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)

2026 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, 3 семестрах 1, 2 курсов. Дисциплину реализует Кафедра информационной безопасности . Дисциплина состоит из 2 разделов и 7 тем и направлена на изучение архитектуры, принципов функционирования и классификации систем обнаружения вторжений, а также методов выявления аномалий и анализа событий безопасности для противодействия кибератакам на различных этапах их жизненного цикла.

Целью освоения дисциплины является формировании у обучающихся компетенций по выбору, внедрению и эксплуатации современных средств мониторинга сетевой и хостовой активности, включая интеграцию СОВ в SIEM-системы для централизованного управления инцидентами информационной безопасности.

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*

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
ПК-1	Способен оценивать уровень безопасности компьютерных систем и сетей		Преддипломная практика;
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; Практические аспекты аудита информационной безопасности**; Обеспечение непрерывности бизнеса**; International Legal Frameworks for Combating Cybercrime and Cyberterrorism**; International Legal Regulation in the Field of Information Security**;*

* - 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 «8» 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)**	
			2	**3**
Контактная работа, ак.ч.	*170*		*102*	*68*
Лекции (**ЛК**)	34		34	0
Лабораторные работы (**ЛР**)	0		0	0
Практические/семинарские занятия (**СЗ**)	136		68	68
Самостоятельная работа обучающихся, ак.ч.	*55*		*42*	*13*
Контроль (экзамен/зачет с оценкой), ак.ч.	*63*		*36*	*27*
Общая трудоемкость дисциплины	**ак.ч.**	***288***	*180*	*108*
	зач.ед.	***8***	*5*	*3*

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	Современные тенденции обеспечения кибербезопасности	1.1	Общие термины и определения по системам обнаружения вторжений	Понятие киберпространства и кибератак. Жизненный цикл кибератаки. Вторжение в автоматизированную систему. Признаки вторжения. Современные задачи и технологии обнаружения и противодействия вторжениям	ЛК, СЗ
		1.2	События ИБ, критерии инцидентов и источники оповещения	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
		1.3	Состав событий ИБ и источники их формирования	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.	ЛК, СЗ
Раздел 2	Архитектура современных систем обнаружения вторжений	2.1	Классификация событий и инцидентов ИБ	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
		2.2	Менеджмент инцидентов информационной безопасности	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	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
		2.3	Современные системы обнаружения вторжений	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 обнаружения вторжений различных производителей. Совершенствование практик эксплуатации и принятия управленческих решений	ЛК, СЗ
		2.4	СОВ как часть SIEM-системы	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 событий. 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	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: 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), сетевые сканеры Nmap, Wireshark (свободно-распространяемое ПО), системы обнаружения/предотвращения вторжений Suricata, Snort (свободно распространяемое ПО), SIEM-система Security Onion (свободно-распространяемое ПО), системы управления инцидентами ИБ TheHive, RTIR, Wazuh (свободно-распространяемое ПО), киберполигон Ampire.

Семинарская	Аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели 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), операционные системы Debian Linux (свободно-распространяемое ПО), pfSense Community Edition (свободно-распространяемое ПО), Kali Linux (свободно-распространяемое ПО), межсетевой экран Netfilter (свободно-распространяемое ПО), сетевые сканеры Nmap, Wireshark (свободно-распространяемое ПО), системы обнаружения/предотвращения вторжений Suricata, Snort (свободно распространяемое ПО), SIEM-система Security Onion (свободно-распространяемое ПО), системы управления инцидентами ИБ TheHive, RTIR, Wazuh (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. Полтавцева, М. А. Высокопроизводительные системы обнаружения вторжений : учебное пособие / М. А. Полтавцева, Д. С. Лаврова. - 2-е изд. - Москва ; Вологда : Инфра-Инженерия, 2023. - 152 с. - ISBN 978-5-9729-1213-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2092484 (дата обращения: 20.04.2026). – Режим доступа:

по подписке.

2. Целых, А. Н. Выявление инцидентов информационной безопасности и мошеннических транзакций методами машинного обучения : учебное пособие / А. Н. Целых, Э. М. Котов ; Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2023. - 116 с. - ISBN 978-5-9275-4515-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2146710 (дата обращения: 15.04.2026). – Режим доступа: по подписке.

Дополнительная литература:

1. Компьютерные сети : учебник и практикум для вузов / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2026. — 515 с. — (Высшее образование). — ISBN 978-5-534-21452-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590190 (дата обращения: 20.04.2026).

2. Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И., - 2-е изд. - Москва :Гор. линия-Телеком, 2016. - 170 с.ISBN 978-5-9912-0363-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/560782 (дата обращения: 15.04.2026). – 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 «Системы обнаружения вторжений».

* - все учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины **в ТУИС**!

РАЗРАБОТЧИК:

Старший преподаватель кафедры информационной безопасности		Валеев Михаил Владимирович
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.*