

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 28.05.2025 12:23:30

Уникальный программный ключ:

ca953a0120d891083f939673078ef1a989dae18a

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

ОСНОВЫ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/специальности)

Освоение дисциплины ведется в рамках реализации основной профессиональной образовательной программы высшего образования (ОП ВО):

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(наименование (профиль/специализация) ОП ВО)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Основы управления инцидентами информационной безопасности» входит в программу бакалавриата «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» по направлению 10.03.01 «Информационная безопасность» и изучается в 8 семестре 4 курса. Дисциплину реализует Кафедра прикладного искусственного интеллекта. Дисциплина состоит из 1 раздела и 5 тем и направлена на изучение методов и процедур выявления, анализа и реагирования на инциденты, связанные с нарушением информационной безопасности. Студенты изучают классификацию инцидентов, процессы расследования и устранения последствий, а также методы предотвращения повторных инцидентов.

Целью освоения дисциплины является формирование у студентов навыков управления инцидентами информационной безопасности, включая разработку планов реагирования, проведение расследований и оценку эффективности принятых мер.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Основы управления инцидентами 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-2	Способен разрабатывать комплекс мер по защите информации в автоматизированных системах при возникновении нештатных ситуаций	ПК-2.1 Обеспечивает функционирование средств защиты информации в автоматизированных системах; ПК-2.2 Восстанавливает работоспособность средств защиты информации в автоматизированных системах при внештатных ситуациях; ПК-2.3 Разрабатывает предложения по совершенствованию средств защиты информации автоматизированных систем;
ПК-3	Способен проводить оценку уровня защищенности автоматизированных систем	ПК-3.1 Выполняет мониторинг защищенности информации в автоматизированных системах; ПК-3.2 Анализирует уязвимости внедряемой системы защиты информации; ПК-3.3 Проводит аудит защищенности информации в автоматизированных системах;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Основы управления инцидентами 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 «Основы управления инцидентами 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-2	Способен разрабатывать комплекс мер по защите информации в автоматизированных системах при возникновении нештатных ситуаций	<i>Информационная безопасность автоматизированных систем**;</i> <i>Технологическая и эксплуатационная безопасность программного обеспечения**;</i> <i>Специальные разделы математики (методы оптимизации)**;</i> <i>Моделирование процессов и систем защиты информации**;</i> <i>Гуманитарные аспекты информационной безопасности**;</i> <i>Основы информационного противоборства**;</i> <i>Организация и управление службой защиты информации**;</i> <i>Информационно-аналитическая деятельность по обеспечению комплексной безопасности**;</i>	
ПК-3	Способен проводить оценку уровня защищенности автоматизированных систем	<i>Международные стандарты в области информационной безопасности**;</i> <i>Международные аспекты управления сетью Интернет**;</i> <i>Специальные разделы математики (методы оптимизации)**;</i> <i>Моделирование процессов и систем защиты информации**;</i> <i>Сетевое и системное администрирование**;</i> <i>Построение и защита корпоративных информационных сетей**;</i>	

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Основы управления инцидентами информационной безопасности» составляет «5» 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)
			8
<i>Контактная работа, ак.ч.</i>	80		80
Лекции (ЛК)	40		40
Лабораторные работы (ЛР)	0		0
Практические/семинарские занятия (СЗ)	40		40
<i>Самостоятельная работа обучающихся, ак.ч.</i>	64		64
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	36		36
Общая трудоемкость дисциплины	ак.ч.	180	180
	зач.ед.	5	5

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	Основы управления инцидентами информационной безопасности	1.1	Общие положения	ЛК, СЗ
		1.2	Планирование системы менеджмента инцидентов ИБ защищенных информационных систем	ЛК, СЗ
		1.3	Использование системы менеджмента инцидентов ИБ защищенных информационных систем	ЛК, СЗ
		1.4	Анализ и улучшение системы менеджмента инцидентов ИБ защищенных информационных систем	ЛК, СЗ
		1.5	Менеджмент конкретных видов инцидентов ИБ защищенных информационных систем	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.	
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 Информационная технология - Методы и средства обеспечения безопасности - Менеджмент инцидентов информационной безопасности.

Дополнительная литература:

1. Зефирова С.Л. Менеджмент инцидентов информационной безопасности: учебное пособие. – Пенза: Издательство Пензенского государственного университета, 2008. – 124с.

2. ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management

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 «Основы управления инцидентами информационной безопасности».

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

РАЗРАБОТЧИК:

Должность, БУП

Подпись

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой

Должность БУП

Подпись

Подолько Павел
Михайлович [М]
заведующий кафедрой

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Должность, БУП

Подпись

Фамилия И.О.