

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 27.08.2026 15:53:52

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)

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 информационной безопасности. Дисциплина состоит из 1 раздела и 4 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 обучающихся 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 нештатных 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	Информационная безопасность автоматизированных систем**; Технологическая и эксплуатационная безопасность программного обеспечения**; Специальные разделы	

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
		математики (методы оптимизации)**; Моделирование процессов и систем защиты информации**; Гуманитарные аспекты информационной безопасности**; Основы информационного противоборства**; Организация и управление службой защиты информации**; Информационно-аналитическая деятельность по обеспечению комплексной безопасности**;	
ПК-3	Способен проводить оценку уровня защищенности автоматизированных систем	Information Security International Standards**; International Issues of Internet Governance**; Специальные разделы математики (методы оптимизации)**; Моделирование процессов и систем защиты информации**; Сетевое и системное администрирование**; Построение и защита корпоративных информационных сетей**;	

* - 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
Контактная работа, ак.ч	80		80
Лекции (ЛК)	40		40
Лабораторные работы (ЛР)	0		0
Практические/семинарские занятия (СЗ)	40		40
Самостоятельная работа обучающихся, ак.ч.	64		64
Контроль (экзамен/зачет с оценкой), ак.ч.	36		36
Общая трудоемкость дисциплины ак.ч.	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	Наименование темы		Вид учебной работы*
Раздел 1	Основы управления инцидентами информационной безопасности	1.1	Нормативные и организационные основы управления инцидентами ИБ	ЛК, СЗ
		1.2	Выявление, регистрация и классификация инцидентов ИБ	ЛК, СЗ
		1.3	Реагирование, расследование и восстановление после инцидентов	ЛК, СЗ
		1.4	Совершенствование процесса управления инцидентами и непрерывность	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. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие : [16+] / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=467139> (дата обращения: 15.04.2026). – Библиогр. в кн. – Текст : электронный.
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. Миловская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: Учебное пособие для вузов / Миловская 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.

2. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2026. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2238628> (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 «Основы управления инцидентами информационной безопасности».

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

РАЗРАБОТЧИКИ:

Заведующий кафедрой
информационной безопасности

Должность

Подпись

Царегородцев А.В.

Фамилия И.О

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой
информационной безопасности

Должность

Подпись

Царегородцев А.В.

Фамилия И.О

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой
информационной безопасности

Должность

Подпись

Царегородцев А.В.

Фамилия И.О