
|---|---|
| Теоретический вопрос | до 5 |
| Задания на проверку умений | до 5 |
| Задания на проверку навыков | до 5 |

Теоретический вопрос

5 баллов выставляется студенту, полностью освоившему материал дисциплины или курса в соответствии с учебной программой, включая вопросы рассматриваемые в рекомендованной программой дополнительной справочно-нормативной и научно-технической литературы, свободно владеющему основными понятиями дисциплины. Требуется полное понимание и четкость изложения ответов по экзаменационному заданию (билету) и дополнительным вопросам, заданных экзаменатором. Дополнительные вопросы, как правило, должны относиться к материалу дисциплины или курса, не отраженному в основном экзаменационном задании (билете) и выявляют полноту знаний студента по дисциплине.

4 балла заслуживает студент, ответивший полностью и без ошибок на вопросы экзаменационного задания и показавший знания основных понятий дисциплины в соответствии с обязательной программой курса и рекомендованной основной литературой.

3 балла дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и

несущественные признаки и причинно-следственные связи. Студент может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции.

2 балла дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

1 балл дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

0 баллов - при полном отсутствии ответа, имеющего отношение к вопросу.

Задания на проверку умений и навыков

5 баллов Задания выполнены в обозначенный преподавателем срок, письменный отчет без замечаний. Работа выполнена в полном объеме с соблюдением необходимой последовательности.

4 балла Задания выполнены в обозначенный преподавателем срок, письменный отчет с небольшими недочетами.

2 баллов Задания выполнены с задержкой, письменный отчет с недочетами. Работа выполнена не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы.

1 баллов Задания выполнены частично, с большим количеством вычислительных ошибок, объем выполненной части работы не позволяет сделать правильных выводов.

0 баллов Задания выполнены, письменный отчет не представлен или работа выполнена не полностью, и объем выполненной части работы не позволяет сделать правильных выводов.

### 7.3. Примерные оценочные материалы для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ»

Задания для промежуточной аттестации включают теоретические вопросы по направлению «поведенческий анализ и мониторинг защищённости с использованием ИИ» и практические задачи, демонстрирующие сформированность компетенций по дисциплине.

Темы письменных работ охватывают ключевые вопросы по направлению «поведенческий анализ и мониторинг защищённости с использованием ИИ» и предполагают самостоятельный анализ и решение прикладных задач.

Примерные оценочные материалы для текущего контроля включают тестовые задания и практические задачи по направлению «поведенческий анализ и мониторинг защищённости с использованием ИИ».

## 8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

**основная**

Л1.1 Очков В. Ф., Орлов К. А., Чудова Ю. В., Ивашов А. П., Тихонов А. И. Информационные технологии в инженерных расчетах: SMath и Python [Электронный ресурс]:учеб. пособие ; ВО - Бакалавриат, Магистратура, Специалитет, Аспирантура. - Санкт-Петербург: Лань, 2023. - 212 с. – Режим доступа: https://e.lanbook.com/book/319406

**дополнительная**

Л2.1 Зубова Е. Д. Информационные технологии в профессиональной деятельности [Электронный ресурс]:учеб. пособие для СПО. - Санкт-Петербург: Лань, 2023. - 212 с. – Режим доступа: https://e.lanbook.com/book/328523

б) Методические материалы, разработанные преподавателями кафедры по дисциплине, в соответствии с профилем ОП.

Л3.1 Погосян В. М., Костылев С. И., Руднев С. Г. Информационные технологии на транспорте [Электронный ресурс]:учеб. пособие ; ВО - Бакалавриат, Специалитет. - Санкт-Петербург: Лань, 2022. - 76 с. – Режим доступа: https://e.lanbook.com/book/206177

Л3.2 Абросимов Л. И., Борисова С. В., Бурцев А. П., Жнякин О. В., Коротких Т. Н., Крепков И. М., Русинова Н. Н. Бизнес и информационные технологии для систем управления предприятием на базе SAP [Электронный ресурс]:учеб. пособие ; ВО - Бакалавриат, Магистратура, Специалитет, Аспирантура. - Санкт-Петербург: Лань, 2022. - 812 с. – Режим доступа: https://e.lanbook.com/book/206579

**9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

| № | Наименование ресурса сети «Интернет» | Электронный адрес ресурса |
|---|---|---|
| 1 | Искусственный интеллект в кибербезопасности : учебное пособие. ЭБС Лань. | https://e.lanbook.com/book/362984 |
| 2 | Машинное обучение в задачах информационной безопасности : учебное пособие. ЭБС Znanium. | https://znanium.ru/catalog/document?id=435080 |
| 3 | Информационная безопасность компьютерных систем и сетей : учебное пособие. ЭБС Лань. | https://e.lanbook.com/book/211997 |
| 4 | Электронно-библиотечная система «Znanium». — Текст: электронный. — URL: https://znanium.com (дата обращения: 21.06.2026). — Режим доступа: для авторизованных пользователей. | https://znanium.com |
| 5 | Электронно-библиотечная система «Лань». — Текст: электронный. — URL: https://e.lanbook.com (дата обращения: 21.06.2026). — Режим доступа: для авторизованных пользователей. | https://e.lanbook.com |
| 6 | Образовательная платформа «Юрайт». — Текст: электронный. — URL: https://urait.ru (дата обращения: 21.06.2026). — Режим доступа: для авторизованных пользователей. | https://urait.ru |

**10. Методические указания для обучающихся по освоению дисциплины**

Освоение дисциплины предполагает последовательное изучение теоретического материала и закрепление практических навыков по направлению «поведенческий анализ и мониторинг защищённости с использованием ИИ» на практических (лабораторных) занятиях. Рекомендуется систематическая работа в течение семестра, своевременное выполнение заданий и подготовка к контрольным точкам.

**11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства и информационных справочных систем (при необходимости).**

*11.1 Перечень лицензионного программного обеспечения*

1. Kaspersky Endpoint Security 12.11 - Антивирус
2. Microsoft Windows Server STDCORE AllLngLicense/Software AssurancePack Academic OLV 16Licenses LevelE AdditionalProduct CoreLic 1Year - Серверная операционная система

*11.3 Перечень программного обеспечения отечественного производства*

1. Kaspersky Endpoint Security 12.11 - Антивирус

При осуществлении образовательного процесса студентами и преподавателем используются следующие информационно справочные системы: СПС «Консультант плюс», СПС «Гарант».

**12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

| № п/п | Наименование специальных помещений и помещений для самостоятельной работы | Номер аудитории | Оснащенность специальных помещений и помещений для самостоятельной работы |
|---|---|---|---|
| 1 | Учебная аудитория для проведения занятий всех типов (в т.ч. лекционного, семинарского, практической подготовки обучающихся), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации | 160/ЭиФ | Оснащение: столы – 32 шт., стулья – 130 шт., мультимедийная доска, учебно-наглядные пособия в виде презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета. |
| | | 423/НК | Оснащение: специализированная мебель на 56 посадочных мест, стол преподавателя – 1 шт., Sharp 70" Информационный ЖК-дисплей – 1 шт., магнитно-маркерная доска – 1 шт., учебно-наглядные пособия в виде тематических презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета. |
| 2 | Помещение для самостоятельной работы обучающихся, подтверждающее наличие материально-технического обеспечения, с перечнем основного оборудования | | |
| | | 184/ЭиФ | Оснащение: столы – 27 шт., стулья – 27 шт., мультимедийная доска, учебно-наглядные пособия в виде презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета. |

**13. Особенности реализации дисциплины лиц с ограниченными возможностями здоровья**

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники и учебные пособия, иная учебная литература, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

а) для слабовидящих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- задания для выполнения, а также инструкция о порядке проведения промежуточной аттестации оформляются увеличенным шрифтом;
- задания для выполнения на промежуточной аттестации зачитываются ассистентом;
- письменные задания выполняются на бумаге, надиктовываются ассистенту;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- студенту для выполнения задания при необходимости предоставляется увеличивающее устройство;

в) для глухих и слабослышащих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- промежуточная аттестация проводится в письменной форме;
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости поступающим предоставляется звукоусиливающая аппаратура индивидуального пользования;
- по желанию студента промежуточная аттестация может проводиться в письменной форме;

д) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента промежуточная аттестация проводится в устной форме.

Рабочая программа дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» составлена на основе Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 916).

Автор (ы)

_____ КИС, Березницкий Андрей Сергеевич

Рецензенты

_____ преп. КИС, Трошков Александр Михайлович

Рабочая программа дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» рассмотрена на заседании Кафедра информационных систем протокол № 9 от 07.04.2026 г. и признана соответствующей требованиям ФГОС ВО и учебного плана по направлению подготовки 09.04.03 Прикладная информатика

Заведующий кафедрой _____ Березницкий Андрей Сергеевич

Рабочая программа дисциплины «Поведенческий анализ и мониторинг защищенности с использованием ИИ» рассмотрена на заседании учебно-методической комиссии Факультет цифровых технологий протокол № 2 от 08.04.2026 г. и признана соответствующей требованиям ФГОС ВО и учебного плана по направлению подготовки 09.04.03 Прикладная информатика

Руководитель ОП _____