**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН**
**МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»**

«Утверждаю»
Декан естественнонаучного факультета
_____ Пещукович А.И.
«____»_____2026 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

# Интеллектуальные системы защиты информации

Направление подготовки - 10.03.01 «Информационная безопасность»
Профиль подготовки – Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)
Форма подготовки – Очная
Уровень подготовки – Бакалавриат

**ДУШАНБЕ - 2026**

Рабочая программа составлена на основе требований федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» **(**уровень Бакалавриат), утвержденного приказом Министерства образования и науки РФ №524 от 08.06.2017 г., Концепции преподавания Интеллектуальные системы защиты информации для специальностей и направлений подготовки, реализуемых в образовательных организациях высшего образования, утвержденной протоколом Экспертного совета по развитию исторического образования Минобрнауки РФ от 06.08.2024 г. №ВФ/35-ПР

При разработке рабочей программы учитываются

- содержание программ дисциплин, изучаемых на предыдущих и последующих этапах обучения;
- новейшие достижения в данной предметной области.

Рабочая программа обсуждена на заседании кафедры Кафедра информатики и информационных технологий протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена УМС естественнонаучного факультета протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена Ученым советом естественнонаучного факультета, протокол № 1 от «___» _____ 2025 г.

## 1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

**Актуальность изучения дисциплины** «Интеллектуальные системы защиты информации»

**1.1 Цели изучения дисциплины** Целью освоения дисциплины "Интеллектуальные системы защиты информации" является формирование у студентов теоретических знаний и практических навыков в области разработки, внедрения и эксплуатации интеллектуальных систем для обеспечения информационной безопасности. Дисциплина направлена на изучение современных подходов и технологий, применяемых для защиты информации от различных угроз, а также на развитие способности к анализу, проектированию и реализации эффективных решений в этой области. В результате освоения дисциплины студенты должны быть готовы к решению практических задач по обеспечению безопасности информационных систем.

**1.2 Задачи изучения дисциплины** Задачи дисциплины:

1. Изучение принципов построения и функционирования интеллектуальных систем защиты информации.
2. Освоение методов анализа угроз и уязвимостей информационных систем.
3. Рассмотрение различных типов интеллектуальных систем защиты, включая системы обнаружения вторжений, анализа вредоносного ПО и управления доступом.
4. Формирование навыков разработки и внедрения интеллектуальных систем защиты информации.
5. Изучение передовых технологий и тенденций в области информационной безопасности.

**1.3 В результате изучения дисциплины «Интеллектуальные системы защиты информации» у обучающихся формируются следующие универсальные и общепрофессиональные компетенции:**

| Код | Результаты освоения ООП | Индикаторы достижения компетенции | Вид оценочного знания |
|---|---|---|---|

| | | | |
|---|---|---|---|
| УК-1. | Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | "ИУК-1.1 Анализирует задачу, выделяя её базовые составляющие.<br><br>ИУК-1.2 Демонстрирует знание особенностей системного и критического мышления и готовность к нему.<br><br>ИУК-1.3 Аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение.<br><br>ИУК-1.4 Предлагает возможные варианты решения задачи, оценивая их достоинства и недостатки." | |
| ПК-1. | Способен проводить обследование организаций и формировать требования к информационной системе | ИПК-1.1 Использует методики обследования организации и выявления информационных потребностей пользователей.<br><br>ИПК-1.2 Анализирует деятельность предприятия и выявляет участки, нуждающиеся в автоматизации.<br><br>ИПК-1.3 Выбирает класс ИС, способы автоматизации, оценивает совокупную стоимость владения ИС, планирует стратегическое и оперативное развитие ИС. | |
| ПК-2. | Способен разрабатывать и адаптировать прикладное программное обеспечение | ИПК-2.1 Применяет современные технологии разработки и адаптации прикладного ПО.<br><br>ИПК-2.2 Разрабатывает и адаптирует ПО на современных языках программирования.<br><br>ИПК-2.3 Применяет современные технологии для разработки веб-приложений. | |

| | | | |
|---|---|---|---|
| ПК-3. | Способен проектировать информационные системы по видам обеспечения | ИПК-3.1 Обосновывает выбор проектных решений по видам обеспечения ИС.<br><br>ИПК-3.2 Участвует в проектировании экономических ИС и их модулей. | |

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

**2.1.** Дисциплина **«Интеллектуальные системы защиты информации»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.В.12).** В процессе преподавания данного курса учитываются знания студентов по таким дисциплинам, как история таджикского народа, история первобытного общества, история древнего мира и средних веков, изучавшихся ими в общеобразовательной средней школе.

**2.2** Преподавание данной дисциплины является необходимым для дальнейшего освоения студентами дисциплин в структуре ОПОП бакалавриата по направлению **«Информационная безопасность».**

Таблица 2.

| **№ п/п** | **Название дисциплины** | **Семестр** | **Место дисциплины в структуре ОПОП** |
|---|---|---|---|
| - | — | — | Предшествующая дисциплина |
| - | — | — | Последующая дисциплина |

При освоении данной дисциплины необходимы умения и готовность («входные» знания) обучающегося по дисциплинам, указанных в Таблице 2. Дисциплины взаимосвязаны с данной дисциплиной, они изучаются параллельно. Теоретическими дисциплинами, для которых освоение данной дисциплины необходимо как предшествующее являются:

## 3. СТРУКТУРА И СОДЕРЖАНИЕ КУРСА, КРИТЕРИИ НАЧИСЛЕНИЯ БАЛЛОВ

Преподавание курса «Интеллектуальные системы защиты информации» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 126 часа, из которых: лекции – 16 часов, практические занятия – 14 часов, лабораторные работы 16 часов, иная контактная работа – 32 часа, самостоятельная работа – 70. Всего часов аудиторной нагрузки – 56 часа.

По итогам 8 семестра планируется сдача студентами зачета с оценкой.

### 3.1 Структура и содержание теоретической части курса

**Лекция 1 Введение в интеллектуальные системы защиты информации. Основные понятия и определения.**

Обзор предметной области. Актуальность и задачи интеллектуальных систем защиты информации. Классификация угроз информационной безопасности.

**Лекция 2 Методы анализа угроз и уязвимостей информационных систем.**

Анализ рисков. Методы оценки уязвимостей. Сканеры безопасности и их применение.

**Лекция 3 Системы обнаружения вторжений (IDS). Архитектура и принципы работы.**

Сетевые и хостовые IDS. Методы обнаружения атак: сигнатурный, аномальный, гибридный.

**Лекция 4 Интеллектуальный анализ трафика и поведения пользователей.**

Использование машинного обучения для обнаружения аномалий и угроз. Анализ логов и событий безопасности.

**Лекция 5 Системы анализа вредоносного ПО. Принципы работы и методы обнаружения.**

Анализ статического и динамического вредоносного кода. Эвристические методы обнаружения. Песочницы.

**Лекция 6 Интеллектуальные системы управления доступом и аутентификации.**

Адаптивная аутентификация. Биометрические методы аутентификации. Ролевая модель доступа.

**Лекция 7 Интеллектуальные методы защиты от утечек информации (DLP).**

Принципы работы DLP-систем. Методы обнаружения утечек. Классификация и категоризация данных.

**Лекция 8 Перспективы развития интеллектуальных систем защиты информации.**

Искусственный интеллект и машинное обучение в информационной безопасности. Будущее систем защиты.

## Структура и содержание практической части курса

**Практическое занятие 1 Ознакомление с инструментами для анализа угроз и уязвимостей. (Практика)**

Практическое применение сканеров безопасности. Настройка и использование.

**Практическое занятие 2 Настройка и использование сетевой системы обнаружения вторжений (IDS). (Практика)**

Установка и настройка Snort или Suricata. Анализ журналов событий.

**Практическое занятие 3 Настройка и использование хостовой системы обнаружения вторжений (HIDS). (Практика)**

Установка и настройка OSSEC или аналогичных систем. Мониторинг целостности файлов.

**Практическое занятие 4 Анализ сетевого трафика с использованием Wireshark. (Практика)**

Перехват и анализ пакетов. Выявление аномалий и подозрительной активности.

**Практическое занятие 5 Практическое применение антивирусных решений и песочниц. (Практика)**

Анализ подозрительных файлов. Использование онлайн-сервисов для анализа вредоносного ПО.

**Практическое занятие 6 Настройка и использование систем управления доступом. (Практика)**

Практическое применение ролевой модели доступа. Настройка политик безопасности.

**Практическое занятие 7 Использование систем DLP (Data Loss Prevention). (Практика)**

Настройка политик DLP. Мониторинг и предотвращение утечек информации.

**Практическое занятие 8 Разработка и внедрение простых скриптов для автоматизации задач безопасности. (Практика)**

Использование Python или Bash для автоматизации рутинных задач. Создание скриптов для мониторинга.

## Структура и содержание лабораторной части курса

**Лабораторная работа 1 Установка и настройка системы обнаружения вторжений (IDS).**

Установка, настройка, тестирование IDS.

**Лабораторная работа 2 Развертывание и настройка хостовой системы обнаружения вторжений (HIDS).**

Установка, настройка, тестирование HIDS.

**Лабораторная работа 3 Практическое применение анализатора трафика (Wireshark).**

Перехват и анализ сетевого трафика. Фильтрация и поиск аномалий.

**Лабораторная работа 4 Анализ вредоносного ПО в песочнице.**

Запуск и анализ вредоносных файлов в изолированной среде.

**Лабораторная работа 5 Настройка и использование системы управления доступом.**

Создание ролей, назначение прав доступа. Аудит доступа.

**Лабораторная работа 6 Использование DLP-системы для защиты данных.**

Настройка политик, мониторинг и анализ событий DLP.

**Лабораторная работа 7 Разработка простого скрипта для автоматизации задач безопасности.**

Создание скрипта для мониторинга логов или сканирования сети.

**Лабораторная работа 8 Внедрение системы SIEM.**

Установка, настройка и первоначальный анализ событий безопасности в SIEM.

## Структура и содержание КСР

**КСР 1 Разработка требований к интеллектуальной системе защиты информации для конкретной организации.**

Анализ деятельности организации, выявление угроз и уязвимостей, формулирование требований.

**КСР 2 Проектирование архитектуры системы обнаружения вторжений (IDS) для заданного сценария.**

Выбор подходящих инструментов и методов, описание архитектуры, разработка плана развертывания.

**КСР 3 Разработка модели угроз и уязвимостей для информационной системы.**

Идентификация угроз, анализ уязвимостей, оценка рисков, разработка контрмер.

**КСР 4 Создание системы анализа логов безопасности (SIEM).**

Выбор инструментов, настройка сбора и анализа логов, разработка отчетов и панелей мониторинга.

## Структура и содержание СРС

**СРС 1 Изучение современных тенденций в области информационной безопасности.**

Обзор новых угроз и уязвимостей, анализ новых технологий защиты, подготовка доклада.

**СРС 2 Анализ и оценка уязвимостей конкретной информационной системы.**

Проведение сканирования уязвимостей, анализ результатов, подготовка отчета.

**СРС 3 Разработка плана реагирования на инциденты информационной безопасности.**

Определение этапов реагирования, выбор инструментов, разработка процедур, подготовка презентации.

**СРС 4 Изучение методов защиты от вредоносного ПО.**

Обзор различных типов вредоносного ПО, анализ методов обнаружения и защиты, подготовка обзора.

**СРС 5 Анализ и проектирование системы защиты от утечек информации (DLP).**

Анализ бизнес-процессов, выбор подходящих DLP-инструментов, разработка архитектуры системы.

**СРС 6 Разработка плана обеспечения безопасности облачных вычислений.**

Анализ угроз и рисков, выбор средств защиты, разработка рекомендаций по безопасности.

**СРС 7 Исследование методов социальной инженерии и способов противодействия.**

Анализ методов социальной инженерии, разработка стратегий защиты, подготовка презентации.

**СРС 8 Подготовка реферата по выбранной теме в области интеллектуальных систем защиты информации.**

Выбор темы, сбор и анализ информации, написание реферата.

**СРС 9 Анализ перспективных направлений в развитии ИБ.**

Анализ трендов, подготовка обзора новых технологий, разработка презентации.

**СРС 10 Оценка соответствия требованиям информационной безопасности.**

Проведение аудита, разработка рекомендаций, подготовка отчета.

**СРС 11 Разработка модели угроз и уязвимостей для мобильных устройств.**

Определение угроз, анализ уязвимостей, разработка рекомендаций по защите.

**СРС 12 Изучение методов защиты баз данных.**

Обзор методов защиты, разработка плана защиты, подготовка презентации.

**СРС 13 Разработка стратегии резервного копирования и восстановления данных.**

Выбор стратегии, проектирование инфраструктуры, подготовка документации.

**СРС 14 Разработка плана обучения персонала по вопросам информационной безопасности.**

Определение потребностей в обучении, разработка программы, подготовка материалов.

**СРС 15 Анализ и защита систем виртуализации.**

Обзор уязвимостей, разработка плана защиты, подготовка отчета.

**СРС 16 Подготовка презентации и защита проекта по интеллектуальной системе защиты информации.**

Подготовка доклада, защита проекта, ответы на вопросы.

**СРС 17 Разработка документации по информационной безопасности для организации.**

Разработка политик, инструкций, регламентов.

**СРС 18 Анализ и моделирование киберугроз с использованием специализированных инструментов.**

Использование инструментов моделирования угроз, анализ результатов, подготовка отчета.

**СРС 19 Разработка тестовых сценариев для проверки эффективности систем защиты.**

Разработка тестовых случаев, проведение тестирования, анализ результатов.

**СРС 20 Создание отчета по результатам анализа уязвимостей и выработке рекомендаций по их устранению.**

Анализ результатов, подготовка отчета, выработка рекомендаций.

**СРС 21 Анализ лучших практик в области информационной безопасности.**

Анализ стандартов, подготовка отчета, выработка рекомендаций.

**СРС 22 Разработка стратегии реагирования на инциденты информационной безопасности.**

Разработка процедур, подготовка документации, проведение практических занятий.

**СРС 23 Исследование современных методов анализа угроз и уязвимостей.**

Анализ новых методов, подготовка отчета, выработка рекомендаций.

**СРС 24 Изучение методов защиты веб-приложений и баз данных.**

Анализ существующих методов, разработка плана защиты, подготовка отчета.

**СРС 25 Разработка плана обеспечения безопасности беспроводных сетей.**

Анализ угроз и рисков, выбор средств защиты, разработка рекомендаций.

**СРС 26 Анализ методов защиты от DDOS-атак.**

Обзор методов защиты, разработка плана защиты, подготовка презентации.

**СРС 27 Анализ нормативных актов и стандартов в области ИБ.**

Изучение требований, подготовка отчета, выработка рекомендаций.

**СРС 28 Подготовка к экзамену.**

Повторение материала, решение задач, подготовка к тестированию.

**СРС 29 Подготовка к защите курсовой работы.**

Подготовка презентации, отработка защиты, подготовка к ответам на вопросы.

**СРС 30 Оформление отчетности по самостоятельной работе.**

Сбор и оформление результатов, подготовка к сдаче.

**СРС 31 Подготовка к итоговой аттестации.**

Обобщение знаний, подготовка к экзамену, решение задач.

**СРС 32 Изучение и анализ реальных примеров инцидентов ИБ.**

Разбор кейсов, изучение методов атак, подготовка отчета.

**СРС 33 Разработка плана повышения осведомленности сотрудников об ИБ.**

Разработка плана обучения, подготовка материалов.

**СРС 34 Исследование методов выявления вредоносного ПО на основе машинного обучения.**

Обзор методов, разработка модели, подготовка презентации.

**СРС 35 Создание системы мониторинга информационной безопасности.**

Выбор инструментов, настройка мониторинга, подготовка отчетов.

## Структура и содержание теоретической, лабораторной части курса, КСР и СРС

**Таблица 3.**

| № п/п | Наименование темы | Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах) | | | | | | Литра | Количество баллов |
|---|---|---|---|---|---|---|---|---|---|
| | | Лек | Прак | КСР | Лаб | СРС | ИКР | | |
| 1 | Введение в интеллектуальные системы защиты информации. Основные понятия и определения. | 2 | | | | 4 | | 1 | 12,5 |
| | Ознакомление с инструментами для анализа угроз и уязвимостей. | | 2 | | | | | 4 | |
| 2 | Установка и настройка системы обнаружения вторжений (IDS). | | | | 2 | 4 | | 3 | 12,5 |
| | Разработка требований к интеллектуальной системе защиты информа-ции для конкретной организации. | | | 2 | | | | | |
| 3 | Методы анализа угроз и уязвимостей информационных систем. | 2 | | | | | | 6 | 12,5 |
| | Настройка и использование сетевой системы обнаружения вторжений (IDS). | | 2 | | | 4 | | 5 | |
| 4 | Развертывание и настройка хостовой системы обнаружения вторжений (HIDS). | | | | 2 | | | 4 | 12,5 |
| | Проектирование архитектуры системы обнаружения вторжений (IDS) для заданного сценария. | | | 2 | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 5 | Системы обнаружения вторжений (IDS). Архитектура и принципы рабо-ты. | 2 | | | | 4 | | 2 | 12,5 |
| | Настройка и использование хостовой системы обнаружения вторжений (HIDS). | | 2 | | | | | 5 | |
| 6 | Практическое применение анализатора трафика (Wireshark). | | | | 2 | 4 | | 7 | 12,5 |
| | Разработка модели угроз и уязвимостей для информационной системы. | | | 2 | | | | | |
| 7 | Интеллектуальный анализ трафика и поведения пользователей. | 2 | | | | | | 2 | 12,5 |
| | Анализ сетевого трафика с использованием Wireshark. | | 2 | | | | | 2 | |
| 8 | Анализ вредоносного ПО в песочнице. | | | | 2 | 4 | | 1 | 12,5 |
| 9 | Системы анализа вредоносного ПО. Принципы работы и методы обна-ружения. | 2 | | | | | | 4 | 12,5 |
| | Практическое применение антивирусных решений и песочниц. | | 2 | | | 2 | | 5 | |
| 10 | Настройка и использование системы управления доступом. | | | | 2 | | | 3 | 12,5 |
| | Создание системы анализа логов безопасности (SIEM). | | | 2 | | | | | |
| 11 | Интеллектуальные системы управления доступом и аутентификации. | 2 | | | | 4 | | 2 | 12,5 |
| | Настройка и использование систем управления доступом. | | 2 | | | | | 5 | |
| 12 | Использование DLP-системы для защиты данных. | | | | 2 | 4 | | 6 | 12,5 |
| 13 | Интеллектуальные методы защиты от утечек информации (DLP). | 2 | | | | | | 5 | 12,5 |
| 14 | Использование систем DLP (Data Loss Prevention). | | 2 | | | 4 | | 6 | 12,5 |
| 15 | Разработка простого скрипта для автоматизации задач безопасности. | | | | 2 | | | 5 | 12,5 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Перспективы развития интеллектуальных систем защиты информации. | 2 | | | | 2 | | 4 | |
| 16 | Разработка и внедрение простых скриптов для автоматизации задач без-опасности. | | 2 | | | | | 5 | 12,5 |
| | Внедрение системы SIEM. | | | | 2 | 2 | | 2 | |
| **Итого:** | | 16 | 16 | 8 | 16 | 42 | 0 | | 200 |

## Формы контроля и критерии начисления баллов

Контроль усвоения студентом каждой темы осуществляется в рамках балльно-рейтинговой системы (БРС), включающей текущий, рубежный и итоговый контроль. Студенты **4 -го курса**, обучающиеся по кредитно-рейтинговой системе обучения, могут получить максимально возможное количество баллов - 300. Из них на текущий и рубежный контроль выделяется 200 баллов или 49% от общего количества.

На итоговый контроль знаний студентов выделяется 51% или 100 баллов.

Порядок выставления баллов: 1-й рейтинг (1-7 недели до 12,5 баллов+12,5 баллов (8 неделя – Рубежный контроль №1) = 100 баллов), 2-й рейтинг (9-15 недели до 12,5 баллов+12,5 баллов (16 неделя – Рубежный контроль №2) = 100 баллов), итоговый контроль 100 баллов.

К примеру, за текущий и 1-й рубежный контроль выставляется 100 баллов: лекционные занятия – 21 балл, за практические занятия (КСР, лабораторные) – 31,5 балл, за СРС – 17,5 баллов, требования ВУЗа – 17,5 баллов, рубежный контроль – 12,5 баллов.

В случае пропуска студентом занятий по уважительной причине (при наличии подтверждающего документа) в период академической недели деканат факультета обращается к проректору по учебной работе с представлением об отработке студентом баллов за пропущенные дни по каждой отдельной дисциплине с последующим внесением их в электронный журнал.

Итоговая форма контроля по дисциплине (зачет, экзамен) проводится как в форме тестирования, так и в традиционной (устной) форме. Тестовая форма

итогового контроля по дисциплине предусматривает: для естественнонаучных направлений – 10 тестовых вопросов на одного студента, где правильный ответ оценивается в 10 баллов, для гуманитарных направлений – 25 тестовых вопросов, где правильный ответ оценивается в 4 балла. Тестирование проводится в электронном виде, устный экзамен на бумажном носителе с выставлением оценки в ведомости по аналогичной системе с тестированием.

**Таблица 4.**

| Неделя | Активное участие на лекционных занятиях, написание конспекта и выполнение других видов работ* | Активное участие на практических (семинарских) занятиях, КСР | СРС Написание реферата, доклада, эссе Выполнение других видов работ | Выполнение положения высшей школы (установленная форма одежды, наличие рабочей папки, а также других пунктов устава высшей школы) | РК №1 | Всего |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 2 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 3 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 4 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 5 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 6 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 7 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 8 | - | - | - | - | 12,5 | 12,5 |
| Первый рейтинг | 21 | 31,5 | 17,5 | 17,5 | 12,5 | 100 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 2 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 3 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 4 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 5 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 6 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 7 | 3 | 4,5 | 2,5 | 2,5 | - | 12,5 |
| 8 | - | - | - | - | 12,5 | 12,5 |
| Второй рейтинг | 21 | 31,5 | 17,5 | 17,5 | 12,5 | 100 |
| Итог | | | | | | 200 |

Формула вычисления результатов дистанционного контроля и итоговой

формы контроля по дисциплине за семестр для студентов 4 -го курсов:

$$ИБ = \left[\frac{(P_1 + P_2)}{2}\right] \cdot 0{,}49 + Эи \cdot 0{,}51 \ ,$$

*где ИБ –итоговый балл,* $P_1$- итоги первого рейтинга, $P_2$- итоги второго рейтинга, *Эи*– результаты итоговой формы контроля (экзамен).

## 4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Методы обработки информации» включает в себя:

**1.** план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

**2.** характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

**3.** требования к представлению и оформлению результатов самостоятельной работы;

**4.** критерии оценки выполнения самостоятельной работы.

План-график выполнения самостоятельной работы по дисциплине

### 4.1. План-график выполнения самостоятельной работы по дисциплине

| № | Объем СРС, ч. | Тема СРС | Форма и вид результатов самостоятельной работы | Форма контроля |
|---|---|---|---|---|
| 1 | 4 | Понятие интеллектуальных систем и их применение в защите информации | Вопросы 1–4. Описание технологии разработки, реферат | Опрос |
| 2 | 4 | Искусственный интеллект в информационной безопасности | Вопросы 5–8. Презентация методов | Выступление |
| 3 | 6 | Машинное обучение как основа интеллектуальных систем защиты | Вопросы 8–10. Презентация, доклад | Выступление |
| 4 | 6 | Экспертные системы в информационной безопасности | Вопросы 11–13. Выполнение задания 1 (1–10) | Защита работы, выступление |
| 5 | 4 | Нейронные сети для обнаружения атак | Выполнение задания 1. Конспект, презентация (вопросы 14–15) | Опрос, выступление |

| | | | | |
|---|---|---|---|---|
| 6 | 4 | Методы интеллектуального анализа данных (Data Mining) | Выполнение задания 2 | Защита работы |
| 7 | 6 | Интеллектуальные системы обнаружения вторжений | Вопросы 16–17. Выполнение задания 3 | Защита работы |
| 8 | 6 | Поведенческий анализ пользователей и устройств | Вопросы 16–17. Выполнение задания 4 | Защита работы |
| 9 | 4 | Интеллектуальные средства предотвращения утечек данных | Выполнение задания 5 | Защита работы |
| 10 | 4 | Самообучающиеся системы защиты | Вопросы 18–25. Выполнение задания 6 | Защита работы |
| 11 | 4 | Интеграция интеллектуальных модулей в системы ИБ | Вопросы 26–29. Выполнить задания 2 и описать в терминах классов | Опрос, защита работы |
| 12 | 4 | Этические и правовые аспекты применения ИИ в ИБ | Вопросы 30–31. Реферат. Выполнение задания 7 | Защита реферата, защита работы |
| 13 | 4 | Интеллектуальные системы мониторинга безопасности | Вопросы 32–37. Презентация | Опрос, выступление |
| 14 | 4 | Проектирование интеллектуальной системы защиты информации | Вопросы 38–40. Выполнение задания 8 (1–4) | Защита работы |
| 15 | 4 | Оценка эффективности интеллектуальных систем защиты | Вопросы 41–44. Выполнение задания 9 | Защита работы |
| 16 | 4 | Комплексная интеллектуальная система защиты информации | Вопросы 45–46. Выполнение задания 8 (4–10) | Защита работы |

### 4.2 Характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

Для выполнения задания, прежде всего, необходимо ознакомиться и изучить основные положения теоретических материалов соответствующей темы из литературных источников. Они указаны в разделе «Содержание и структура дисциплины». Конспекты и задания можно выполнить в отдельном тетради или в лекционной (практической) тетради в произвольной форме.

### 4.3 Критерии оценки выполнения самостоятельной работы.

Критерии оценки выполнения самостоятельной работы является полнота освещения вопроса, логичность изложения, проявления самостоятельность в обработке материала.

### 4.4. Критерии оценки выполнения самостоятельной работы.

Самостоятельная работа прививает студентам навыки работы с источниками и учебной литературой, помогает повысить уровень знаний по предмету, которые можно использовать на практике.

Оценка «отлично» выставляется студенту, если индивидуальное задание выполнено полностью и по данной теме защищена лабораторная работа.

Оценка «хорошо» выставляется студенту, если лабораторная работа по теме индивидуального задания защищена, а само индивидуальное задание выполнено с отдельными замечаниями.

Оценка «удовлетворительно» выставляется студенту, если лабораторная работа по теме индивидуального задания защищена, а само индивидуальное задание выполнено не до конца, т.е. не полностью.

Оценка «неудовлетворительно» выставляется студенту, если лабораторная работа по теме индивидуального задания не защищена, а само индивидуальное задание выполнено не до конца, т.е. не полностью.

## 5. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕ- ЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1. Основная литература:

1. 1. Острейковский В.А. Информатика. Учебник для вузов. – М.: Юрайт, 2020. – 464 с.

2. Гаврилов А.В., Гусев А.А. Защита информации в компьютерных системах. Учебник и практикум для вузов. – М.: Юрайт, 2020. – 390 с.

3. Ситников А.Е. Информационная безопасность. Учебник для вузов. – СПб.: Питер, 2019. – 432 с.

4. Баранов В.В., Горбачев А.А. Интеллектуальные системы. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2020. – 384 с.

5. Крупин В.А. Компьютерная безопасность. – М.: ДМК Пресс, 2019. – 512 с.

6. Щербаков А.Ю. Защита информации. Учебник для вузов. – М.: Горячая линия – Телеком, 2019. – 584 с.

7. Липов А. В. Информационная безопасность: учебник и практикум для вузов. – М.: Юрайт, 2020. – 412 с.

## 5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Бройдо В.Л. Компьютерные сети. Учебник для вузов. – СПб.: Питер, 2018. – 496 с.

2. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 2017. – 368 с.

3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы. – М.: Горячая линия – Телеком, 2017. – 606 с.

4. Курбатов С.В. Основы информационной безопасности. – М.: Изд-во РАГС, 2016. – 376 с.

5. Спесивцев А.В. Безопасность компьютерных систем и сетей. – М.: Форум, 2016. – 288 с.

6. Андреев А.А. Защита информации в компьютерных системах и сетях. – М.: Гелиос АРВ, 2015. – 320 с.

7. Зуев А.С. Защита информации в информационных системах. – М.: ИНТУИТ, 2014. – 288 с.

## 5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. 1. Федеральный закон «О персональных данных» (№ 152-ФЗ).

2. Стандарты информационной безопасности ISO 27000.

3. Ресурсы CERT (Computer Emergency Response Team).

4. Сайт компании Microsoft по безопасности.

5. Сайт компании Cisco по безопасности.

## 5.4. Перечень информационных технологий и программного обеспечения

Используются лицензионное программное обеспечение ОС Windows -/11 и программное обеспечение открытого доступа (Open source), среды программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

# 6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для обеспечения систематической и регулярной работы по изучению дисциплины «Интеллектуальные системы защиты информации» и успешного прохождения текущих и итоговых контрольных испытаний студенту рекомендуется придерживаться следующего порядка обучения:

1. Самостоятельно определить объем времени, необходимого для проработки каждой темы.

2. Регулярно изучать каждую тему дисциплины, используя различные формы индивидуальной работы.

3. Согласовывать с преподавателем виды работы по изучению дисциплины.

4. По завершении отдельных тем передавать выполненные работы (рефераты) преподавателю.

Обучение по дисциплине «Интеллектуальные системы защиты информации» строится следующим образом. На лекциях преподаватель дает общую характеристику рассматриваемого вопроса, различные научные концепции или позиции, которые есть по данной теме. Во время лекции рекомендуется составлять конспект, фиксирующий основные положения лекции и ключевые определения по пройденной теме. Во время лекционного занятия необходимо фиксировать все спорные моменты и проблемы, на которых останавливается преподаватель. Потом именно эти аспекты станут предметом самого пристального внимания и изучения на практических занятиях.

При подготовке к практическому занятию обязательно требуется изучение дополнительной литературы по теме занятия. Без использования нескольких источников информации невозможно проведение дискуссии на занятиях, обоснование собственной позиции, построение аргументации. Если обсуждаемый аспект носит дискуссионный характер, следует изучить существующие точки зрения и выбрать тот подход, который вам кажется наиболее верным. При этом следует учитывать необходимость обязательной аргументации собственной позиции. Во время практических занятий рекомендуется активно участвовать в обсуждении рассматриваемой темы, выступать с подготовленными заранее рефератами, докладами и презентациями.

Самостоятельная работа должна соответствовать графику прохождения программы дисциплины. Самостоятельная работа по дисциплине «Интеллектуальные системы защиты информации» включает:

а) работу с литературой;

б) подготовку устного выступления на практическом занятии;

в) подготовку к занятию в интерактивной форме;

г) подготовку реферата с презентацией;

д) подготовку к дискуссии;

е) заполнение хронологической таблицы;

ж) подготовку к текущей и итоговой аттестации по дисциплине.

Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа студентов, которая может осуществляться студентами индивидуально и под руководством преподавателя.

Самостоятельная работа студентов предполагает самостоятельное изучение отдельных тем, дополнительную подготовку студентов к каждому практическому занятию.

Самостоятельная работа студентов является важной формой образовательного процесса. Она реализуется непосредственно в процессе аудиторных занятий, в контакте с преподавателем, а также в библиотеке, дома, при выполнении студентом учебных и творческих задач.

Цель самостоятельной работы студентов - научить студента осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы привить умение в дальнейшем непрерывно повышать свою квалификацию.

При изучении дисциплины организация самостоятельной работы студентов форм представлена следующим образом:

1) внеаудиторная самостоятельная работа;

2)аудиторная самостоятельная работа, которая осуществляется под непосредственным руководством преподавателя.

Аудиторная самостоятельная работа может реализовываться при

проведении практических занятий и во время чтения лекций.

На практических занятиях различные виды самостоятельной работы позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

Для проведения занятий необходимо иметь большой банк заданий, причем эти задания могут быть дифференцированы по степени сложности.

На каждом этапе самостоятельной работы следует разъяснять цели работы, контролировать понимание этих целей студентами, постепенно формируя у них умение самостоятельной постановки задачи и выбора цели.

При чтении лекционного курса непосредственно в аудитории необходимо контролировать усвоение материала основной массой студентов

путем проведения экспресс-опросов по конкретным темам.

На практических занятиях различные виды самостоятельной работы позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

На практических занятиях нужно не менее 1 часа из двух (50% времени) отводить на самостоятельное рассмотрение заданий.

По результатам самостоятельного рассмотрения задания следует выставлять по каждому занятию оценку. Оценка предварительной подготовки студента к практическому занятию может быть сделана путем экспресс-опроса в течение 5, максимум - 10 минут.

По материалам раздела целесообразно выдавать студенту домашнее задание и на последнем практическом занятии по разделу подвести итоги его изучения (например, провести контрольную работу), обсудить оценки каждого студента, выдать дополнительные задания тем студентам, которые хотят повысить оценку.

Результативность самостоятельной работы студентов во многом определяется наличием активных методов ее контроля. Существуют следующие виды контроля:

- входной контроль знаний и умений студентов при начале изучения очередной дисциплины;

- текущий контроль, то есть регулярное отслеживание уровня усвоения материала на лекциях, практических занятиях;

- самоконтроль, осуществляемый студентом в процессе изучения дисциплины при подготовке к контрольным мероприятиям;

- итоговый контроль по дисциплине в виде зачета, зачета с оценкой (в устной форме).

## 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины при кафедре информатики и ИТ РТСУ имеются 4 компьютерных классов. Для занятий используются лицензионное программное обеспечение ОС Windows -7/8/10/11 и программное обеспечение открытого доступа (Open source), среды программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

В Университете созданы специальные условия для обучающихся с ограниченными возможностями здоровья - специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания организаций и другие условия, без которых невозможно или затруднено освоение дисциплины обучающимися с ограниченными возможностями здоровья.

Обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература, а также обеспечивается:

- наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проёмов, лифтов).

## 8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Промежуточная аттестации осуществляется: для зачета – контрольная работа и опрос. Экзамен проводится в форме тестирования. Защита курсового проекта: представляется пояснительная записка и презентация выступления.

Текущий контроль студентов осуществляется путем защиты лабораторных работ, выполнения самостоятельного задания, обсуждения теоретических вопросов.

Контролирующие материалы по дисциплине содержат:

Контрольные вопросы и задания для текущего контроля знаний по дисциплине.

Тестовые задания для промежуточного контроля знаний по дисциплине;

Методические рекомендации и тематика курсового проектирования.

Также указаны критерии оценки курсового проекта.

**Итоговая система оценок по кредитно-рейтинговой системе с использованием буквенных символов**

| Оценка по буквенной системе | Диапазон соответствующих наборных баллов | Численное выражение оценочного балла | Оценка по традиционной системе |
|---|---|---|---|
| **A** | 10 | 95-100 | Отлично |
| **A-** | 9 | 90-94 | |
| **B+** | 8 | 85-89 | Хорошо |
| **B** | 7 | 80-84 | |
| **B-** | 6 | 75-79 | |
| **C+** | 5 | 70-74 | Удовлетворительно |
| **C** | 4 | 65-69 | |
| **C-** | 3 | 60-64 | |

| | | | |
|---|---|---|---|
| **D+** | 2 | 55-59 | |
| **D** | 1 | 50-54 | |
| **Fx** | 0 | 45-49 | Неудовлетвори-тельно |
| **F** | 0 | 0-44 | |

Содержание текущего контроля, промежуточной аттестации, итогового контроля раскрываются в фонде оценочных средств, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС ВО.

ФОС по дисциплине является логическим продолжением рабочей программы учебной дисциплины. ФОС по дисциплине прилагается.