Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов имени Патриса Лумумбы»

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КРИПТОЛОГИЯ И ПРАКТИКА ШИФРОВАНИЯ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

02.04.02 ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
(код и наименование направления подготовки/специальности)

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

АНАЛИЗ БОЛЬШИХ ДАННЫХ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ
(наименование (профиль/специализация) ОП ВО)

2023 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Криптология и практика шифрования» входит в программу магистратуры «Анализ больших данных и технологии защиты информации» по направлению 02.04.02 «Фундаментальная информатика и информационные технологии» и изучается во 2, 3 семестрах 1, 2 курсов. Дисциплину реализует Департамент механики и процессов управления. Дисциплина состоит из 6 разделов и 21 тема и направлена на изучение фундаментальных основ реализации криптографических и иных, связанных с безопасностью, функциональных возможностей в приложениях .NET; разбор основных методов решения типовых задач и знакомство с областью их применения в профессиональной деятельности.

Целью освоения дисциплины является формирование фундаментальных знаний и навыков применения методов решения задач, необходимых для профессиональной деятельности, повышение общего уровня цифровой грамотности студентов, чтобы научить их применять на практике криптографические возможности среды .NET.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Криптология и практика шифрования» 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 проводить анализ математических моделей, создавать инновационные методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования	ОПК-3.1 Знает основные подходы к решению прикладных задач профессиональной деятельности в области информатики и математического моделирования; ОПК-3.2 Умеет проводить анализ математических моделей, обосновывать методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования; ОПК-3.3 Разрабатывает новые алгоритмы и методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования;
ПК-1	Способен формулировать цели, задачи научных исследований в области защиты информации, выбирать методы и средства решения задач	ПК-1.1 Знает методы и средства решения задач научных исследований в области защиты информации; ПК-1.2 Умеет формулировать цель и задачи научных исследований в профессиональной области, готовить к публикации результаты научных исследований и формировать документы для подачи заявки на изобретение; ПК-1.3 Владеет приемами для формулировки цели и задач научных исследований, умеет выбирать методы и средства решения задач профессиональной деятельности;
ПК-2	Способен применять методы и технологии защиты информации для решения задач управления проектами в области информационных технологий в условиях неопределенностей и рисков информационных угроз	ПК-2.1 Знает современные теоретические и экспериментальные методы, применяемые для разработки технологий защиты информации и процессов профессиональной деятельности; ПК-2.2 Умеет определять эффективность применяемых методов для разработки технологий защиты информации и процессов профессиональной деятельности; ПК-2.3 Владеет современными теоретическими и экспериментальными методами для разработки технологий защиты информации и процессов профессиональной деятельности;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Криптология и практика шифрования» 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 «Криптология и практика шифрования».

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 проводить анализ математических моделей, создавать инновационные методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования	Информационные технологии в математическом моделировании; Численные методы решения задач математического моделирования; Машинное обучение и анализ больших данных; Статистические методы анализа данных; Анализ уязвимостей программного обеспечения;	Преддипломная практика;
ПК-1	Способен формулировать цели, задачи научных исследований в области защиты информации, выбирать методы и средства решения задач		Научно-исследовательская работа; Преддипломная практика;
ПК-2	Способен применять методы и технологии защиты информации для решения задач управления проектами в области информационных технологий в условиях неопределенностей и рисков информационных угроз	Статистические методы анализа данных; Машинное обучение и анализ больших данных;	Научно-исследовательская работа; 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 «Криптология и практика шифрования» составляет «10» 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)**	
			2	**3**
Контактная работа, ак.ч.	*108*		*72*	*36*
Лекции (**ЛК**)	54		36	18
Лабораторные работы (**ЛР**)	54		36	18
Практические/семинарские занятия (**СЗ**)	0		0	0
Самостоятельная работа обучающихся, ак.ч.	*207*		*153*	*54*
Контроль (экзамен/зачет с оценкой), ак.ч.	*45*		*27*	*18*
Общая трудоемкость дисциплины	**ак.ч.**	***360***	*252*	*108*
	зач.ед.	***10***	*7*	*3*

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	Криптография и безопасность в .NET	1.1	Криптография и безопасность в .NET. Природа криптографии и других средств обеспечения безопасности.	ЛК, ЛР
		1.2	Безопасность в Windows: возраст зрелости. Среда разработки .NET Framework и "виртуальная машина" CRL	ЛК, ЛР
		1.3	Программирование с использованием криптографии в .NET. Программирование с использованием средств обеспечения безопасности в .NET.	ЛК, ЛР
Раздел 2	Основы криптографии	2.1	Основы криптографии. Основные термины криптографии	ЛК, ЛР
		2.2	Секретные ключи против секретных алгоритмов. Классические методы сохранения тайны	ЛК, ЛР
		2.3	Стеганография. Современные шифры	ЛК, ЛР
		2.4	Симметричная криптография. Асимметричная криптография	ЛК, ЛР
		2.5	Криптографические алгоритмы. Криптографические протоколы. Криптоаналитические атаки	ЛК, ЛР
Раздел 3	Симметричная криптография	3.1	Симметричная криптография. Симметричные шифры. DES. Тройной DES. Rijndael.	ЛК, ЛР
		3.2	Основные криптографические классы - класс SymmetricAlgorithm и производные от него	ЛК, ЛР
		3.3	Проблемы передачи ключей. Шифрованные хеши и целостность сообщения	ЛК, ЛР
		3.4	Хеш-алгоритмы с ключом и целостность сообщения	ЛК, ЛР
Раздел 4	Асимметричная криптография	4.1	Асимметричная криптография. Проблемы, связанные с использованием симметричных алгоритмов: проблема распределения ключей и проблема доверия	ЛК, ЛР
		4.2	Идея асимметричной криптографии. RSA: самый распространенный асимметричный алгоритм	ЛК, ЛР
		4.3	Программирование при помощи .NET Asymmetric Cryptography. Сохранение ключей в формате XML. Цифровые сертификаты	ЛК, ЛР
Раздел 5	Цифровая подпись. Хеш-алгоритмы	5.1	Цифровая подпись. Хеш-алгоритмы. Характеристики хорошей хеш-функции	ЛК, ЛР
		5.2	Класс HashAlgorithm. Классы MD5 и SHA	ЛК, ЛР
		5.3	Класс KeyedHashAlgorithm. RSA в качестве алгоритма цифровой подписи	ЛК, ЛР
		5.4	Алгоритм цифровой подписи DSA Иерархия класса AsymmetricAlgorithm. Класс DSACryptoServiceProvider	ЛК, ЛР
Раздел 6	Криптография и XML	6.1	Криптография и XML. XML Encryption - шифрование XML	ЛК, ЛР
		6.2	XML Signatures - подпись XML	ЛК, ЛР

* - заполняется только по **ОЧНОЙ** форме обучения: *ЛК – лекции; ЛР – лабораторные работы; СЗ – 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	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническими средствами мультимедиа презентаций.	
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве 15 шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	
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.	

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.

2. Глухов М.М. Пичкур А.Б. Черемушкин А.В. Введение в теоретико-числовые методы криптографии. - Санкт-Петербург: Лань, 2011. - 400 с.

3. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. - М.: Физматлит, 2012. - 280с.

4. Введение в теоретико-числовые методы криптографии : учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090101 "Криптография" / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин, Санкт-Петерург [и др.] : Лань, 2011, 394 с.

Дополнительная литература:

1. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012.

2. Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с.

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 «Криптология и практика шифрования».

* - 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 «Криптология и практика шифрования» представлены в Приложении к настоящей Рабочей программе дисциплины.

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

РАЗРАБОТЧИК:

Доцент		Варфоломеев Александр Алексеевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Директор ДМПУ		Разумный Юрий Николаевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Доцент		Варфоломеев Александр Алексеевич
Должность, БУП	*Подпись*	*Фамилия И.О.*