МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И.
Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ В.Р. Храмшин

03.02.2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МЕТОДЫ, МОДЕЛИ И СРЕДСТВА МОНИТОРИНГА, ПРЕДУПРЕЖДЕНИЯ, ОБНАРУЖЕНИЯ И ПРОТИВОДЕЙСТВИЯ НАРУШЕНИЯМ И КОМПЬЮТЕРНЫМ АТАКАМ

Научная специальность
2.3.6. Методы и системы защиты информации, информационная безопасность

Уровень высшего образования - подготовка кадров высшей квалификации

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	2
Семестр	3

Магнитогорск
2026 год

Рабочая программа составлена на основе ФГТ (приказ Минобрнауки России от 20.10.2021 г. № 951)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
22.01.2026, протокол № 5

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
03.02.2026 г. протокол № 5

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
зав. кафедрой ИиИБ, д-р техн. наук _____ И.И. Баранкова

Рецензент:
начальник отдела информационной безопасности «КУБ» (АО) ,

_____ М.М.Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целью дисциплины «Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам» является формирование профессиональных навыков мониторинга, тестирования ИС на выявление нарушений безопасности

2 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам» обучающийся должен обладать следующими компетенциями:

КНС-2 Способен разрабатывать, модифицировать и применять методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам	

3. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 2 зачетных единиц 72 акад. часов, в том числе:
– контактная работа – 42 акад. часов:
– аудиторная – 42 акад. часов;
– внеаудиторная – 0 акад. часов;
– самостоятельная работа – 30 акад. часов;

Форма аттестации - зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)		Самостоятельная работа студента	Форма текущего контроля успеваемости и промежуточной аттестации
		Лек.	практ. зан.		
1. Подходы и методы выявления нарушений ИБ					
1.1 Способы построения «образа» нормального функционирования защищаемой системы. Определение общего показателя аномальности.	3	4	4	12,8	Выполнение задания, собеседование
1.2 Анализ методов обнаружения злоупотреблений. Базы сигнатур атак.		4	10	10	Выполнение задания, собеседование
1.3 Методы обнаружения аномалий: накопление наиболее характерной статистической информации для каждого параметра оценки; обучение нейронных сетей значениями параметров оценки; событийное представление;		5	5	4,2	Выполнение задания, собеседование
1.4 Получение единой оценки состояния защищаемой системы. Статистика Байеса.		8	2	3	Выполнение задания, собеседование
Итого по разделу		21	21	30	
Итого за семестр		21	21	30	зачёт
Итого по дисциплине		21	21	30	зачет

4 Оценочные средства для проведения текущей и промежуточной аттестации

Представлены в приложении 1.

5 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Лозовецкий, В. В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей : учебное пособие для вузов / В. В. Лозовецкий, Е. Г. Комаров, В. В. Лебедев ; под редакцией В. В. Лозовецкий. — 2-е изд., стер. — Санкт-Петербург : Лань, 2024. — 488 с. — ISBN 978-5-507-47615-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/397355 (дата обращения: 11.03.2026). — Режим доступа: для авториз. пользователей.

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 352 с. — (Высшее образование). — ISBN 978-5-534-19386-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 234 — URL: https://urait.ru/bcode/586060/p.234 (дата обращения: 11.03.2026).

б) Дополнительная литература:

1. Брюхомицкий, Ю.А. Искусственные иммунные системы в информационной безопасности: учебное пособие / Ю. А. Брюхомицкий; Южный федеральный университет. - Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2019. - 147 с. - ISBN 978-5-9275-3212-4. - Текст: электронный. - URL: https://new.znanium.com/catalog/product/1088177 (дата обращения: 11.03.2026)

в) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно	бессрочно
LibreOffice	свободно	бессрочно
Браузер	свободно	бессрочно
Браузер Mozilla	свободно распространяемое	бессрочно
Linux	свободно	бессрочно
MS Visual Studio Code	свободно распространяемое	бессрочно
СЗИ Страж NT в.3	К-271-12 от 16.10.2012	бессрочно
VIP Net Client	Д-946-14 от	бессрочно
VIP Net CryptoService	Д-946-14 от 22.07.2014	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский индекс научного	URL: https://elibrary.ru/project_risc.asp

Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053
Информационная система - Банк данных угроз безопасности	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962

ПРИЛОЖЕНИЕ 1

Оценочные средства для проведения текущей и промежуточной аттестации

КНС-2 Способен разрабатывать, модифицировать и применять методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам
Задания: 1. Провести сравнительный анализ (методов и алгоритмов, используемых в работе систем) 2х систем обнаружения и предотвращения вторжений (IPS/IDS), имеющихся на сегодняшний день на рынке 2. Написать алгоритм администрирования выбранной системы выявления нарушений информационной безопасности в виде майнд-карты с учетом требований безопасности информации Теоретические вопросы: 1. Обнаружение аномалий в защищаемой системе. 2. Обнаружение злоупотреблений в защищаемой системе. 3. Накопление наиболее характерной статистической информации для каждого параметра оценки. 4. Обучение нейронных сетей значениями параметров оценки. 5. Статистика Байеса.

Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

– на оценку «**зачтено**» – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации;

– на оценку «**не зачтено**» – обучающийся не может показать знания на уровне воспроизведения и объяснения информации.