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)

2026 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 информационной безопасности . Дисциплина состоит из 2 разделов и 8 тем и направлена на изучение технологий реализации функций защиты информации и обеспечения информационой безопасности в киберпространстве и физической среде, включая методы идентификации и аутентификации, управления доступом, обнаружения вторжений, криптографической защиты и предотвращения утечки по техническим каналам.

Целью освоения дисциплины является формировании у обучающихся компетенций по построению комплексных систем защиты информации для объектов информатизации, основанных на инженерном подходе к проектированию, внедрению и управлению жизненным циклом средств обеспечения информационной безопасности.

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;	Проектно-технологическая практика; Управление информационной безопасностью; Разработка технической документации; Информационно-психологическая безопасность;
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Теория управления;	Методология проектирования систем обеспечения информационной безопасности; Проектно-технологическая практика;
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности		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	Наименование темы		Содержание 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	Технологии идентификации и аутентификации. Технологии	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
			назначения в процессах обработки и передачи данных.	управления доступом к информации и ресурсам автоматизированных информационных систем. Технологии обеспечения доверенной среды обработки информации. Технологии защиты от компьютерных вирусов. Технологии защиты 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	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				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 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	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				различных контуров безопасности. Технология защищённой работы с глобальной сетью Интернет, демилитаризованные зоны функционирования.	
		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. 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.	ЛК, ЛР
		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	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				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.	

* - 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.
Лаборатория	Аудитория для проведения лабораторных работ, индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и оборудованием.	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: среда виртуализации Oracle VM VirtualBox (свободно-распространяемое ПО), операционная система Debian Linux (свободно-распространяемое ПО), Wireshark (свободно-распространяемое ПО), GNS3 (свободно-распространяемое ПО), программные пакеты симуляции физических атак SeseLab и GRFICSv3 (свободно-распространяемое ПО), операционная система pfSense Community Edition (свободно-распространяемое ПО), Kali Linux (свободно-распространяемое ПО), межсетевой экран Netfilter (свободно-распространяемое ПО), системы обнаружения/предотвращения вторжений Suricata, Snort (свободно распространяемое ПО), SIEM-система Security Onion (свободно-

		распространяемое ПО), учебные пакеты OWASP WebGoat, OWASP Juice Shop, OWASP Dependency-Check (свободно-распространяемое ПО), сканер уязвимостей ZAP (Zed Attack Proxy), онлайн-база данных угроз БДУ ФСТЭК России.
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: среда виртуализации Oracle VM VirtualBox (свободно-распространяемое ПО), операционная система Debian Linux (свободно-распространяемое ПО), Wireshark (свободно-распространяемое ПО), GNS3 (свободно-распространяемое ПО), программные пакеты симуляции физических атак SeseLab и GRFICSv3 (свободно-распространяемое ПО), операционная система pfSense Community Edition (свободно-распространяемое ПО), Kali Linux (свободно-распространяемое ПО), межсетевой экран Netfilter (свободно-распространяемое ПО), системы обнаружения/предотвращения вторжений Suricata, Snort (свободно распространяемое ПО), SIEM-система Security Onion (свободно-распространяемое ПО), учебные пакеты OWASP WebGoat, OWASP Juice Shop, OWASP Dependency-Check (свободно-распространяемое ПО), сканер уязвимостей ZAP (Zed Attack Proxy), онлайн-база данных угроз БДУ

		ФСТЭК России.
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. Трайнев, В. А. Системный подход к обеспечению информационной безопасности предприятия (фирмы) / В. А. Трайнев ; Международная академия наук информации, информационных процессов и технологий (МАН ИПТ). – 5-е изд. – Москва : Дашков и К°, 2022. – 332 с. : схем., ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=698555 (дата обращения: 22.04.2026). – Библиогр. в кн. – ISBN 978-5-394-05035-0. – Текст : электронный.

2. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 22.04.2026). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

Дополнительная литература:

1. Привалов, А. А. Обеспечение информационной безопасности, проектирования, создания, модернизации объектов информации на базе компьютерных систем в защищенном исполнении : учебно-методическое пособие к курсовой работе / А. А. Привалов. - Москва : РУТ (МИИТ), 2018. - 48 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1895288 (дата обращения: 22.04.2026). – Режим доступа: по подписке.

2. Макаренко, С. И. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Часть 2: Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях : учебное пособие / С. И. Макаренко, А. А. Ковальский, С. А. Краснов. - Санкт-Петербург : Наукоемкие технологии, 2020. - 359 с. - ISBN 978-5-6044429-8-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2238917 (дата обращения: 22.04.2026)

3. Обеспечение информационной безопасности информационных сетей : учебно-методическое пособие / Е. В. Булгакова, А. Н. Кубанков, В. В. Булгаков, Д. С. Дойников. – Москва ; Вологда : Инфра-Инженерия, 2025. - 92 с. – ISBN 978-5-9729-2344-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2225339 (дата обращения: 22.04.2026). – Режим доступа: по подписке.

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 «Технологии обеспечения информационной безопасности».

* - 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.*