

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 22.05.2026 12:31:00

Уникальный программный ключ:

sa953a0120d891083f939673078ef1a989dae18a

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

МЕТОДЫ ВЫЯВЛЕНИЯ И АНАЛИЗА ИНЦИДЕНТОВ 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 «Методы выявления и анализа инцидентов информационной безопасности» 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 6 тем и направлена на изучение процессов идентификации, сбора, корреляции и классификации событий информационной безопасности, а также методологии организации деятельности подразделений по реагированию на инциденты в соответствии с отечественными и международными стандартами.

Целью освоения дисциплины является формирование у обучающихся практических навыков выявления нарушений ИБ на основе анализа событий от различных источников и применения циклической модели менеджмента инцидентов для планирования, реализации и совершенствования системы защиты информации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Методы выявления и анализа инцидентов 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)
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 «Методы выявления и анализа инцидентов информационной безопасности» 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 «Методы выявления и анализа инцидентов 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*
ПК-1	Способен оценивать уровень безопасности компьютерных систем и сетей		Преддипломная практика;
ПК-2	Способен разрабатывать системы защиты информации автоматизированных систем		<i>Практические аспекты аудита информационной безопасности**;</i> <i>Обеспечение непрерывности бизнеса**;</i> Преддипломная практика;
ПК-3	Способен формировать требования к защите информации в автоматизированных системах		<i>Преддипломная практика;</i> <i>Практические аспекты аудита информационной безопасности**;</i> <i>Обеспечение непрерывности бизнеса**;</i> <i>International Legal Frameworks for Combating Cybercrime and Cyberterrorism**;</i> <i>International Legal Regulation in the Field of Information Security**;</i>

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Методы выявления и анализа инцидентов информационной безопасности» 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
<i>Контактная работа, ак.ч.</i>	170		102	68
Лекции (ЛК)	34		34	0
Лабораторные работы (ЛР)	0		0	0
Практические/семинарские занятия (СЗ)	136		68	68
<i>Самостоятельная работа обучающихся, ак.ч.</i>	55		42	13
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	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	События и инциденты информационной безопасности	1.1	Стандарты, документы и организация реагирования на инциденты ИБ	Отечественные и зарубежные стандарты и документы по вопросам осуществлению организации и управления деятельностью группы реагирования на инциденты информационной безопасности, термины и определения. Предлагаемый подход к осуществлению организации и управления деятельностью группы реагирования на инциденты информационной безопасности.	ЛК, СЗ
		1.2	События ИБ, критерии инцидентов и источники оповещения	Файловые системы (файлы и каталоги) Выполнение операций с файлами и каталогами посредством командной строки. Ссылки (жёсткие, символические) Управление разделами и дисками (физические, логические) Управление пользователями и группами пользователей. Разграничение прав доступа Модели управления доступом Обновление ОС. Управление пакетами, установка/удаление и настройка ПО Резервное копирование Техническая документация и репозитории	ЛК, СЗ
		1.3	Состав событий ИБ и источники их формирования	Определение состава событий информационной безопасности, рекомендуемых к использованию для анализа с целью выявления нарушений в обеспечении информационной безопасности Пример состава событий информационной безопасности, рекомендуемых к использованию для анализа с целью выявления нарушений в обеспечении информационной безопасности, перечень событий информационной безопасности по группам, Определение состава типов (классов) технических средств, являющихся источниками, формирующими события информационной безопасности, пример состава типов (классов) технических средств, являющихся источниками, формирующими события информационной безопасности.	ЛК, СЗ
		1.4	Сбор и корреляция событий ИБ	Определение правил сбора и корреляции событий информационной безопасности, позволяющих осуществить оперативное выявление нарушений информационной безопасности Правила сбора событий информационной безопасности, корреляция событий информационной	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				безопасности	
Раздел 2	Классификация событий и инцидентов информационной безопасности	2.1	Классификация событий и инцидентов ИБ	Критерии классификации событий информационной безопасности в качестве свидетельств нарушений информационной безопасности. Требования к критериям классификации, обзор и анализ известных подходов к классификации событий ИБ, сравнение с требованиями, предложение по критериям классификации событий информационной безопасности в качестве свидетельств нарушения информационной безопасности, реализация критериев классификации событий информационной безопасности в качестве свидетельств нарушения информационной безопасности, принципы и критерии классификации инцидентов ИБ, выбор атрибутов для классификации инцидентов ИБ, классификатор инцидентов ИБ.	ЛК, СЗ
		2.2	Менеджмент инцидентов информационной безопасности	Процессы менеджмента инцидентов информационной безопасности Группы процессов СМИИБ в виде циклической модели циклической модели Деминга, планирование менеджмента инцидентов ИБ, реализация менеджмента инцидентов ИБ, анализ менеджмента инцидентов ИБ, совершенствование системы менеджмента инцидентов ИБ, требования к хранению данных о событиях информационной безопасности, которые классифицированы в качестве свидетельств нарушений информационной безопасности	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.
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. 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.

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.

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. 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.

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/>
- Научометрическая база данных Lens.org <https://www.lens.org>

Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля:*

1. Курс лекций по дисциплине «Методы выявления и анализа инцидентов информационной безопасности».

* - 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

Должность, БУП

Подпись

Валеев Михаил
Владимирович

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой
информационной безопасности

Должность БУП

Подпись

Царегородцев Анатолий
Валерьевич

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой
информационной безопасности

Должность, БУП

Подпись

Царегородцев Анатолий
Валерьевич

Фамилия И.О.