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:

27.04.04 УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ СИСТЕМАХ
(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)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Криптология и практика шифрования» входит в программу магистратуры «Анализ больших данных и технологии защиты информации» по направлению 27.04.04 «Управление в технических системах» и изучается во 2, 3 семестрах 1, 2 курсов. Дисциплину реализует Кафедра 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-4	Способен осуществлять оценку эффективности результатов разработки систем управления математическими методами	ОПК-4.1 Знает основные математические методы применяемые для оценки эффективности результатов систем управления;; ОПК-4.2 Умеет применять математические методы для оценки эффективности результатов систем управления;; ОПК-4.3 Владеет методами для проведения оценки эффективности результатов систем управления.;
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-4	Способен осуществлять оценку эффективности результатов разработки систем управления математическими методами	Машинное обучение и анализ больших данных;	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;		Преддипломная практика; Научно-исследовательская работа;

* - 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	Наименование темы		Содержание 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.	Природа криптографии как науки о методах защиты информации. Место криптографии в общей системе обеспечения информационной безопасности. Взаимосвязь криптографических и некриптографических средств защиты, включая аутентификацию, контроль доступа и аудит. Роль криптографии в защите данных при хранении и передаче.	ЛК, ЛР
		1.2	Безопасность в Windows: возраст зрелости. Среда разработки .NET Framework и "виртуальная машина" CRL	Эволюция механизмов безопасности операционной системы Windows. Уровни зрелости подсистем безопасности. Архитектура безопасности Windows: идентификаторы безопасности, списки управления доступом, привилегии и токены доступа. Среда разработки .NET Framework. Общая языковая среда выполнения Common Language Runtime как «виртуальная машина». Механизмы безопасности CLR: управляемый код, контроль типов, проверка доказательств.	ЛК, ЛР
		1.3	Программирование с использованием криптографии в .NET. Программирование с использованием средств обеспечения безопасности в .NET.	Пространства имён .NET Framework для криптографии. Программирование симметричных и асимметричных алгоритмов. Работа с хеш-функциями и цифровыми подписями. Программирование средств безопасности: управление доступом к коду, разрешения и наборы разрешений. Обработка криптографических исключений и безопасное управление ключевой информацией.	ЛК, ЛР
Раздел 2	Основы криптографии	2.1	Основы криптографии. Основные термины криптографии	Понятия: открытый текст, шифротекст, шифрование, дешифрование, ключ. Классификация криптографических алгоритмов: симметричные, асимметричные, хеш-функции. Основные свойства криптографических систем: стойкость, производительность, сложность реализации. Понятие криптографического протокола.	ЛК, ЛР
		2.2	Секретные ключи против секретных алгоритмов. Классические методы сохранения тайны	Принцип Керкгоффса: безопасность системы только в секретности ключа, но не алгоритма. Сравнительный анализ подходов: секретный алгоритм против открытого алгоритма с секретным ключом. Классические методы сохранения тайны: шифры замены, включая моноалфавитные и полиалфавитные, а также шифры перестановки. Примеры: шифр Цезаря, шифр	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				Виженера. Уязвимости классических методов перед частотным анализом.	
		2.3	Стеганография. Современные шифры	Стеганография как метод сокрытия самого факта передачи информации. Отличие стеганографии от криптографии. Классические стеганографические методы: невидимые чернила, микроточки, сокрытие в графических и аудиофайлах. Современные стеганографические технологии в цифровых изображениях, аудио и видео. Понятие пропускной способности стеганоканала и устойчивости к стегоанализу. Современные шифры: блочные и поточные. Принципы построения современных шифров: диффузия и конфузия по К. Шеннону.	ЛК, ЛР
		2.4	Симметричная криптография. Асимметричная криптография	Симметричная криптография: один общий секретный ключ для шифрования и дешифрования. Достоинства: высокая скорость, простота аппаратной реализации. Недостатки: проблема распределения ключей. Асимметричная криптография: пара ключей из открытого и закрытого. Шифрование открытым ключом, дешифрование закрытым. Использование асимметричной криптографии для конфиденциальности и аутентификации. Понятие односторонней функции и функции с потайным входом.	ЛК, ЛР
		2.5	Криптографические алгоритмы. Криптографические протоколы. Криптоаналитические атаки	Криптографические алгоритмы: формальное определение, требования к стойкости. Примеры современных алгоритмов: AES, RSA, ECC, хеш-функции семейства SHA. Криптографические протоколы: протоколы аутентификации Kerberos, протоколы обмена ключами Diffie-Hellman, протоколы с нулевым разглашением. Криптоаналитические атаки: атака только по шифротексту, атака с известным открытым текстом, атака с выбранным открытым текстом, атака с выбранным шифротекстом. Понятие вычислительной стойкости и абсолютно стойких систем на примере одноразового блокнота Вернама.	ЛК, ЛР
Раздел 3	Симметричная криптография	3.1	Симметричная криптография. Симметричные шифры. DES. Тройной DES. Rijndael.	Общая схема симметричного шифрования. Режимы работы блочных шифров.Требования к раундовым ключам и функциям преобразования.	ЛК, ЛР
		3.2	Основные криптографические классы -	Пространство имён System.Security.Cryptography. Абстрактный	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
			класс SymmetricAlgorithm и производные от него	базовый класс SymmetricAlgorithm: свойства BlockSize, KeySize, Key, IV, Mode, Padding и методы CreateEncryptor, CreateDecryptor, GenerateKey, GenerateIV. Производные классы: DESCryptoServiceProvider, TripleDESCryptoServiceProvider, AesCryptoServiceProvider, AesManaged. Правильная инициализация вектора инициализации IV и ключа. Режимы заполнения Padding: PKCS7, Zeros, ANSIX923, ISO10126. Примеры программной реализации шифрования и дешифрования с использованием производных классов.	
		3.3	Проблемы передачи ключей. Шифрованные хеши и целостность сообщения	Проблема передачи симметричных ключей по незащищённым каналам связи. Методы решения: использование защищённых физических каналов, предварительное распределение ключей, протоколы согласования ключей, например Diffie-Hellman. Шифрованные хеши или хеш-функции как средство контроля целостности сообщения. Понятие имитовставки Message Authentication Code, MAC. Отличие MAC от цифровой подписи. Способы вычисления MAC: на основе блочных шифров CBC-MAC, CMAC и на основе хеш-функций HMAC. Обеспечение одновременной конфиденциальности и целостности: схемы Encrypt-then-MAC, MAC-then-Encrypt, Encrypt-and-MAC.	ЛК, ЛР
		3.4	Хеш-алгоритмы с ключом и целостность сообщения	Хеш-алгоритмы с ключом Keyed Hash Algorithms. Конструкция HMAC Hash-based Message Authentication Code: внутренний и внешний заполнители, двойное хеширование. Свойства HMAC: стойкость к коллизиям, невозможность восстановления ключа по известным парам сообщение и HMAC. Алгоритм HMAC в .NET: класс HMAC, производные HMACMD5, HMACSHA1, HMACSHA256, HMACSHA384, HMACSHA512. Требования к длине и случайности ключа. Целостность сообщения с использованием HMAC: сравнение вычисленного и переданного кода аутентификации. Применение HMAC в сетевых протоколах TLS, IPSec и API-аутентификации.	ЛК, ЛР
Раздел 4	Асимметричная криптография	4.1	Асимметричная криптография. Проблемы, связанные с использованием симметричных алгоритмов: проблема распределения ключей и проблема доверия	Две фундаментальные проблемы симметричной криптографии: проблема распределения ключей и проблема доверия. Экспоненциальный рост числа ключей при увеличении числа участников обмена. Невозможность неопровержимости	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				авторства сообщения. Ограничения симметричной криптографии в открытых системах, включая сеть Интернет.	
		4.2	Идея асимметричной криптографии. RSA: самый распространенный асимметричный алгоритм	Использование пары ключей: открытого для шифрования и закрытого для дешифрования. Вычислительная невозможность получения закрытого ключа из открытого. Понятие односторонней функции с потайным входом. Алгоритм RSA как наиболее распространённый асимметричный алгоритм. Области применения: обеспечение конфиденциальности и цифровая подпись. Рекомендуемые размеры ключей RSA на современном этапе.	ЛК, ЛР
		4.3	Программирование при помощи .NET Asymmetric Cryptography. Сохранение ключей в формате XML. Цифровые сертификаты	Пространство имён System.Security.Cryptography. Абстрактный базовый класс AsymmetricAlgorithm. Классы RSA и RSACryptoServiceProvider. Методы шифрования, дешифрования, создания и проверки цифровой подписи. Сохранение ключей в формате XML. Цифровые сертификаты X.509. Класс X509Certificate2. Хранение сертификатов в хранилищах Windows. Извлечение открытого ключа из сертификата.	ЛК, ЛР
Раздел 5	Цифровая подпись. Хеш-алгоритмы	5.1	Цифровая подпись. Хеш-алгоритмы. Характеристики хорошей хеш-функции	Цифровая подпись как аналог собственноручной подписи в электронном виде. Хеш-алгоритмы как неотъемлемая часть цифровой подписи. Характеристики хорошей хеш-функции: детерминированность, необратимость, устойчивость к коллизиям, лавинный эффект. Схема формирования и проверки цифровой подписи. Отличие цифровой подписи от кода аутентификации сообщения.	ЛК, ЛР
		5.2	Класс HashAlgorithm. Классы MD5 и SHA	Пространство имён System.Security.Cryptography. Абстрактный базовый класс HashAlgorithm. Алгоритм MD5: размер хеша 128 бит, известные уязвимости. Алгоритмы семейства SHA: SHA1 размер 160 бит, уязвимость и вывод из доверенного использования. SHA2: SHA256, SHA384, SHA512. Рекомендации по выбору хеш-алгоритма в современных системах.	ЛК, ЛР
		5.3	Класс KeyedHashAlgorithm. RSA в качестве алгоритма цифровой подписи	Класс KeyedHashAlgorithm как базовый для хеш-алгоритмов с ключом. Использование RSA для цифровой подписи: вычисление хеша сообщения и его шифрование закрытым ключом отправителя. Проверка подписи: расшифровка	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				открытым ключом и сравнение с вычисленным хешем. Методы SignData и VerifyData класса RSA.	
		5.4	Алгоритм цифровой подписи DSA Иерархия класса AsymmetricAlgorithm. Класс DSACryptoServiceProvider	Алгоритм цифровой подписи DSA. Отличие DSA от RSA: использование только для подписи, но не для шифрования. Математическая основа DSA: дискретное логарифмирование. Иерархия класса AsymmetricAlgorithm. Класс DSA. Производный класс DSACryptoServiceProvider. Формирование и проверка подписи DSA. Применение DSA в государственных и корпоративных стандартах электронной подписи.	ЛК, ЛР
Раздел 6	Криптография и XML	6.1	Криптография и XML. XML Encryption - шифрование XML	Стандарт XML Encryption от W3C для обеспечения конфиденциальности XML-документов. Симметричное и асимметричное шифрование XML-данных. Шифрование всего документа или отдельных элементов. Элементы EncryptedData и EncryptedKey. Пространство имён System.Security.Cryptography.Xml. Классы EncryptedData, EncryptedKey, EncryptedXml. Программное шифрование и дешифрование XML-документов в .NET.	ЛК, ЛР
		6.2	XML Signatures - подпись XML	Стандарт XML Signature для обеспечения целостности, аутентификации и неопровержимости XML-документов. Типы подписей: завернутая, завернутая и отдельная. Элементы Signature, SignedInfo, Reference, DigestMethod, SignatureValue, KeyInfo. Проблема каноникализации XML перед подписанием. Пространство имён System.Security.Cryptography.Xml. Классы SignedXml, Reference, KeyInfo. Программное создание и проверка XML Signature. Применение сертификатов X.509 для подписи XML. Совместное использование XML Encryption и XML Signature для обеспечения конфиденциальности и целостности XML-данных.	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	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 ____ 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 https://mega.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 «Знаниум» https://znanium.ru/

2. Базы данных и поисковые системы

- Sage https://journals.sagepub.com/
- Springer Nature Link https://link.springer.com/
- Wiley Journal Database https://onlinelibrary.wiley.com/
- Наукометрическая база данных Lens.org https://www.lens.org

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**!

РАЗРАБОТЧИК:

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

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой		Разумный Юрий Николаевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Профессор		Разумный Юрий Николаевич
Должность, БУП	*Подпись*	*Фамилия И.О.*