

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 27.02.2025 15:31:35

Уникальный программный ключ:

ca953a0120d891083f939673078ef1a989dae18a

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«Российский университет дружбы народов имени Патриса Лумумбы»**

**Факультет искусственного интеллекта**

(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

### **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

(наименование дисциплины/модуля)

**Рекомендована МССН для направления подготовки/специальности:**

#### **10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

(код и наименование направления подготовки/специальности)

**Освоение дисциплины ведется в рамках реализации основной профессиональной образовательной программы высшего образования (ОП ВО):**

#### **ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)**

(наименование (профиль/специализация) ОП ВО)

2025 г.

## 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность автоматизированных систем» входит в программу бакалавриата «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» по направлению 10.03.01 «Информационная безопасность» и изучается в 7 семестре 4 курса. Дисциплину реализует Кафедра прикладного искусственного интеллекта. Дисциплина состоит из 4 разделов и 4 тем и направлена на изучение методов и средств защиты информации в автоматизированных системах различного назначения. Студенты изучают принципы построения защищённых автоматизированных систем, методы анализа и оценки рисков, а также способы предотвращения, обнаружения и устранения нарушений информационной безопасности.

Целью освоения дисциплины является формирование у студентов знаний и навыков, необходимых для проектирования, внедрения и эксплуатации автоматизированных систем с высоким уровнем информационной безопасности, а также для обеспечения надёжности и устойчивости этих систем к внешним и внутренним угрозам.

## 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Информационная безопасность автоматизированных систем» направлено на формирование у обучающихся следующих компетенций (части компетенций):

*Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)*

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
ПК-1	Способен администрировать средства защиты информации в компьютерных системах и сетях	ПК-1.2 Администрирует средства защиты информации прикладного и системного программного обеспечения; ПК-1.3 Администрирует системы защиты информации автоматизированных систем;
ПК-2	Способен разрабатывать комплекс мер по защите информации в автоматизированных системах при возникновении нештатных ситуаций	ПК-2.1 Обеспечивает функционирование средств защиты информации в автоматизированных системах; ПК-2.2 Восстанавливает работоспособность средств защиты информации в автоматизированных системах при внештатных ситуациях; ПК-2.3 Разрабатывает предложения по совершенствованию средств защиты информации автоматизированных систем;

## 3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Информационная безопасность автоматизированных систем» относится к части, формируемой участниками образовательных отношений блока 1 «Дисциплины (модули)» образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Информационная безопасность автоматизированных систем».

*Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины*

<b>Шифр</b>	<b>Наименование компетенции</b>	<b>Предшествующие дисциплины/модули, практики*</b>	<b>Последующие дисциплины/модули, практики*</b>
ПК-1	Способен администрировать средства защиты информации в компьютерных системах и сетях	<i>Сетевое и системное администрирование**;</i> <i>Построение и защита корпоративных информационных сетей**;</i>	Преддипломная практика;
ПК-2	Способен разрабатывать комплекс мер по защите информации в автоматизированных системах при возникновении нештатных ситуаций	<i>Специальные разделы математики (методы оптимизации)**;</i> <i>Моделирование процессов и систем защиты информации**;</i> <i>Гуманитарные аспекты информационной безопасности**;</i> <i>Основы информационного противоборства**;</i>	<i>Основы управления инцидентами информационной безопасности**;</i> <i>Основы управления непрерывностью бизнеса**;</i> Преддипломная практика;

\* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО

\*\* - элективные дисциплины /практики

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Информационная безопасность автоматизированных систем» составляет «4» зачетные единицы.

Таблица 4.1. Виды учебной работы по периодам освоения образовательной программы высшего образования для очной формы обучения.

Вид учебной работы	ВСЕГО, ак.ч.		Семестр(-ы)
			7
<i>Контактная работа, ак.ч.</i>	68		68
Лекции (ЛК)	34		34
Лабораторные работы (ЛР)	34		34
Практические/семинарские занятия (СЗ)	0		0
<i>Самостоятельная работа обучающихся, ак.ч.</i>	58		58
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	18		18
<b>Общая трудоемкость дисциплины</b>	<b>ак.ч.</b>	<b>144</b>	<b>144</b>
	<b>зач.ед.</b>	<b>4</b>	<b>4</b>

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
Раздел 1	Основные понятия в области информационной безопасности.	1.1	Угрозы, уязвимости, атаки, инциденты. Моделирование угроз. Модель нарушителя. Меры и основные принципы обеспечения безопасности информационных технологий.	ЛК, ЛР
Раздел 2	Распределённые прикладные системы как объект защиты.	2.1	Архитектура распределённых приложений. Модель «клиент-сервер», двухзвенные, трёхзвенные архитектуры. Web-приложения. Уровни информационной инфраструктуры. Жизненный цикл автоматизированных систем. Анализ сценариев возможных атак на автоматизированные системы.	ЛК, ЛР
Раздел 3	Многоуровневый подход к защите прикладных систем.	3.1	Сегментирование, разделение информационных потоков распределённых систем. Межсетевые экраны, фильтрация трафика, анализ содержимого трафика, NGFW. Обнаружение сетевых атак IPS\IDS\WAF.	ЛК, ЛР
Раздел 4	Методы защиты автоматизированных систем.	4.1	Защита от несанкционированного доступа. Мониторинг событий безопасности. Подходы к шифрованию данных. Меры защиты от утечек.	ЛК, ЛР

\* - заполняется только по **ОЧНОЙ** форме обучения: ЛК – лекции; ЛР – лабораторные работы; СЗ – практические/семинарские занятия.

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 6.1. Материально-техническое обеспечение дисциплины

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
Лекционная	Лекционный класс для практической подготовки, проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Комплект специализированной мебели: учебная доска; технические средства: Интерактивная панель 86 дюймов HUAWEI idea Hub S2 IHS2-86SA со встраиваемым OPS компьютером HUAWEI в комплекте с подвижной подставкой HUAWEI idea Hub White Rolling Stand_25, Двух объективная PTZ-видеокамера Nearity V520d, Системный блок CPU Intel Core I9-13900F/MSI PRO Z790-S Soc-1700 Intel Z790 / Samsung DDR5 16GB DIMM 5600MHz 2шт/ Samsung SSD 1Tb /Видеокарта RTX3090 2; Монитор LCD LG 27" 27UL500-W белый IPS 3840x2160 5ms 300cd 1000:1 (Mega DCR) DisplayPort P HDMIx2 Audioout, vesa. Программное обеспечение: продукты Microsoft (OC, пакет офисных приложений, в т. ч. MS Office/Office 365, Teams, Skype). Количество посадочных мест - 28.
Семинарская	Лаборатория для проведения практической подготовки, практико-лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной	Комплект специализированной мебели: учебная доска; технические средства: Интерактивная панель 86 дюймов HUAWEI idea Hub S2 IHS2-86SA со встраиваемым OPS компьютером HUAWEI в комплекте с подвижной подставкой HUAWEI idea Hub White Rolling Stand_25, Двух объективная PTZ-видеокамера Nearity V520d, Системный блок CPU Intel Core I9-13900F/MSI PRO Z790-S Soc-1700 Intel Z790 / Samsung DDR5 16GB DIMM 5600MHz 2шт/ Samsung SSD 1Tb /Видеокарта RTX3090 2; Монитор LCD LG 27"

	аттестации.	27UL500-W белый IPS 3840x2160 5ms 300cd 1000:1 (Mega DCR) DisplayPort P HDMIx2 Audioout, vesa. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/Office 365, Teams, Skype). Количество посадочных мест - 25.
Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	Компьютерный класс для практической подготовки, проведения занятий практико-лабораторного характера, самостоятельной работы, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Комплект специализированной мебели; учебная доска; технические средства: Моноблок HP ProOne 440 Intel I5 10500T/8 GB/256 GB/audio, монитор 24"; Мультимедиа проектор Casio XJ-V100W; Экран, моторизованный Digis Electra 200*150 Dsem-4303 Программное обеспечение: Продукты Microsoft (MS Windows, MS Office) – подписка Enrollment for Education Solution (EES) №56278518 от 23.04.2019
		Компьютерный класс - учебная аудитория для практической подготовки, лабораторно-практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также самостоятельной работы Комплект специализированной мебели; (в т.ч. электронная доска); мультимедийный проектор BenqMP610; экран моторизованный Sharp 228*300; доска аудиторная поворотная; Комплект ПК iRU Corp 317 TWR i7 10700/16GB/ SSD240GB/2TB 7.2K/ GTX1660S-6GB /WIN10PRO64/ BLACK + Комплект Logitech Desktop MK120, (Keyboard&mouse), USB, [920-002561] + Монитор HP P27h G4 (7VH95AA#ABB) (УФ-00000000059453)-5шт., Компьютер Pirat Doctrin4шт., ПО для ЭВМ LiraServis Academic Set 2021 Состав пакета ACADEMIC SET: программный комплекс "ЛИРА-САПР FULL". программный комплекс "МОНОМАХ-САПР PRO". программный комплекс "ЭСПРИ.

\* - аудитория для самостоятельной работы обучающихся указывается **ОБЯЗАТЕЛЬНО!**

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### Основная литература:

1. Грушо, А. А. Кибербезопасность предприятия : учебное пособие / А.А. Грушо, Е.Е. Тимонина. – Электронные текстовые данные . – Москва : РУДН, 2023. – 78 с. : ил. URL: [https://lib.rudn.ru/MegaPro/UserEntry?Action=Link\\_FindDoc&id=510195&idb=0](https://lib.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=510195&idb=0).

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/511998> (дата обращения: 24.11.2023).

3. Стасышин, В. М. Базы данных: технологии доступа : учебное пособие для вузов / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 164 с. — (Высшее образование). — ISBN 978-5-534-08687-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/514252> (дата обращения: 24.11.2023).

### Дополнительная литература:

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст :

электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/515435> (дата обращения: 20.11.2023).

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/513300> (дата обращения: 20.11.2023).

*Ресурсы информационно-телекоммуникационной сети «Интернет»:*

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров

- Электронно-библиотечная система РУДН – ЭБС РУДН

<http://lib.rudn.ru/MegaPro/Web>

- ЭБС «Университетская библиотека онлайн» <http://www.biblioclub.ru>

- ЭБС Юрайт <http://www.biblio-online.ru>

- ЭБС «Консультант студента» [www.studentlibrary.ru](http://www.studentlibrary.ru)

- ЭБС «Троицкий мост»

2. Базы данных и поисковые системы

- электронный фонд правовой и нормативно-технической документации

<http://docs.cntd.ru/>

- поисковая система Яндекс <https://www.yandex.ru/>

- поисковая система Google <https://www.google.ru/>

- реферативная база данных SCOPUS

<http://www.elsevierscience.ru/products/scopus/>

*Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля\*:*

1. Курс лекций по дисциплине «Информационная безопасность автоматизированных систем».

\* - все учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины **в ТУИС!**

## **8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ**

Оценочные материалы и балльно-рейтинговая система\* оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Информационная безопасность автоматизированных систем» представлены в Приложении к настоящей Рабочей программе дисциплины.

\* - ОМ и БРС формируются на основании требований соответствующего локального нормативного акта РУДН.