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

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ
(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 «Системы обнаружения вторжений» 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 5 разделов и 5 тем и направлена на изучение принципов построения защищенных каналов передачи данных и и управления ими; обучение использованию программных и аппаратных средств защиты каналов передачи данных; ознакомление с методами проектирования, развертывания и сопровождения защищенных каналов передачи данных, с методами обследования и анализа защищенности каналов передачи данных.

Целью освоения дисциплины является знакомство студентов с технологиями обнаружения атак, а также понимание ими причин недостаточности традиционных средств защиты и способов повышения защищённость сетей и систем

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Системы обнаружения вторжений» 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)
ПК-1	Способен оценивать уровень безопасности компьютерных систем и сетей	ПК-1.1 Проводит контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации в компьютерных системах и сетях; ПК-1.2 Проводит анализ безопасности компьютерных систем; ПК-1.3 Проводит инструментальный мониторинг защищенности компьютерных систем и сетей;
ПК-2	Способен разрабатывать системы защиты информации автоматизированных систем	ПК-2.1 Проводит тестирование систем защиты информации автоматизированных систем;
ПК-3	Способен формировать требования к защите информации в автоматизированных системах	ПК-3.2 Определяет угрозы безопасности информации, обрабатываемой автоматизированной системой;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Системы обнаружения вторжений» относится к части, формируемой участниками образовательных отношений 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 «Системы обнаружения вторжений».

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
ПК-1	Способен оценивать уровень безопасности компьютерных систем и сетей		Преддипломная практика; *Инструментальные средства анализа рисков информационной безопасности***; *Имитационное моделирование систем обеспечения информационной безопасности***;
ПК-2	Способен разрабатывать системы защиты информации автоматизированных систем		*Практические аспекты аудита информационной безопасности***; *Обеспечение непрерывности бизнеса***; Преддипломная практика;
ПК-3	Способен формировать требования к защите информации в автоматизированных системах		*Преддипломная практика;* *Инструментальные средства анализа рисков информационной безопасности***; *Имитационное моделирование систем обеспечения информационной безопасности***; *Практические аспекты аудита информационной безопасности***; *Обеспечение непрерывности бизнеса***; *Международные аспекты противодействия киберпреступности и кибертерроризму***; *Международно-правовое регулирование в области информационной безопасности***;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Системы обнаружения вторжений» 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**)	0		0
Практические/семинарские занятия (**СЗ**)	34		34
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	Современные тенденции обеспечения кибербезопасности	1.1	Понятие киберпространства и кибератак. Жизненный цикл кибератаки. Вторжение в автоматизированную систему. Признаки вторжения. Современные задачи и технологии обнаружения и противодействия вторжениям	ЛК, СЗ
Раздел 2	Архитектура современных систем обнаружения вторжений	2.1	Представление и назначение системы обнаружения вторжений (СОВ). Сфера использования СОВ. Типовая архитектура системы СОВ. Логическая структура современных СОВ: информационный фонд, специальный компонент «агент БД»; координационный центр; консоль администратора; модуль интеграции с сетевым оборудованием, его функциональные модули; модуль почтовых уведомлений, агент и сетевые датчики; хостовой датчик. Интеграция компонентов. Типовая схема включения системы СОВ в автоматизированную информационную систему	ЛК, СЗ
Раздел 3	Сравнительный анализ существующих систем обнаружения вторжений	3.1	Классификация аномалий в IP-сетях. Два класса систем СОВ: сетевые системы, системы выявления злоупотреблений и аномалий. Критерий оценки системы СОВ. Виды систем СОВ по уровню наблюдения: сетевая, узловая и гибридная. Используемый метод обнаружения: эвристический и экспертный. Адаптивность к неизвестным атакам. Вид управления процессами: централизованное и распределенное. Устойчивость: глобальная и локальная. Архитектура системы: распределённая и нераспределённая. Расширяемость: программные интерфейсы, стандарты взаимодействия сетевых компонентов. Ответная реакция на атаку: активная и пассивная. Защищенность. Максимальная скорость снятия информация с сетевого интерфейса. Обзорный анализ современных систем обнаружения вторжений	ЛК, СЗ
Раздел 4	Системные и конструктивные направления развития систем обнаружения и противодействия вторжениям	4.1	Построение модели нарушителей информационной безопасности и угроз при реализации вторжения в автоматизированные системы. Возможные угрозы и атаки на хост, защищенный хостовым датчиком. Проблема ложных срабатываний и обеспечение корреляции событий. Повышение производительности системы. Повышение отказоустойчивости системы с целью недопущения снижения доступности к критическим приложениям. Поддержка новых технологий и протоколов для противодействия атакам на прикладном уровне. Решение проблемы кооперации систем обнаружения вторжений разных производителей в рамках одной инфраструктуры предотвращения атак. Повышение функциональности хостовых датчиков, способных работать с системами	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			обнаружения вторжений различных производителей. Совершенствование практик эксплуатации и принятия управленческих решений	
Раздел 5	Применение SIEM-систем в задачах информационной безопасности	5.1	Назначение SIEM-системы. Упрощенное внедрение системы. Компоненты системы, потоки данных. Управление активами и уязвимостями. Метрики CVSSv2, CVSSv3. Контекстные метрики. БДУ ФСТЭК РФ. Настройка SIEM-системы. Пользователи и роли. Сбор и работа с событиями. Таксономия собы-тий. Корреляции. Обзор системных правил корреляции. Инциденты и доставка уведомлений. Статистика и отчеты. Обзор документации. Журналы и решение проблем.	ЛК, СЗ

* - 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	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 работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	Компьютерный класс для проведения лабораторно-практических занятий, курсового проектирования, 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. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие / Н.В.Гришина. - Москва: ФОРУМ, 2019. - 216 с. - ЭБС ZNANIUM.com — URL: http://znanium.com/catalog/product/1017663(дата обращения 07.03.2023). - Текст: электронный

2. Гамза, В.А. Безопасность банковской деятельности: учебник для академического бакалавриата / И.Ф. Гамза, И.Б.Ткачук, И.М.Жилкин. - 4-е изд., перераб. и доп. - Москва: Юрайт, 2019. — 432 с. - ЭБС Юрайт. - URL: https://www.biblio-online.ru/book/bezopasnost-bankovskoy-deyatelnosti-432157(дата обращения: 07.03.2023). - Текст: электронный

3. Баранова Е.К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Е.К.Баранова, А.В.Бабаш. - Москва: ИЦ РИОР: НИЦ Инфра-М, 2018. - 336 с - ЭБС ZNANIUM.com — URL: https://znanium.com/catalog/document?id=393765(дата обращения 07.03.2023). - Текст: электронный

Дополнительная литература:

1. Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) [Электронный ресурс]: учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. - Москва: Гор. Линия-Телеком, 2013. - 220 с.

2. Курило А.П. Вопросы управления информационной безопасностью [Электронный ресурс]: учебное пособие для вузов / А.П. Курило

3. Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации».

4. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности

5. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем» РС БР ИББС-2.6-2014 (приняты и введены в действие Распоряжением Банка России от 10.07.2014 N Р-556).

6. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014 (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-339).

7. Методические документы. Профили защиты средств обнаружения вторжений. Утверждены ФСТЭК России 6 марта 2012 г.

8. Указ Президента РФ от 15.01.2013 №31с «О создании ГосСОПКА».

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 «Системы обнаружения вторжений».

* - 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 «Системы обнаружения вторжений» представлены в Приложении к настоящей Рабочей программе дисциплины.

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