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)

2026 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 информационной безопасности . Дисциплина состоит из 1 раздела и 19 тем и направлена на изучение основных понятий современной криптографии; основных методов и результатов теории и практики криптографической защиты информации; алгоритмов шифрования и расширфования данных, а также методов аутентификации и цифровой подписи; теоретико-информационных и теоретико-сложностных особенностей и характеристик криптографических систем и криптографических протоколов.

Целью освоения дисциплины является формирование у обучающихся знаний о базовых криптографических системах, схемах и протоколах, их основных параметрах, и практических навыков применения криптографических средств и технологий защиты информации для обеспечения конфиденциальности, целостности и подлинности 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; Специальные разделы математики (методы оптимизации);	Технологическая практика;
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Эксплуатационная практика; Защита информации от утечки по техническим каналам; Физические основы защиты информации;	Технологическая практика;

* - 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	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 1	Методы и средства криптографической защиты информации	1.1	История криптографии	От древнейших времен до средних веков: Сцитала, Табличка Энея, Квадрат Полибия, Шифр Цезаря. Криптография средних веков: Диск Альберти, Таблица Тритемия, Таблица Порта, шифр Кардано, Таблица Виженера. Криптография XVII – XVIII веков: черные кабинеты, астраномические анаграммы, шифры Ришелье и Гронсфельда. Криптография XIX века: шифратор Джефферсона, Шифратор Уитсона и шифр Плейфера, шифры гаммирования. «Военная криптография» Керкгоффса. Криптография мировых войн XX века: колесные шифраторы Энигма и «Хагелин». Математическая теория криптографии Клода Шеннона. Абсолютно надежный шифр. Телефонные шифраторы. Электронные шифраторы второй половины XX века. Стандарт шифрования данных (DES). Криптография с открытым ключом.	ЛК, СЗ
		1.2	Основные понятия криптографии	Открытые и шифрованные сообщения. Закономерности открытых сообщений. Криптология, криптография, криптоанализ. Конфиденциальность. Целостность Имитостойкость. Аутентификация. Ключи, ключевая система, распределение ключей. Симметричная и асимметричная криптография. Шифр (шифрпреобразование) и шифрсистема. Криптография и математика. Основные требования к шифрам. Криптографическая стойкость шифров. Вопросы практической стойкости. Предварительное и линейное шифрование. Блочные и поточные шифры. Аппаратная и программная реализация шифров. Физические и организационные меры при использовании шифрсистем. Темы курсовых работ.	ЛК, СЗ
		1.3	Криптография и прикладная математика	Математики-криптографы: Джеро́ламо Кардано, Франсуа Виет, Галилео Галилей, Христиан Гольдбах, Чарльз Беббидж, Огю́ст Керкго́ффс, Алан Тьюринг, Мариан Реевский, Клод Шеннон, В.Я.Верченко. Первостепенные (для криптографии) разделы дискретной математики: модульная арифметика, кольца вычетов, решение сравнений с неизвестным. Расширенный алгоритм Евклида. Конечные группы, кольца и поля. Малая	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				теорема Ферма, теоремы Эйлера и Лагранжа. Цикличность мультипликативной группы конечного поля. Построение конечных полей. Простые числа. Проверка на простоту. Нахождение больших простых чисел. Основная теорема арифметики и факторизация больших целых чисел. Дискретное логарифмирование.	
		1.4	Модели открытого текста. Критерии открытого текста	Алгебраические модели открытого текста. Языки и алфавиты. Последовательности символов алфавита. Разрешенные и запрещенные биграммы символов алфавита. Критерий запрещенных биграмм. Вероятностные модели открытого текста. Модель на основе вероятности встречаемости отдельных символов. К-граммные модели открытого текста. Модель на основе цепей Маркова. Статистический критерий согласия как критерий распознавания открытого текста. Энтропия и избыточность языка. Вероятностно-энтропийный метод оценки количества смысловых текств К.Шеннона. Комбинаторный метод оценки количества смысловых текстов А.Колмогорова. Расстояние единственности.	ЛК, СЗ
		1.5	Шифры перестановки и шифры замены	Симметричные шифры. Математическая модель шифра перестановки. Маршрутные перестановки. Математическая модель шифра маршрутной перестановки. Элементы криптоанализа шифров перестановки. Метод тотального опробования основных лингвистических единиц. Шифр простой замены. Математическая модель шифра простой замены. Криптоанализ шифра простой замены. Поточные шифры замены. Блочные шифры замены. Многоалфавитные шифры замены. Фундаментальность криптографических преобразований замены и перестановки, «рассеивание и перемешивание». Модель композиции шифров. Дисковые многоалфавитные шифры замены.	ЛК, СЗ
		1.6	Шифры гаммирования	Определение процедуры гаммирования. Шифр одноразового гаммирования случайной равновероятной гаммой. Понятие абсолютно стойкого шифра. Слабости шифра гаммирования неравновероятной гаммой. Слабости шифра гаммирования при повторном использовании гаммы. Метод «протяжки вероятного слова». Книжная гамма. Возможности вскрытия книжной	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				гаммы. Шифрование гаммой короткого периода. Определение длины периода гаммы. Индекс совпадения символов шифрованного текста. Индекс взаимного совпадения. Шифр Виженера. Криптоанализ шифра Виженера. Метод Беббиджа-Касиски криптоанализа шифров гаммирования. Ошибки шифрования и их использование при вскрытии шифров гаммирования.	
		1.7	Стойкость криптографических преобразований и шифрсистем	Правила Керкгоффса Понятие стойкости шифра. Теоретико-информационный и теоретико-сложностной подходы к определению стойкости шифра. Теоретическая стойкость шифра по Шеннону. Понятие практической стойкости шифра. Оценки сложности криптографических алгоритмов. Зависимость между стойкостью шифров и производительностью вычислительной техники. Зависимость между стойкостью шифров и методами криптоанализа. Метод тотального перебора ключей. Различные схемы опробования ключей. Опробования с возвращением. Опробования ключей без возвращения. Эквивалентные ключи. Расстояние единственности.	ЛК, СЗ
		1.8	Поточные шифры. Генерация псевдослучайных последовательностей	Самосинхронизирующиеся шифры. Линейные рекуррентные последовательности над конечными полями. Период линейной рекуррентной последовательности. Математическое описание линейной рекуррентной последовательности. Характеристический многочлен линейной рекуррентной последовательности. Построение линейной рекуррентной последовательности максимального периода. Фильтрующие и комбинирующие генераторы. Аналитические и статистические методы анализа фильтрующих и комбинирующих генераторов. Генераторы с неравномерным движением. Регистры сдвига с нелинейной обратной связью. Алгоритмы поточного шифрования.	ЛК, СЗ
		1.9	Блочные шифры	Принципы блочного шифрования. Основные преимущества блочных шифров. Структура блочного алгоритма шифрования. Сеть Фейстеля. Алгоритм DES. Обобщенная сеть Фейстеля, алгоритм RC4. Алгоритм «Магма» ГОСТ 28147-89. SP-сеть, алгоритм AES. Алгоритм «Кузнечик». Различные режимы	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				использования блочных шифров. Режим электронной кодировочной книги (ECB - Electronic Code Book). Режим сцепления блоков шифрованного текста (CBC - Cipher Block Chaining). Режим обратной связи по шифрованному тексту (CFB - Cipher Feedback). Режим обратной связи по выходу (OFB - Output Feedback). Режим счетчика.	
		1.10	Системы шифрования с открытыми ключами	Основополагающие идеи ассиметричного шифрования. Односторонние математические функции и функции ловушки. Проблема нахождения больших простых чисел. Разложимость целых чисел на простые множители. Проблема факторизации больших целых чисел. Проблема дискретного логарифмирования. Система открытого распределения ключей Диффи-Хеллмана. Шифрсистема RSA. Математическая модель шифра RSA. Открытые и секретные ключи шифрсистемы шифра RSA. Практические аспекты использования шифра RSA. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиса. Шифрсистема Мейера-Мюллера.	ЛК, СЗ
		1.11	Электронная цифровая подпись	Постановка задачи проверки подлинности источника сообщения. Общая схема цифровой подписи. Цифровые подписи на основе симметричных шифрсистем. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровые подписи на основе шифрсистемы RSA. Алгоритм цифровой подписи Фиата-Шамира. Алгоритм цифровой подписи Эль-Гамаля. Алгоритм цифровой подписи Шнора. Алгоритм цифровой подписи, основанный на проблеме дискретного логарифмирования в группе точек эллиптической кривой, алгоритм DSA. Стандарт ГОСТ Р 34.10-2018. Практические аспекты применения цифровой подписи. Инфраструктура электронной цифровой подписи. Сертификаты. Центры сертификации.	ЛК, СЗ
		1.12	Методы проверки подлинности объектов коммуникации. Идентификация объекта	Слабая идентификация с использованием фиксированных паролей. Сильная идентификация «запрос – ответ». «Запрос – ответ» с использованием симметричных алгоритмов шифрования. «Запрос – ответ» с использованием асимметричных алгоритмов шифрования. Протоколы идентификация объекта с нулевым разглашением. Атаки на	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				протоколы идентификация. Подмена запросов. Повторное навязывание запросов либо ответов. Задержка передачи протокольного сообщения. Атака с использованием специально подобранных запросов. Использование злоумышленником своих средств в качестве части телекоммуникационной структуры.	
		1.13	Функции хеширования	Функции хеширования и целостность данных. Основные идеи и методы построения и использования функций хеширования. Код обнаружения изменений MDC. Алгоритм хеширования MD. Алгоритм хеширования SHA. Ключевые функции хеширования. Целостность данных и аутентификация сообщений. Функции хеширования, использующие алгоритмы блочного шифрования. Функция хеширования ГОСТ Р 34.11-94. Функция хеширования «Стрибог» ГОСТ Р 34.11-2018. Вопросы анализа функций хеширования. Функция хеширования HMAC. Возможные атаки на функции хеширования.	ЛК, СЗ
		1.14	Управление ключами	Ключевые системы. Множества ключей. Строение ключевого множества. Алгебраические и вероятностные свойства множества ключей. Производные ключи. Жизненный цикл ключей. Доверенная третья сторона. Распределение ключей в коммуникационных сетях. Стойкость ключевой системы сети к частичной компрометации. Протоколы выработки общего ключа. Базовый протокол Диффи-Хеллмана. Возможные атаки на выработку общего ключа со злоумышленником посередине. Протокол выработки общего ключа со взаимной аутентификацией. Проблемы распределения открытых ключей. Центры сертификации открытых ключей.	ЛК, СЗ
		1.15	Основы технологии инфраструктур открытых ключей	Компоненты и сервисы инфраструктуры открытых ключей. Архитектура и технологии инфраструктуры открытых ключей. Стандарты в области инфраструктуры открытых ключей. Структуры данных инфраструктуры открытых ключей. Сертификаты открытых ключей. Атрибутные сертификаты. Риски создания, распространения и принятия сертификатов. Набор положений политики инфраструктуры открытых ключей. Развертывание инфраструктуры открытых ключей.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				Программное обеспечение инфраструктуры открытых ключей ведущих мировых производителей и отечественных компаний.	
		1.16	Криптографические методы обеспечения информационной безопасности в сети Интернет	Протокол S/MIME и безопасное использование электронной почты. Используемые в S/MIME криптографические алгоритмы, методы хеширования, способы распределения криптографических ключей. Использование асимметричного шифрования для аутентификации, симметричного шифрования для конфиденциальности и кодов аутентичности сообщений для сохранения целостности сообщений в протоколе защиты транспортного уровня TLS. Криптографические аспекты функционирования набора протоколов сетевого уровня.	ЛК, СЗ
		1.17	Практические аспекты использования шифрсистем	Анализ интенсивности и направленности потоков шифрованных сообщений. Установление факта сокрытия передачи шифрованных сообщений. Элементы использования стеганографических методов. Использование пустых сообщений. Ошибки операторов шифрсвязи. Повторная передача одного и того же открытого сообщения, зашифрованного с использованием разных ключей. Повторное использование одного и того же ключа для шифрования и передачи различных открытых сообщений. Особенности использования аппаратных и программных систем шифрования. Физические и организационные меры безопасности при использовании шифрсистем. Требования режима секретности для персонала шифровальных служб.	ЛК, СЗ
		1.18	Нормативная база в области криптографической защиты информации	Федеральные законы связанные с защитой информации. Национальные стандарты Российской Федерации по криптографии и защите информации: «О безопасности», «О государственной тайне», «Об информации, информационных технологиях и защите информации», «О Федеральной службе безопасности». Ведомственные акты. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005). Положение о лицензировании. Требования к средствам электронной подписи. Требования к средствам удостоверяющего центра.	ЛК, СЗ
		1.19	Прикладные квантовые технологии для	Введение в применение технологии квантового распределения	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
			защиты информации	ключа (КРК) в криптографии. Современные и перспективные сценарии применения КРК. Основы квантовой физики и квантовой информатики. Реализация технологии квантового распределения ключей. Атаки на протоколы и аппаратуру КРК. Практика использования квантовых генераторов случайных чисел в системах КРК.	

* - 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.	Персональный компьютер или моноблок с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска.
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве 25 шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	Персональные компьютеры или моноблоки с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска. Программное обеспечение: обучающие криптографические пакеты CrypTool 1, CrypTool 2 (свободно-распространяемое ПО), криптографическая библиотека OpenSSL (свободно-распространяемое ПО), средства для работы с электронной подписью GnuPG, DSS, Surguch, openCryptoki (свободно-распространяемое ПО), пакет шифрования VeraCrypt (свободно-распространяемое ПО), киберполигон Ampire.
Семинарская	Аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом	Персональные компьютеры или моноблоки с доступом к сети Интернет и прикладным ПО (веб-

	специализированной мебели и техническими средствами мультимедиа презентаций.	браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска. Программное обеспечение: обучающие криптографические пакеты CrypTool 1, CrypTool 2 (свободно-распространяемое ПО), криптографическая библиотека OpenSSL (свободно-распространяемое ПО), средства для работы с электронной подписью GnuPG, DSS, Surguch, openCryptoki (свободно-распространяемое ПО), пакет шифрования VeraCrypt (свободно-распространяемое ПО), киберполигон Ampire.
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.	Персональный компьютер или моноблок с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет).

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2026. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583156 (дата обращения: 07.04.2026).

2. Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 07.04.2026). – Режим доступа: по подписке.

3. Тырышкин, С. Ю. Квантовая информатика. Информационно-измерительные и управляющие системы : учебник для вузов / С. Ю. Тырышкин. — Москва : Издательство Юрайт, 2026. — 102 с. — (Высшее образование). — ISBN 978-5-534-19540-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590346 (дата обращения: 07.04.2026).

Дополнительная литература:

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2026. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583633 (дата обращения: 07.04.2026).

2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2026. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584129 (дата обращения: 07.04.2026).

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 «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**!

РАЗРАБОТЧИК:

Заведующий кафедрой информационной безопасности		Царегородцев Анатолий Валерьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой информационной безопасности		Царегородцев Анатолий Валерьевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой информационной безопасности		Царегородцев Анатолий Валерьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*