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

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

(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 «Методы и средства криптографической защиты информации» 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 1 раздела и 18 тем и направлена на изучение основ криптографии, алгоритмов шифрования и дешифровки данных, а также методов аутентификации и цифровой подписи. Студенты изучают принципы работы симметричных и асимметричных криптосистем, современные стандарты шифрования, такие как AES и RSA, а также методы реализации криптографических протоколов в информационных системах.

Целью освоения дисциплины является формирование у студентов глубоких знаний в области криптографии и её применения для защиты информации, а также развитие навыков использования криптографических средств для обеспечения конфиденциальности, целостности и подлинности передаваемых данных.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Методы и средства криптографической защиты информации» 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)
ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1 Знает необходимые математические методы для решения задач профессиональной деятельности; ОПК-3.2 Использует необходимые математические методы для решения задач профессиональной деятельности;
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1 Применяет средства криптографической защиты информации для решения задач профессиональной деятельности;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Методы и средства криптографической защиты информации» относится к обязательной части 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 «Методы и средства криптографической защиты информации».

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

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности	Эксплуатационная практика; Математика (математический анализ, линейная алгебра и аналитическая геометрия); Теория вероятностей и математическая статистика; Математическая логика и теория алгоритмов; Дискретная математика;	Технологическая практика;
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Эксплуатационная практика; Аппаратные средства вычислительной техники; Защита информации от утечки по техническим каналам; Физические основы защиты информации;	Технологическая практика; Комплексное обеспечение защиты информации объекта информатизации;

* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО
** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Методы и средства криптографической защиты информации» составляет «5» зачетных единиц.

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
Контактная работа, ак.ч.	*68*		*68*
Лекции (**ЛК**)	34		34
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	34		34
Самостоятельная работа обучающихся, ак.ч.	*85*		*85*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
Общая трудоемкость дисциплины	**ак.ч.**	***180***	*180*
	зач.ед.	***5***	*5*

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	Методы и средства криптографической защиты информации	1.1	История криптографии	ЛК, СЗ
		1.2	Основные понятия криптографии	ЛК, СЗ
		1.3	Криптография и прикладная математика	ЛК, СЗ
		1.4	Модели открытого текста. Критерии открытого текста	ЛК, СЗ
		1.5	Шифры перестановки и шифры замены	ЛК, СЗ
		1.6	Шифры гаммирования	ЛК, СЗ
		1.7	Стойкость криптографических преобразований и шифрсистем	ЛК, СЗ
		1.8	Поточные шифры. Генерация псевдослучайных последовательностей	ЛК, СЗ
		1.9	Блочные шифры	ЛК, СЗ
		1.10	Системы шифрования с открытыми ключами	ЛК, СЗ
		1.11	Электронная цифровая подпись	ЛК, СЗ
		1.12	Методы проверки подлинности объектов коммуникации. Идентификация объекта	ЛК, СЗ
		1.13	Функции хеширования	ЛК, СЗ
		1.14	Управление ключами	ЛК, СЗ
		1.15	Основы технологии инфраструктур открытых ключей	ЛК, СЗ
		1.16	Криптографические методы обеспечения информационной безопасности в сети Internet	ЛК, СЗ
		1.17	Практические аспекты использования шифрсистем	ЛК, СЗ
		1.18	Нормативная база в области криптографической защиты информации	ЛК, СЗ

* - 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 (ОС, пакет офисных приложений, в т. ч. MS Office/Office 365, Teams, Skype). Количество посадочных мест - 28.
Семинарская	Лаборатория для проведения практической	Комплект специализированной мебели: учебная доска; технические средства: Интерактивная панель 86 дюймов HUAWEI idea Hub S2 IHS2-86SA со

	подготовки, практико-лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	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 (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, (Keybord&mouse), USB, [920-002561] + Монитор HP P27h G4 (7VH95AA#ABB) (УФ-000000000059453)-5шт., Компьютер Pirit 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. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информациит 2-е изд. Учебник для академического бакалавриата. 2016 г.

2. Кириллов И.А. Криптографическая защита информации. – М.: ИПК МГЛУ Рема, 2010.

3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005.

4. Бабенко Л.К., Ищукова Е.А. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: СИММЕТРИЧНОЕ ШИФРОВАНИЕ. Учебное пособие для вузов. 2016.

5. Грушо А.А., Тимонина Е.Е., Применко Э.А. Теоретические основы компьютерной безопасности. М.: Academia, 2009.

Дополнительная литература:

1. Шеннон К. Теория связи в секретных системах.// В кн.: Работы по теории информации и кибернетике. – М.:ИЛ, 1963.
2. Фомичев В.М., Мельников Д.А. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В 2 Ч. ЧАСТЬ 1. МАТЕМАТИЧЕСКИЕ АСПЕКТЫ. Учебник для академического бакалавриата. 2016.
3. Фомичев В.М., Мельников Д.А. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В 2 Ч. ЧАСТЬ 2. МАТЕМАТИЧЕСКИЕ АСПЕКТЫ. Учебник для академического бакалавриата. 2016.
4. Сингх С. Книга шифров. М.: АСТ-Астрель, 2006.
5. Черчхаус Р. Коды и шифры. М.: Весь мир, 2005.
6. Соболева Т.А. Тайнопись в истории России. История криптографической службы России XVIII – начало XX в. М.: Международные отношения, 1994.
7. Э.А.Применко. Алгебраические основы криптографии. М.: Книжный дом «ЛИБРОКОМ», 2014.

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
   - 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 «Методы и средства криптографической защиты информации».

* - 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 «Методы и средства криптографической защиты информации» представлены в Приложении к настоящей Рабочей программе дисциплины.

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