

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ястребов Олег Александрович
Должность: Ректор
Дата подписания: 29.05.2025 15:00:47
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)

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; <i>Инструментальные средства анализа рисков информационной безопасности**;</i> <i>Имитационное моделирование систем обеспечения информационной безопасности**;</i>
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>Инструментальные средства анализа рисков информационной безопасности**;</i> <i>Имитационное моделирование систем обеспечения информационной безопасности**;</i> <i>Практические аспекты аудита информационной безопасности**;</i> <i>Обеспечение непрерывности бизнеса**;</i> <i>Международные аспекты противодействия киберпреступности и кибертерроризму**;</i> <i>Международно-правовое регулирование в области информационной безопасности**;</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 «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 атрибутов для классификации инцидентов ИБ, классификатор инцидентов ИБ.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
Раздел 4	Перечень разделов (тем) для самостоятельного изучения обучающимися	4.1	Процессы менеджмента инцидентов информационной безопасности Группы процессов СМИБ 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	

* - 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.	
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.	
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.	

* - 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

<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://znaniyum.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:

<i>Должность, БУП</i>	<i>Подпись</i>	Баум Валентина Владимировна <i>Фамилия И.О.</i>

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой <i>Должность БУП</i>	<i>Подпись</i>	Подолько Павел Михайлович [М] заведующий кафедрой <i>Фамилия И.О.</i>

РУКОВОДИТЕЛЬ ОП ВО:

<i>Должность, БУП</i>	<i>Подпись</i>	<i>Фамилия И.О.</i>