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)

2025 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 семестре 1 курса. Дисциплину реализует Кафедра прикладного искусственного интеллекта. Дисциплина состоит из 4 разделов и 6 тем и направлена на изучение - изучение концепции инженерно-технической защиты информации; - изучение теоретических основ инженерно - технической защиты информации; - изучение физических основ инженерно-технической защиты информации; - изучение технических средств добывания и защиты информации; - изучение организационных основ инженерно-технической защиты информации; - изучение методического обеспечения инженерно-технической защиты информации.

Целью освоения дисциплины является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах

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; *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 «Методы выявления и анализа инцидентов 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**)	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	Вводная часть	1.1	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
Раздел 2	События и инциденты информационной безопасности	2.1	Перечень событий, относящихся к ИБ. Критерии отнесения событий ИБ к инцидентам ИБ, Источники событий ИБ и способы оповещений о событиях ИБ	ЛК
		2.2	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
		2.3	Определение правил сбора и корреляции событий информационной безопасности, позволяющих осуществить оперативное выявление нарушений информационной безопасности Правила сбора событий информационной безопасности, корреляция событий информационной безопасности	ЛК, СЗ
Раздел 3	Классификация событий и инцидентов информационной безопасности	3.1	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	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			атрибутов для классификации инцидентов ИБ, классификатор инцидентов ИБ.	
Раздел 4	Перечень разделов (тем) для самостоятельного изучения обучающимися	4.1	Процессы менеджмента инцидентов информационной безопасности Группы процессов СМИИБ в виде циклической модели циклической модели Дёминга, 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	

* - 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. ГОСТ Р ИСО/МЭК 18044-2007
2. РС БР ИББС-2.5-2014
3. Федеральный закон от 27 июля 2006 года № 149-ФЗ.
4. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ в декабре 2016 г. № Пр-1895).
5. «О подписании Соглашения о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности». Расп. Пр. РФ от 28.05.2012 № 856-р «Собрание законодательства РФ», 04.06.2012, № 23, ст. 3058.
6. Международная информационная безопасность: Теория и практика: В 3-х т. Учебник для вузов МГИМО/Под общ. ред. А.В. Крутских. – М.: «Аспект-пресс». 2019. – 384 с.

Дополнительная литература:

1. Международная информационная безопасность: Теория и практика: В 3-х т. Учебник для вузов МГИМО/Под общ. ред. А.В. Крутских. – М.: «Аспект-пресс». 2019. – 384 с.

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 «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**!

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 «Методы выявления и анализа инцидентов информационной безопасности» представлены в Приложении к настоящей Рабочей программе дисциплины.

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