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

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ
(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 «Защищенные информационные системы» входит в программу магистратуры «Управление информационной безопасностью» по направлению 10.04.01 «Информационная безопасность» и изучается в 1 семестре 1 курса. Дисциплину реализует Кафедра информационной безопасности . Дисциплина состоит из 2 разделов и 18 тем и направлена на изучение комплексных принципов построения, архитектуры и технологий проектирования защищенных информационных систем, а также программно-аппаратных средств обеспечения их безопасности, включая межсетевые экраны, системы обнаружения атак и механизмы криптографической защиты.

Целью освоения дисциплины является формирование у обучающихся компетенций по реализации политик разграничения доступа, обеспечению целостности и конфиденциальности данных, а также безопасному конфигурированию сетевых сервисов для противодействия актуальным угрозам информационной безопасности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Защищенные информационные системы» 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-1.2 Разрабатывает проект технического задания на создание системы обеспечения информационной безопасности;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Защищенные информационные системы» 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 «Защищенные информационные системы».

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		Проектно-технологическая практика; Теория игр и исследование операций; Технологии обеспечения информационной безопасности;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
	ее создание		Управление информационной безопасностью; Разработка технической документации; Информационно-психологическая безопасность;

* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Защищенные информационные системы» 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)**
			1
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.	*76*		*76*
Контроль (экзамен/зачет с оценкой), ак.ч.	*36*		*36*
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	Комплексный подход к организации защищенных информационных систем.	1.1	Основные понятия защищенных информационных систем.	Понятие «информационная система». Концепция безопасности информационной системы. Цели обеспечения информационной безопасности. Санкционированный и несанкционированный доступ. Угрозы безопасности и каналы реализации угроз.	ЛК, ЛР
		1.2	Общие принципы построения защищенных информационных систем.	Уровни защиты информации. Стандарты безопасности. Классы защищенности информационных систем. Нормативная база Российской Федерации. Современная доктрина информационной безопасности Российской Федерации.	ЛК, ЛР
		1.3	Архитектура информационных систем на основе баз данных.	Трехуровневая архитектура информационных систем на основе баз данных. Модели данных. Структура данных. Целостность реляционных данных.	ЛК, ЛР
		1.4	Технологии проектирования баз данных.	Основные этапы проектирования баз данных. Технологии проектирования на основе нормализации. Технологии проектирования на основе модели «Сущность-связь».	ЛК, ЛР
		1.5	Разграничения доступа к ресурсам информационной системы.	Основные понятия систем разграничения доступа. Сущность и определение политики безопасности. Основные типы политик безопасности: мандатные, ролевые, контроля целостности информационных ресурсов, избирательного разграничения доступа. Субъектно-объектная модель информационной системы.	ЛК, ЛР
		1.6	Средства обеспечения целостности информационных систем на основе баз данных.	Угрозы целостности информации. Способы противодействия. Понятие и основные свойства транзакций. Механизм блокировок. Декларативная и процедурная ссылочные целостности. Способы поддержания ссылочной целостности. Триггеры и правила.	ЛК, ЛР
		1.7	Средства обеспечения конфиденциальности информации в системах на основе баз данных.	Угрозы конфиденциальности информации. Средства идентификации и аутентификации в СУБД. Средства управления доступом. Виды привилегий. Использование механизма ролей. Метки безопасности. Использование представлений для обеспечения конфиденциальности информации.	ЛК, ЛР
		1.8	Способы хранения конфиденциальной информации.	Положение о конфиденциальной информации в электронном виде. Контентная категоризация. Классификация информации	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				по уровню конфиденциальности. Метки документов. Способы хранение конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация.	
		1.9	Основные направления защиты информации.	Защита документов. Защита каналов утечки конфиденциальной информации. Мониторинг действий пользователей. Классификация внутренних нарушителей: неосторожные, манипулируемые, саботажники, нелояльные, мотивированные извне. Другие градации.	ЛК, ЛР
		1.10	Организационные меры защиты информации в организации.	Кадровая политика. Определение прав локальных пользователей. Стандартизация программного обеспечения. Организация процедуры хранения физических носителей информации. Определение уровней контроля информационных потоков. Режимы архива, сигнализации, активной защиты.	ЛК, ЛР
Раздел 2	Программно-аппаратные средства обеспечения информационной безопасности информационных систем.	2.1	Межсетевые экраны.	Понятие межсетевого экрана. Классификация. Установление TCP – соединения. Пакетные фильтры, набор правил. Пограничные роутеры. Stateful Inspection и Host-based межсетевые экраны. Персональные межсетевые экраны и их персональные устройства. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Гибридные технологии межсетевых экранов. Трансляция сетевых адресов (NAT). Статическая и скрытая трансляция NAT.	ЛК, ЛР
		2.2	Типы окружений межсетевых экранов.	Принцип построения окружения межсетевого экрана. DMZ сети. Конфигурация с одной DMZ- сетью. Service Leg конфигурация. Конфигурация с двумя DMZ-сетями. Виртуальные частные сети. Расположение VPN-серверов. Интранет. Экстранет. Компоненты инфраструктуры: концентраторы и коммутаторы. Расположение серверов в DMZ-сетях. Внешне доступные серверы. VPN и Dial-in серверы. Внутренние серверы. DNS серверы. SMTP – серверы.	ЛК, ЛР
		2.3	Политика безопасности межсетевого экрана.	Политика межсетевого экрана. Реализация его набора правил. Тестирование политики межсетевого экрана. Возможные подходы к эксплуатации межсетевого экрана. Сопровождение межсетевого экрана и управление им. Физическая безопасность окружения межсетевого экрана. Администрирование межсетевого экрана. Встраивание межсетевого экрана в ОС.	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				Стратегия восстановления после сбоев. Возможность создания логов межсетевого экрана. Инциденты безопасности. Создание резервных копий данных и конфигурации.	
		2.4	Системы обнаружения атак.	Понятие системы обнаружения атак (IDS). Типы и базовая структура IDS. Совместное расположение Host и Target. Разделение Host и управления. Полностью распределенное управление. Network-based IDS, Host-based IDS, Application-based IDS. Анализ, выполняемый IDS.Определение злоупотреблений. Активные и пассивные ответные действия. Использование SNMP TRAPS. Системы анализа и оценки уязвимостей. Host-based и Network-based анализ уязвимостей. Способы взаимодействия сканера уязвимостей и IDS.	ЛК, ЛР
		2.5	Безопасное использование службы доменных имен (DNS).	Безопасность DNS.Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности. Основные механизмы безопасности для сервисов DNS. Данные DNS и ПО DNS. Name-серверы, Авторитетные и кэширующие Name-серверы. Resolver□ы. Транзакции DNS. Запрос/ответ DNS. Зонная пересылка. Динамические обновления. Безопасность окружения DNS. Угрозы для ПО и данных DNS.	ЛК, ЛР
		2.6	Обеспечение безопасности WEB-серверов.	Причины уязвимости WEB – сервера. Планирование развертывания WEB – сервера. Безопасное инсталлирование и конфигурирование используемой ОС. Удаление или запрещение ненужных сервисов и приложений. Управление ресурсами на уровне ОС. Альтернативные платформы для web - сервера. Использование Appliances для web – сервера. Специально усиленные ОС и web –серверы. Тестирование безопасности ОС. Безопасное инсталлирование и конфигурирование web – сервера. Соответствующий список действий. Разграничение доступа для ПО web – сервера. Управление доступом к директории содержимого web – сервера.	ЛК, ЛР
		2.7	Безопасность WEB-ориентированного контента.	Публикации информации на web-сайтах. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies. Уязвимости технологий активного содержимого на стороне клиента. Уязвимости технологий создания содержимого на стороне сервера. Необходимые	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				действия для обеспечения безопасности web-содержимого.	
		2.8	Технологии аутентификации и шифрования.	Требования к аутентификации и шифрованию. Аутентификация, основанная на IP -адресе. Basic и Digest аутентификации. SSL/TLS. Возможности и слабые места SSL/TLS. Пример SSL/TLS сессии. Схемы шифрования SSL/TLS. Список действий при использовании технологий аутентификации и шифрования. Межсетевые экраны прикладного уровня для Web.	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.	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), операционные системы Debian Linux (свободно-распространяемое ПО), 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), киберполигон Ampire.
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	Персональные компьютеры или моноблоки с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска. Программное

	средствами мультимедиа презентаций.	обеспечение: среда виртуализации Oracle VM VirtualBox (свободно-распространяемое ПО), операционные системы Debian Linux (свободно-распространяемое ПО), 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), 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. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2026. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584673 (дата обращения: 26.03.2026).

2. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 366 с. — (Высшее образование). — ISBN 978-5-534-15951-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590557 (дата обращения: 22.04.2026).

Дополнительная литература:

1. Мандрица, И. В. Управление проектами по информационной безопасности и экономика защиты информации. Часть 1 / И. В. Мандрица, В. И. Петренко, О. В. Мандрица. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-45723-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/311825 (дата обращения: 22.04.2026). — Режим доступа: для авториз. пользователей.

2. 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.

3. Лозовецкий, В. В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей : учебное пособие для вузов / В. В. Лозовецкий, Е. Г. Комаров, В. В. Лебедев ; под редакцией В. В. Лозовецкий. — 2-е изд., стер. — Санкт-Петербург : Лань, 2024. — 488 с. — ISBN 978-5-507-47615-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/397355 (дата обращения: 22.04.2026). — Режим доступа: для авториз. пользователей.

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 «Защищенные информационные системы».

* - 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.*