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

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
(код и наименование направления подготовки/специальности)

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

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
(наименование (профиль/специализация) ОП ВО)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Технологии обеспечения информационной безопасности» входит в программу магистратуры «Управление информационной безопасностью» по направлению 10.04.01 «Информационная безопасность» и изучается во 2 семестре 1 курса. Дисциплину реализует Кафедра прикладного искусственного интеллекта. Дисциплина состоит из 2 разделов и 8 тем и направлена на изучение основных понятий и определений, классификаций современных тенденций и угроз информационной безопасности; получение знаний о нормативных правовых документах по защите информации; получение навыков разработки оригинальных алгоритмов и программных средств, в том числе с использованием современных интеллектуальных технологий; формирование у студентов устойчивого понимания роли и значения информационной безопасности личности, общества, государства и информационной инфраструктуры общества и государства; получение навыков разработки компонентов программно-аппаратных комплексов обработки информации и автоматизированного проектирования; выработка практических навыков применения современных методов и средств защиты информации

Целью освоения дисциплины является формирование комплекса знаний, навыков и компетенций в области информационной безопасности и применения на практике методов и средств защиты информации на основе современных интеллектуальных технологий, средств и языков программирования.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Технологии обеспечения информационной безопасности» 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-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Обосновывает требования к системе обеспечения информационной безопасности;
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.1 Знает порядок разработки и структуру технических проектов систем (подсистем либо компонентов систем) обеспечения информационной безопасности;
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1 Знает порядок разработки и требования к организационно-распорядительным документам по обеспечению информационной безопасности;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Технологии обеспечения информационной безопасности» 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 «Технологии обеспечения информационной безопасности».

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-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	Защищенные информационные системы;	Управление информационной безопасностью; Разработка технической документации; Информационно-психологическая безопасность; Проектно-технологическая практика;
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Теория управления;	Проектно-технологическая практика; Методология проектирования систем обеспечения информационной безопасности;
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности		Управление информационной безопасностью; Проектно-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 «Технологии обеспечения информационной безопасности» 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)**
			2
Контактная работа, ак.ч.	*68*		*68*
Лекции (**ЛК**)	34		34
Лабораторные работы (**ЛР**)	34		34
Практические/семинарские занятия (**СЗ**)	0		0
Самостоятельная работа обучающихся, ак.ч.	*40*		*40*
Контроль (экзамен/зачет с оценкой), ак.ч.	*36*		*36*
Общая трудоемкость дисциплины	**ак.ч.**	***144***	*144*
	зач.ед.	***4***	*4*

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	Технологии реализации функций назначения по защите информации	1.1	Природа технологий обеспечения информационной безопасности. Информационное общество, противоречивость его развития. Информационная безопасность как правовой аспект регулирования отношений доступа в среде обработки информации и информационного взаимодействия. Угрозы информационного характера, субъектно-объектный подход при их проявлении. Угрозы информации и информационные угрозы. Информационные риски, их влияние на риски основной деятельности объекта информатизации. Функции назначения по защите информации. Технологии обеспечения информационной безопасности, реализующие функции назначения. Объекты защиты, их виды при решении задач информационной безопасности. Представление информационной сферы социотехнического объекта защиты (объекта информатизации). Объекты информатизации финансовой сферы деятельности. Единое информационное пространство и информационная безопасность. Интерпретация понятий «киберсреда» и «киберпространство». Понятие кибератаки, внешние и внутренние кибератаки	ЛК, ЛР
		1.2	Предметные направления технологий обеспечения информационной безопасности в киберпространстве. Обеспечение доверенной организационно-технологической среды и условий защищённости на объектах размещения средств автоматизированной обработки и передачи информации. Секретное и конфиденциальное делопроизводство и документооборот ручного и автоматизированного контуров обработки информации на объектах информатизации. Защита информации от несанкционированного доступа при её автоматизированной обработке. Информационная безопасность телекоммуникационной среды. Криптографические средства защиты информации. Защита от скрытного внедрения в программно-техническую среду компьютерных и телекоммуникационных систем. Защита информации от утечки по техническим и физическим каналам.	ЛК, ЛР
		1.3	Технологии реализации функций назначения в процессах обработки и передачи данных. Технологии идентификации и аутентификации. Технологии управления доступом к информации и ресурсам автоматизированных информационных систем. Технологии обеспечения доверенной среды обработки информации. Технологии защиты от компьютерных вирусов. Технологии защиты	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			информации в телекоммуникационных сетях на уровне инфраструктурных решений: шифрование данных, создание логических доверенных сетей, контроль соединений по адресам, экранирование информационных потоков на стыках сетей, фильтрация информационных потоков. Технологии обнаружения вторжений и противодействия кибератакам: обнаружение атак, контроль целостности, мониторинг процессов, контроль состояния информационной безопасности, реагирование	
		1.4	Технологии и средства реализации функций назначения в физической среде. Представление информации и её защита от утечки по техническим каналам. Физические сигналы как материальные носители информации. Объекты защиты информации от утечки по техническим каналам. Компоненты и показатели образования технических каналов утечки. Виды технических каналов утечки информации. Виды каналов перехвата информации. Организационно-технические мероприятия по защите и технологии их реализации: категорирование и аттестация объектов информатизации; сертификация средств ТСПИ и ВТСС; определение, становление и оборудование контролируемых зон; проведение специальных проверок на закладные устройства и специальных исследований по побочным излучениям ТСПИ. Пассивные и активные средства предотвращения утечки информации по техническим каналам. Технологии реализации пассивных средств защиты. Технологии реализации активных средств защиты. Технологии мониторинга и ситуационного контроля состояния объекта информатизации в части возможности утечки информации по техническим каналам	ЛК, ЛР
Раздел 2	Системные технологии обеспечения информационной безопасности	2.1	Подходы системной инженерии к реализации технологий обеспечения информационной безопасности. Системный подход и обеспечение информационной безопасности в автоматизированных системах обработки информации (АСОД). Понятие целевой системы, большая система, сложная система, примеры из области обеспечения ИБ. Системный анализ как инструмент решения проблемы обеспечения ИБ. Дескриптивная и конструктивная задачи системного анализа, последовательность их решения. Понятие системности и комплексности. Системы обеспечения информационной безопасности (СОИБ) для АСОД и объектов информатизации (ОИ). Жизненный цикл СОИБ и управление им как основа подхода системной инженерии к обеспечению ИБ. СОИБ как целевая обеспечивающая система в операционном окружении, интересы к функционированию и	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			стейкхолдеры. Представление СОИБ в разных предметных онтологиях, опорный и принципиальный уровни описания СОИБ. Совместное взаимосвязанное и согласованное рассмотрение функций организации (предприятия), среды ее деятельности, функциональных приложений и информационно-коммуникационной инфраструктуры АСОД и СОИБ. Понятие системных технологий обеспечения информационной безопасности.	
		2.2	Системный подход и комплексная защита от НСД к информации в автоматизированных системах . Понятие состояния информационной безопасности в АСОД. Эталонная и функциональная модели отношений доступа между пользователями и ресурсами системы. Базовые функции защиты информации от НСД. Функции аудита и управления. Функции обеспечения. Функциональные и обеспечивающие структурные блоки системы защиты информации (СЗИ) от НСД, обоснование их выделения. Структурно-функциональная схема комплексной СЗИ от НСД и зависимости между функциональными блоками системы. Защита информации от НСД, основанная на архитектуре сегментации среды обработки по признаку конфиденциальности. Контуры безопасности. Технология контроля доступа и действий путём доменной организации локальной вычислительной сети контура безопасности. Технологии и средства обеспечения доверенной загрузки серверов и автоматизированных рабочих мест. Технологии и средства защиты информации при работе удалённых пользователей через телекоммуникационную сеть. Защита информации в сети. Технология формирования конечного информационного продукта из информации различных контуров безопасности. Технология защищённой работы с глобальной сетью Интернет, демилитаризованные зоны функционирования.	ЛК, ЛР
		2.3	Системная организация и технологии комплексной защиты информации на объектах информатизации. Объект информатизации как объект защиты с многопрофильной автоматизацией и информатизацией. Объекты информатизации финансовой сферы деятельности. Концептуальное представление комплексной системы защиты информации (КСЗИ). Системный подход к созданию КСЗИ: принцип анализа задач (дескриптивная задача) и синтеза структур (конструктивная задача). Структура КСЗИ. Функциональные подсистемы. Функциональные комплексы, обеспечение типовых решений. Обеспечивающие подсистемы. Технологическое обеспечение КСЗИ.	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			Особенности и значимость информационного обеспечения КСЗИ. Цель и значимость управления информационной безопасностью. Управление как структурный компонент КСЗИ. Нормативно-правовое обеспечение КСЗИ. Взаимодействие системы со средствами, обеспечивающими профильную реализацию по другим видам безопасности. Структурно-функциональная схема КСЗИ. Особенности решения проблемы информационной безопасности ситуационных центров	
		2.4	Системные технологии обеспечения информационной безопасности корпоративных объектов информатизации. Сущность системы корпоративного управления. Факторы, влияющие на решение проблемы обеспечения ИБ на корпоративных объектах информатизации: единое информационное пространство, наследование функциональных IT-приложений бизнес-процессов, тенденция изменения текущей корпоративной информационно-технологической архитектуры, территориальная разбросанность объектов корпоративного предприятия. Состояние доверенности среды функционирования информационных технологий. Системные технологии обеспечения информационной безопасности корпораций как сложный организационно-технологический и программно-технический процесс. Системная организация обеспечения ИБ и технологии системного управления процессами и менеджмента. Объекты информационной индустрии и архитектура информационно-технологической среды корпоративного предприятия. Общесистемные компоненты и базовые объекты информационной инфраструктуры корпоративного предприятия. Обеспечивающие объектовые компоненты: корпоративный центр управления (КЦУ), корпоративный технологический центр (КТЦ), центр сертификации и технологий (ЦСиТ), корпоративный удостоверяющий центр (КУЦ). Комплексная система защиты информации (КСЗИ) для объектов информационной индустрии корпорации. Подсистемы информационного обеспечения (ПОИБ) автоматизированных систем и функциональных сервисов. Системы обеспечения информационной безопасности (СОИБ) объектов информатизации корпорации. Схема архитектуры обеспечения ИБ корпоративного предприятия.	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 (ОС, пакет офисных приложений, в т. ч. MS Office/Office 365, Teams, Skype). Количество посадочных мест - 28.
Семинарская	Научно-учебная лаборатория «Управление инфокоммуникациями» для практической подготовки, проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Комплект специализированной мебели: Интерактивная доска Prestigio MB, компьютер, монитор. Технические средства: Мультимедийная доска Samsung, рабочая станция с монитором для мультимедийной доски; выход в интернет через ЛВС и Wi-Fi. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/ Office 365, Teams, Skype); программное обеспечение со свободной лицензией: браузер Firefox (лицензия MPL-2.0), браузер Chrome (лицензия Google Chrome Terms of Service); медиаплеер (например, VLC Media Player, лицензия GPL-2), Adobe Reader (лицензия Adobe Software License Agreement). Android Studio, IntelliJ IDEA Community Edition 2021.2.2, Java SE Development Kit 17, NoxPlayer, 7-Zip.
Семинарская	Научно-учебная лаборатория «Управление инфокоммуникациями» (учебный класс) для проведения занятий лекционного типа, семинаров и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Комплект специализированной мебели, доска меловая/маркерная передвижная; Технические средства: Мультимедийная доска Samsung, рабочая станция с монитором для мультимедийной доски; выход в интернет через ЛВС и Wi-Fi. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/ Office 365, Teams, Skype); программное обеспечение со свободной лицензией: браузер Firefox (лицензия MPL-2.0), браузер Chrome (лицензия Google Chrome Terms of Service); медиаплеер (например, VLC Media Player, лицензия GPL-2), Adobe Reader (лицензия Adobe Software License Agreement). Android Studio, IntelliJ IDEA Community Edition 2021.2.2, Java SE Development Kit 17, NoxPlayer, 7-Zip.
Семинарская	Научно-учебная лаборатория «Управление инфокоммуникациями» (учебный класс) для проведения занятий лекционного типа, семинаров и практических занятий, групповых и индивидуальных консультаций, текущего контроля и	Комплект специализированной мебели, доска меловая/маркерная передвижная; Технические средства: Мультимедийная доска Samsung, рабочая станция с монитором для мультимедийной доски; выход в интернет через ЛВС и Wi-Fi. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/ Office 365, Teams, Skype); программное обеспечение со свободной лицензией: браузер Firefox (лицензия MPL-2.0), браузер Chrome (лицензия Google Chrome Terms of Service); медиаплеер (например, VLC Media Player, лицензия GPL-2), Adobe Reader (лицензия Adobe Software License Agreement). Android Studio, IntelliJ

	промежуточной аттестации.	IDEA Community Edition 2021.2.2, Java SE Development Kit 17, NoxPlayer, 7-Zip.
Семинарская	Лаборатория вычислительных систем и методов обработки больших данных для практической подготовки, проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Комплект специализированной мебели: учебная доска; технические средства: Персональные рабочие графические станции на базе системного блока AVK-1, Интерактивная доска Polyvision TSL 610, Проектор Epson EB-X02, Коммутатор Cisco Catalyst 2960 24, Сетевой фильтр. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/ Office 365, Teams, Skype), Borland Developer Studio 2006, MATLAB R2008b, Notepad++, Acrobat Reader DC, Anaconda 5 (Python 3).
Семинарская	Лаборатория радиоэлектроники для проведения лабораторных и практических занятий.	Комплект специализированной мебели: учебная доска; технические средства: Осциллограф Iwatsu ACK-7042, Прибор для измерения АЧХ Х1-53, Осциллограф МНИПИ С1-151, Источник питания СИП-301, Источник питания ВИП-010, Генератор импульсов Г5-54, Генератор сигналов НЧ МНИПИ Г3-131, Вольтметр универсальный В7-21, Генератор сигналов ВЧ Г4-116, Вольтметр В7-35, Измеритель индуктивности Е7-11, Прибор для измерения АЧХ Х1-48, Генератор-частотомер Актаком АНР-1001, Генератор сигналов Г3-20, Генератор сигналов НЧ Г3-118, Источник питания ТЕС 20, Источник питания ТЕС 21, Источник питания ТЕС 9, Источник питания ТЕС 13, Источник питания ТЕС 18, Частотомер Ч3-34А, Частотомер Ч3-54, Анализатор спектра С4-25, Блок СВЧ С4-24, Генератор сигналов ВЧ Г4-102А, Синтезатор частоты Ч6-31, Блок генераторный к Х1-53, Блок ГКЧ Х1-46, Мост емкостей Е8-2, Измеритель нелинейных искажений С6-1А, Лабораторный стенд СПЭ-8, Лабораторный стенд ЛРС-2, Усилитель измерительный НЧ У4-28, Милливольтметр В3-43. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т.ч. MS Office/ Office 365, Teams, Skype), Borland Developer Studio 2006, MATLAB R2008b, Notepad++, Acrobat Reader DC, Anaconda 5 (Python 3).
Семинарская	Компьютерный класс для проведения занятий практико-лабораторного характера, 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). Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire» (ПК «Ampire») (версия для учебных заведений). Количество посадочных мест - 25.
Для самостоятельной	Аудитория для самостоятельной работы	Компьютерный класс для проведения лабораторно-практических занятий, курсового проектирования,

работы	обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	практической подготовки. Комплект специализированной мебели; доска маркерная; технические средства: персональные компьютеры, проекционный экран, мультимедийный проектор, NEC NP-V302XG, выход в Интернет. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т.ч. MS Office/Office 365, Teams, Skype), Autodesk AutoCAD 2021, Autodesk AutoCAD 2021 (англ. яз.), Autodesk Inventor 2021, Autodesk Revit 2021, ArchiCAD 23 (бесплатные учебные версии)
		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. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2022. — 336 с. — (Высшее образование). - ЭБС ZNANIUM.com. - URL: https://znanium.com/catalog/product/1861657 (дата обращения: 16.10.2023). – Текст: электронный

2. Партыка, Т. Л. Информационная безопасность: учебное пособие / Т. Л. Партыка, И. И. Попов. – Москва: ФОРУМ, НИЦ ИНФРА-М, 2017. - 432 с. - Текст: непосредственный. - То же. - 2021. - ЭБС ZNANIUM.com. – URL: https://new.znanium.com/catalog/product/1189328 (дата обращения: 16.10.2023). - Текст: электронный

Дополнительная литература:

1. Гришина, Н. В. Информационная безопасность предприятия: учебное пособие / Н. В. Гришина. — 2-е изд., доп. — Москва: ФОРУМ: ИНФРА-М, 2019. — 239 с. — (Среднее профессиональное образование). – ЭБС ZNANIUM.com. - URL: https://znanium.com/catalog/product/1001363 (дата обращения: 16.10.2023). – Текст: электронный

2.

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 «Технологии обеспечения информационной безопасности».

* - 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 «Технологии обеспечения информационной безопасности» представлены в Приложении к настоящей Рабочей программе дисциплины.

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