**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение высшего образования**

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по УР
_____Сенченко П.В.
«11» _____12_____ 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **09.04.04 Программная инженерия**
Направленность (профиль) / специализация: **Искусственный интеллект в биомедицинских системах**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **2**
Семестр: **3**
Учебный план набора 2025 года

Объем дисциплины и виды учебной деятельности

| Виды учебной деятельности | 3 семестр | Всего | Единицы |
|---|---|---|---|
| Лекционные занятия | 24 | 24 | часов |
| Лабораторные занятия | 28 | 28 | часов |
| Самостоятельная работа | 92 | 92 | часов |
| Подготовка и сдача экзамена | 36 | 36 | часов |
| Общая трудоемкость (включая промежуточную аттестацию) | 180 | 180 | часов |
| | 5 | 5 | з.е. |

| Формы промежуточной аттестации | Семестр |
|---|---|
| Экзамен | 3 |



Томск

## 1. Общие положения

### 1.1. Цели дисциплины

1. Целью дисциплины является приобретение навыков анализа информационно-аналитических систем для нахождения уязвимостей и подбора механизмов защиты.

### 1.2. Задачи дисциплины

1. Получить теоретические знания и практические навыки для анализа информационно-аналитических систем.
2. Получить навыки работы с методами и алгоритмами искусственного интеллекта.
3. Приобрести навыки нахождения уязвимостей ИАС и построения систем защиты.

## 2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль направления подготовки (hard skills – HS).
Индекс дисциплины: Б1.О.02.07.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

## 3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

| Компетенция | Индикаторы достижения компетенции | Планируемые результаты обучения по дисциплине |
|---|---|---|
| **Универсальные компетенции** | | |
| - | - | - |
| **Общепрофессиональные компетенции** | | |
| ОПК-3. Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями | ОПК-3.1. Знает принципы, методы и средства анализа и структурирования профессиональной информации | Знает принципы, методы и средства анализа и структурирования информации при профессиональной деятельности |
| | ОПК-3.2. Умеет анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров | Демонстрирует умение находить, анализировать, структурировать и оформлять в виде обзора информацию при профессиональной деятельности |
| | ОПК-3.3. Владеет методами подготовки научных докладов, публикаций и аналитических обзоров с обоснованными выводами и рекомендациями | Владеет методами подготовки научных докладов, публикаций и аналитических обзоров с обоснованными выводами и рекомендациями |

| | | |
|---|---|---|
| ОПК-4. Способен применять на практике новые научные принципы и методы исследований | ОПК-4.1. Знает общие принципы исследований, методы проведения исследований | Знает общие принципы, методы и подходы проведения исследований |
| | ОПК-4.2. Умеет формулировать принципы исследований, находить, сравнивать, оценивать методы исследований | Умеет формулировать принципы исследований, проводить анализ методов исследований |
| | ОПК-4.3. Владеет методами проведения исследований для решения практических задач профессиональной деятельности | Владеет методами проведения исследований в профессиональной деятельности |
| **Профессиональные компетенции** | | |

| | | |
|---|---|---|
| ПК-1. Способен анализировать и применять методы искусственного интеллекта и машинного обучения для задач анализа биомедицинских данных; | ПК-1.1. Знает этические и правовые особенности применения методов искусственного интеллекта в медицине: обработка конфиденциальной информации в биомедицинских системах, Системный анонимизация программист. персональных данных, оформление заявок клинических исследований | Знает этические и правовые особенности применения методов искусственного интеллекта в медицине: обработка конфиденциальной информации в биомедицинских системах, персональных данных, оформление заявок клинических исследований |
| | ПК-1.2. Знает основные принципы и методы сегментации и детектирования объектов при обработке медицинских изображений и способен применять их на практике | Знает принципы и методы сегментации и детектирования объектов при обработке медицинских изображений и способен применять их на практике |
| | ПК-1.3. Умеет применять методы искусственного интеллекта и машинного обучения для анализа биомедицинских данных в различных контекстах: биомедицинские технологии, медицинская реабилитация и медицинская диагностика | Умеет применять методы искусственного интеллекта и машинного обучения для анализа биомедицинских данных в профессиональной деятельности |
| | ПК-1.4. Владеет навыками работы с наборами биомедицинских данных: подготовка данных, выбор подходящих моделей и алгоритмов, оценка и интерпретация результатов | Владеет навыками работы с наборами биомедицинских данных |
| | ПК-1.5. Владеет навыками разработки и применения моделей искусственного интеллекта для решения конкретных задач в области биомедицины: предсказание, классификация, кластеризация и регрессия | Владеет навыками разработки и применения моделей искусственного интеллекта в профессиональной деятельности |
| | ПК-1.6. Владеет знаниями методов искусственного интеллекта и машинного обучения для анализа биомедицинских данных: классификация, регрессия, кластеризация, уменьшение размерности, сегментация и детектирование объектов на медицинских изображениях | Владеет знаниями методов искусственного интеллекта и машинного обучения для анализа биомедицинских данных |

## 4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

| Виды учебной деятельности | Всего часов | Семестры |
|---|---|---|
| | | 3 семестр |
| **Контактная аудиторная работа обучающихся с преподавателем, всего** | 52 | 52 |
| Лекционные занятия | 24 | 24 |
| Лабораторные занятия | 28 | 28 |
| **Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего** | 92 | 92 |
| Подготовка к тестированию | 42 | 42 |
| Подготовка к лабораторной работе, написание отчета | 50 | 50 |
| **Подготовка и сдача экзамена** | 36 | 36 |
| **Общая трудоемкость (в часах)** | 180 | 180 |
| **Общая трудоемкость (в з.е.)** | 5 | 5 |

## 5. Структура и содержание дисциплины

### 5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

| Названия разделов (тем) дисциплины | Лек. зан., ч | Лаб. раб. | Сам. раб., ч | Всего часов (без экзамена) | Формируемые компетенции |
|---|---|---|---|---|---|
| **3 семестр** | | | | | |
| 1 Информационно-аналитические системы | 6 | - | 12 | 18 | ОПК-3 |
| 2 Атаки отравлением | 6 | 18 | 30 | 54 | ОПК-3, ПК-1 |
| 3 Генерация и анализ вредоносных входных данных | 6 | 6 | 30 | 42 | ОПК-3, ПК-1 |
| 4 Подходы и механизмы защиты ИАС | 6 | 4 | 20 | 30 | ОПК-4 |
| Итого за семестр | 24 | 28 | 92 | 144 | |
| Итого | 24 | 28 | 92 | 144 | |

### 5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

| Названия разделов (тем) дисциплины | Содержание разделов (тем) дисциплины (в т.ч. по лекциям) | Трудоемкость (лекционные занятия), ч | Формируемые компетенции |
|---|---|---|---|
| **3 семестр** | | | |

| | | | |
|---|---|---|---|
| 1 Информационно-аналитические системы | Классификация атак, связанных с ИИ: направление, цель, подготовка, уровень угрозы<br>Методы противодействия атакам на безопасность ИС и КС, атакам на конфиденциальность, атакам отравления<br>Методы противодействия атакам отклонения, атакам извлечения и атакам путем генерации изображений<br>Виды атак на модели МО, мотивация к атакам.<br>Вредоносные данные. | 6 | ОПК-3 |
| | Итого | 6 | |
| 2 Атаки отравлением | Атаки отравления: суть подхода, виды атак отравления.<br>Отравление данных.<br>Бэкдоры и триггеры. | 6 | ПК-1 |
| | Итого | 6 | |
| 3 Генерация и анализ вредоносных входных данных | Входные пространства и данные вне распределения.<br>Ландшафт предсказаний и карта значимости.<br>Искажающая атака и вредоносная заплатка<br>Оценка выявляемости атак: Lp-норма, абсолютный порог ощущения и адаптация чувств.<br>Генерация вредоносных изображений.<br>Атаки на реальные системы. | 6 | ОПК-3, ПК-1 |
| | Итого | 6 | |
| 4 Подходы и механизмы защиты ИАС | Оценка устойчивости модели. :<br>Защита модели через улучшение.<br>Защита модели через предварительную обработку данных.<br>Защита модели через сокрытие информации о целевой системе.<br>Перспективы повышения надежности ИИ. | 6 | ОПК-4 |
| | Итого | 6 | |
| | Итого за семестр | 24 | |

| | | |
|---|---|---|
| Итого | 24 | |

### 5.3. Практические занятия (семинары)

Не предусмотрено учебным планом

### 5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

| Названия разделов (тем) дисциплины | Наименование лабораторных работ | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| **3 семестр** | | | |
| 2 Атаки отравлением | Отравление наборов данных | 6 | ОПК-3, ПК-1 |
| | Отравление данных с использованием библиотек cleverhans и adversal robustness toolbox | 6 | ОПК-3, ПК-1 |
| | Методология отравления речевых данных | 6 | ОПК-3, ПК-1 |
| | Итого | 18 | |
| 3 Генерация и анализ вредоносных входных данных | Методология состязательных атак на речевой сигнал | 6 | ОПК-3, ПК-1 |
| | Итого | 6 | |
| 4 Подходы и механизмы защиты ИАС | Атаки на наборы данных временных рядов | 4 | ОПК-4 |
| | Итого | 4 | |
| Итого за семестр | | 28 | |
| Итого | | 28 | |

### 5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

### 5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6. – Виды самостоятельной работы, трудоемкость и формируемые компетенции

| Названия разделов (тем) дисциплины | Виды самостоятельной работы | Трудоемкость, ч | Формируемые компетенции | Формы контроля |
|---|---|---|---|---|
| **3 семестр** | | | | |
| 1 Информационно-аналитические системы | Подготовка к тестированию | 12 | ОПК-3 | Тестирование |
| | Итого | 12 | | |
| 2 Атаки отравлением | Подготовка к тестированию | 10 | ОПК-3, ПК-1 | Тестирование |
| | Подготовка к лабораторной работе, написание отчета | 20 | ОПК-3, ПК-1 | Лабораторная работа |
| | Итого | 30 | | |

| | | | | |
|---|---|---|---|---|
| 3 Генерация и анализ вредоносных входных данных | Подготовка к тестированию | 10 | ОПК-3, ПК-1 | Тестирование |
| | Подготовка к лабораторной работе, написание отчета | 20 | ОПК-3, ПК-1 | Лабораторная работа |
| | Итого | 30 | | |
| 4 Подходы и механизмы защиты ИАС | Подготовка к тестированию | 10 | ОПК-4 | Тестирование |
| | Подготовка к лабораторной работе, написание отчета | 10 | ОПК-4 | Лабораторная работа |
| | Итого | 20 | | |
| Итого за семестр | | 92 | | |
| | Подготовка и сдача экзамена | 36 | | Экзамен |
| Итого | | 128 | | |

### 5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

| Формируемые компетенции | Виды учебной деятельности | | | Формы контроля |
|---|---|---|---|---|
| | Лек. зан. | Лаб. раб. | Сам. раб. | |
| ОПК-3 | + | + | + | Лабораторная работа, Тестирование, Экзамен |
| ОПК-4 | + | + | + | Лабораторная работа, Тестирование, Экзамен |
| ПК-1 | + | + | + | Лабораторная работа, Тестирование, Экзамен |

## 6. Рейтинговая система для оценки успеваемости обучающихся

### 6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

| Формы контроля | Максимальный балл на 1-ую КТ с начала семестра | Максимальный балл за период между 1КТ и 2КТ | Максимальный балл за период между 2КТ и на конец семестра | Всего за семестр |
|---|---|---|---|---|
| **3 семестр** | | | | |
| Лабораторная работа | 0 | 12 | 18 | 30 |
| Тестирование | 10 | 10 | 20 | 40 |
| Экзамен | | | | 30 |
| Итого максимум за период | 10 | 22 | 38 | 100 |
| Нарастающим итогом | 10 | 32 | 70 | 100 |

### 6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

| Баллы на дату текущего контроля | Оценка |
|---|---|
| ≥ 90% от максимальной суммы баллов на дату ТК | 5 |
| От 70% до 89% от максимальной суммы баллов на дату ТК | 4 |
| От 60% до 69% от максимальной суммы баллов на дату ТК | 3 |
| < 60% от максимальной суммы баллов на дату ТК | 2 |

### 6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

| Оценка | Итоговая сумма баллов, учитывает успешно сданный экзамен | Оценка (ECTS) |
|---|---|---|
| 5 (отлично) (зачтено) | 90 – 100 | A (отлично) |
| 4 (хорошо) (зачтено) | 85 – 89 | B (очень хорошо) |
| | 75 – 84 | C (хорошо) |
| | 70 – 74 | D (удовлетворительно) |
| 3 (удовлетворительно) (зачтено) | 65 – 69 | |
| | 60 – 64 | E (посредственно) |
| 2 (неудовлетворительно) (не зачтено) | Ниже 60 баллов | F (неудовлетворительно) |

## 7. Учебно-методическое и информационное обеспечение дисциплины

### 7.1. Основная литература

1. Баланов, А. Н. Машинное обучение и искусственный интеллект : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 172 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/414920.

### 7.2. Дополнительная литература

1. Золкин, А. Л. Реализация принципов организации и использования средств машинного обучения и искусственного интеллекта в медицине : учебное пособие / А. Л. Золкин, В. Д. Мунистер. — Самара : , 2024. — 123 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/429719.

### 7.3. Учебно-методические пособия

#### 7.3.1. Обязательные учебно-методические пособия

1. Безопасность информационно аналитических систем: Учебно-методическое пособие к лабораторным работам / Д. И. Новохрестова, П. Ю. Лаптев - 2025. 50 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/11106.

#### 7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

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

**Для лиц с нарушениями зрения:**

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

– в форме электронного документа;
– в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

– в форме электронного документа;
– в печатной форме.

### 7.4. Современные профессиональные базы данных и информационные справочные системы

При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

## 8. Материально-техническое и программное обеспечение дисциплины

### 8.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

### 8.2. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 504 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Усилитель Roxton AA-60M;
- Потолочный громкоговоритель Roxton PA-20T;
- Магнитно-маркерная доска;
- Обучающий стенд локальные компьютерные сети Microtik routerboard - 2 шт.;
- ViPNET УМК "Безопасность сетей";
- Коммутатор Mikrotik CRS125-24G-1S-IN - 6 шт.;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 - 3 шт.;
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 - 2 шт.;
- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 - 2 шт.;
- Маршрутизатор Cisco C881-V-K9 - 2 шт.;
- Маршрутизатор Check Point CPAP-SG1200R-NGFW - 2 шт.;

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:

- абонентские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- межсетевые экраны: ИКС Lite, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- точки доступа: D-link dwl3600ap.

Стенды для изучения средств криптографической защиты информации в банковском деле, включающие:

- абонентские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- средства криптографической защиты информации: программно-аппаратный комплекс шифрования "ФПСУ-IP", программно-аппаратный комплекс шифрования "ФПСУ-IP/Клиент".

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

### 8.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 101 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 107 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 130 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

### 8.4. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

## 9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

### 9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

| Названия разделов (тем) дисциплины | Формируемые компетенции | Формы контроля | Оценочные материалы (ОМ) |
|---|---|---|---|
| 1 Информационно-аналитические системы | ОПК-3 | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |

| | | | |
|---|---|---|---|
| 2 Атаки отравлением | ОПК-3, ПК-1 | Лабораторная работа | Темы лабораторных работ |
| | | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |
| 3 Генерация и анализ вредоносных входных данных | ОПК-3, ПК-1 | Лабораторная работа | Темы лабораторных работ |
| | | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |
| 4 Подходы и механизмы защиты ИАС | ОПК-4 | Лабораторная работа | Темы лабораторных работ |
| | | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

| Оценка | Баллы за ОМ | Формулировка требований к степени сформированности планируемых результатов обучения | | |
|---|---|---|---|---|
| | | знать | уметь | владеть |
| 2 (неудовлетворительно) | < 60% от максимальной суммы баллов | отсутствие знаний или фрагментарные знания | отсутствие умений или частично освоенное умение | отсутствие навыков или фрагментарные применение навыков |
| 3 (удовлетворительно) | от 60% до 69% от максимальной суммы баллов | общие, но не структурированные знания | в целом успешно, но не систематически осуществляемое умение | в целом успешное, но не систематическое применение навыков |
| 4 (хорошо) | от 70% до 89% от максимальной суммы баллов | сформированные, но содержащие отдельные проблемы знания | в целом успешное, но содержащие отдельные пробелы умение | в целом успешное, но содержащие отдельные пробелы применение навыков |
| 5 (отлично) | ≥ 90% от максимальной суммы баллов | сформированные систематические знания | сформированное умение | успешное и систематическое применение навыков |

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

| Оценка | Формулировка требований к степени компетенции |
|---|---|
| 2 (неудовлетворительно) | Не имеет необходимых представлений о проверяемом материале или<br>Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения. |
| 3 (удовлетворительно) | Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях. |
| 4 (хорошо) | Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения. |
| 5 (отлично) | Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины. |

### 9.1.1. Примерный перечень тестовых заданий

1. Для какого вида атак необходима подготовка: Разведка средств защиты информационных систем?
    1. Использование вредоносного ПО
    2. Deepfake
    3. Атака генерацией изображений
    4. Атака созданием фальшивых личностей
2. Как называется отображение значения важности каждого пикселя изображения в пользу конкретной категории классификации?
    1. изображение значимости
    2. карта значимости
    3. картина значимости
    4. схема значимости
3. Как называются методы атаки, которые позволяют создавать вредоносные входные данные, основываясь на полной осведомленности о ГНС-модели?
    1. методы черного ящика
    2. методы черного ящика с оценкой
    3. методы ограниченного черного ящика
    4. методы белого ящика
4. Какой из методов НЕ относится к методам белого ящика?
    1. Метод граничной атаки
    2. Метод Карлини и Вагнера
    3. Методы JSMA
    4. Метод FGSM
5. Какой метод относится к подходу защиты "Минимизация осведомленности злоумышленника"?
    1. Маскирование градиентов
    2. Фильтрация и предобработка данных
    3. Дистилляция модели
    4. Сокрытие информации о целевой системе
6. Как называется дополнение к определенной (пространственной

или временной) области входных данных, заставляющее модель возвращать неверный результат. Вредоносная заплатка обычно вполне заметна для человека, но часто камуфлируется под нечто неопасное.
    1. Вредоносное искажение
    2. Вредоносная заплатка
    3. Вредоносная вставка
    4. Вредоносная картинка
7. В граничной атаке встраивание происходит в:
    1. атакуемое изображение
    2. атакующее изображение
    3. и в атакуемое, и в атакующее изображения
    4. в граничной атаке встраивание не происходит
8. В какой схеме атаки злоумышленник разрабатывает атаку против замещающей модели, которая аппроксимирует целевую систему?
    1. Атака с копированием
    2. Прямая атака
    3. Универсальная атака с переносом.
    4. Атака с переносом
9. Для какого типа атаки необходимо определить принцип работы модели?
    1. Атака на конфиденциальность данных
    2. Атака отравления
    3. Атака извлечения
    4. Атака отклонения
10. Целью какой атаки является обучающие данные нейросети?
    1. Атака на конфиденциальность данных
    2. Атака отравления
    3. Атака извлечения
    4. Атака отклонения

### 9.1.2. Перечень экзаменационных вопросов

1. Классификация атак, связанных с ИИ: направление, цель, подготовка, уровень угрозы
2. Методы противодействия атакам на безопасность ИС и КС, атакам на конфиденциальность, атакам отравления
3. Методы противодействия атакам отклонения, атакам извлечения и атакам путем генерации изображений
4. Виды атак на модели МО, мотивация к атакам.
5. Вредоносные данные.
6. Атаки отравления: суть подхода, виды атак отравления.
7. Отравление данных.
8. Бэкдоры и триггеры.
9. Входные пространства и данные вне распределения.
10. Ландшафт предсказаний и карта значимости.
11. Искажающая атака и вредоносная заплатка
12. Оценка выявляемости атак: Lp-норма, абсолютный порог ощущения и адаптация чувств.
13. Генерация вредоносных изображений: методы белого ящика
14. Генерация вредоносных изображений: методы ограниченно черного ящика и черного ящика с оценкой.
15. Атаки на реальные системы: прямая атака и атака с копированием
16. Атаки на реальные системы: атака с переносом и универсальная атака с переносом.
17. Многократно используемые заплатки и искажения.
18. Оценка устойчивости модели: цели, возможности, ограничения и знания злоумышленника.
19. Оценка устойчивости модели: эмпирический и теоретических подход.
20. Защита модели через улучшение: маскирование градиентов и оценка неопределенности случайного отсева.
21. Защита модели через улучшение: вредоносное обучение и детекция данных вне распределения.

22. Защита модели через предварительную обработку данных.
23. Защита модели через сокрытие информации о целевой системе.
24. Перспективы повышения надежности ИИ.

### 9.1.3. Темы лабораторных работ

1. Отравление наборов данных
2. Отравление данных с использованием библиотек cleverhans и adversal robustness toolbox
3. Методология отравления речевых данных
4. Методология состязательных атак на речевой сигнал
5. Атаки на наборы данных временных рядов

## 9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

## 9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.4.

Таблица 9.4 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

| Категории обучающихся | Виды дополнительных оценочных материалов | Формы контроля и оценки результатов обучения |
|---|---|---|
| С нарушениями слуха | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы | Преимущественно письменная проверка |
| С нарушениями зрения | Собеседование по вопросам к зачету, опрос по терминам | Преимущественно устная проверка (индивидуально) |

| | | |
|---|---|---|
| С нарушениями опорно-двигательного аппарата | Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету | Преимущественно дистанционными методами |
| С ограничениями по общемедицинским показаниям | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы | Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент проверки |

### 9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;
– в печатной форме с увеличенным шрифтом;
– в форме электронного документа;
– методом чтения ассистентом задания вслух;
– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;
– набор ответов на компьютере;
– набор ответов с использованием услуг ассистента;
– представление ответов устно.

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

**Для лиц с нарушениями зрения:**
– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**
– в форме электронного документа;
– в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**
– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

**ЛИСТ СОГЛАСОВАНИЯ**

Рассмотрена и одобрена на заседании кафедры БИС
протокол № 10 от «28» 11 2024 г.

**СОГЛАСОВАНО:**

| Должность | Инициалы, фамилия | Подпись |
|---|---|---|
| Заведующий выпускающей каф. КИБЭВС | А.А. Шелупанов | Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d |
| Заведующий обеспечивающей каф. БИС | Е.Ю. Костюченко | Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463 |
| Начальник учебного управления | И.А. Лариошина | Согласовано, c3195437-a02f-4972-a7c6-ab6ee1f21e73 |

**ЭКСПЕРТЫ:**

| | | |
|---|---|---|
| Доцент, каф. КИБЭВС | Е.Ю. Костюченко | Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463 |
| Доцент, каф. КИБЭВС | А.Ю. Якимук | Согласовано, 4ffdf265-fb78-4863-b293-f03438cb07cc |

**РАЗРАБОТАНО:**

| | | |
|---|---|---|
| Доцент, каф. КИБЭВС | Д.И. Новохрестова | Разработано, 7a28d148-33a2-48d2-b02b-b311de2c008d |