

Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ДАННЫХ И ПРОЦЕССОВ

Блок:	Блок 1 «Дисциплины (модули)»
Часть образовательной программы:	Часть, формируемая участниками образовательных отношений
№ дисциплины по учебному плану:	Б4.Ч.01
Трудоемкость в зачетных единицах:	1 семестр - 2;
Часов (всего) по учебному плану:	72 часа
Лекции	1 семестр - 16 часов;
Практические занятия	не предусмотрено учебным планом
Лабораторные работы	не предусмотрено учебным планом
Консультации	проводится в рамках часов аудиторных занятий
Самостоятельная работа	1 семестр - 55,7 часа;
в том числе на КП/КР	не предусмотрено учебным планом
Иная контактная работа	проводится в рамках часов аудиторных занятий
включая:	
Контрольная работа	
Промежуточная аттестация:	
Зачет	1 семестр - 0,3 часа;

Москва 2022

ПРОГРАММУ СОСТАВИЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Минзов А.С.
	Идентификатор	R17801759-MinzovAS-e8de8907

(подпись)

А.С. Минзов

(расшифровка
подписи)

СОГЛАСОВАНО:

Руководитель
образовательной программы

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Минзов А.С.
	Идентификатор	R17801759-MinzovAS-e8de8907

(подпись)

А.С. Минзов

(расшифровка
подписи)

Заведующий выпускающей
кафедры

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю. Невский

(расшифровка
подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: формирование у обучаемых знаний принципов, методов, технологий и средств применения систем извлечения знаний методами Data Mining и интеллектуального анализа данных для комплексной оценки безопасности автоматизированных систем управления и разработки систем проактивной защиты информации на основе анализа событий в информационной системе

Задачи дисциплины

- приобрести знания о технологиях интеллектуального анализа;
- приобрести знания о технологии Data Mining и обрести навыки по её практическому применению;
- овладеть навыками по разработке систем проактивной информационной безопасности на основе анализа событий в информационной системе;
- приобрести знания о технологиях разработки экспертных систем для оценки безопасности ИС и обрести навыки по реализации данных технологий в профессиональной деятельности.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
ПК-1 Оценивание уровня безопасности компьютерных систем и сетей	ПК-1.5 _{ПК-1} Проводит инструментальный мониторинг защищенности компьютерных систем и сетей	знать: - статистические методы обработки данных большого объема; - принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений; - классификацию технологий интеллектуального анализа данных и классификацию задач, при решении которых целесообразно с использованием технологий интеллектуального анализа данных и методов искусственного интеллекта. уметь: - применять методы и технологии применения ИТ экспертных систем в профессиональной деятельности; - разрабатывать систему проактивной информационной безопасности на основе анализа событий в информационной системе; - использовать технологию Data Mining и оболочки экспертных систем на практике.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам основной профессиональной образовательной программе Управление информационной безопасностью (далее – ОПОП),

направления подготовки 10.04.01 Информационная безопасность, уровень образования: высшее образование - магистратура.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа							СР			
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
КПР	ГК	ИККП	ТК											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Технологии и средства интеллектуального анализа	22	1	2	-	-	-	-	-	-	-	20	-	<p><u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Технологии и средства интеллектуального анализа"</p> <p><u>Подготовка к аудиторным занятиям:</u> Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><u>Подготовка домашнего задания:</u> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Технологии и средства интеллектуального анализа" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.</p> <p><u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Технологии и средства интеллектуального анализа"</p> <p><u>Изучение материалов литературных источников:</u> [2], 5-112 [3], 5-120</p>
1.1	Термины и определения	22		2	-	-	-	-	-	-	-	-	20	

2	Теоретические основы техно-логий интеллектуального анализа и экспертных систем для оценки безопасности ИС	24		6	-	-	-	-	-	-	-	18	-	<u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Теоретические основы техно-логий интеллектуального анализа и экспертных систем для оценки безопасности ИС" <u>Подготовка к аудиторным занятиям:</u>
2.1	Статистические методы обработки данных большого объема (BigDate): корреляционный, кластерный и регрессионный анализ	24		6	-	-	-	-	-	-	-	18	-	Проработка лекции, выполнение и подготовка к защите лаб. работы <u>Подготовка домашнего задания:</u> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Теоретические основы техно-логий интеллектуального анализа и экспертных систем для оценки безопасности ИС" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. <u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Теоретические основы техно-логий интеллектуального анализа и экспертных систем для оценки безопасности ИС" <u>Изучение материалов литературных источников:</u> [2], 256-300
3	Практическое применение технологии Data Mining и экспертных систем	25.7		8	-	-	-	-	-	-	-	17.7	-	<u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Практическое применение технологии Data Mining и экспертных систем" <u>Подготовка к аудиторным занятиям:</u>
3.1	Практическое использование технологии Data Mining и оболочек	25.7		8	-	-	-	-	-	-	-	17.7	-	Проработка лекции, выполнение и подготовка к защите лаб. работы <u>Подготовка домашнего задания:</u> Подготовка домашнего задания направлена

	экспертных систем												на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Практическое применение технологии Data Mining и экспертных систем" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. <u>Изучение материалов литературных источников:</u> [1], 5-65
	Зачет	0.3	-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	72.0	16	-	-	-	-	-	-	0.3	55.7	-	
	Итого за семестр	72.0	16	-	-	-	-	-	-	0.3	55.7	-	

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПр – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Технологии и средства интеллектуального анализа

1.1. Термины и определения

Классификация задач, решение которых целесообразно с использованием технологий интеллектуального анализа данных и методов искусственного интеллекта. Классификации технологий интеллектуального анализа данных.

2. Теоретические основы техно-логий интеллектуального анализа и экспертных систем для оценки безопасности ИС

2.1. Статистические методы обработки данных большого объема (BigDate):
корреляционный, кластерный и регрессионный анализ

Выявление латентных переменных методами факторного анализа. Анализ журналов событий. Разработка систем проактивной информационной безопасности на основе анализа событий в информационной системе. Технологии разработки экспертных систем для комплексной оценки безопасности ИС.

3. Практическое применение технологии Data Mining и экспертных систем

3.1. Практическое использование технологии Data Mining и оболочек экспертных систем
Методы и технологии применения ИТ экспертных систем в профессиональной деятельности.

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Технологии и средства интеллектуального анализа"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Теоретические основы техно-логий интеллектуального анализа и экспертных систем для оценки безопасности ИС"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Практическое применение технологии Data Mining и экспертных систем"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)			Оценочное средство (тип и наименование)
		1	2	3	
Знать:					
классификацию технологий интеллектуального анализа данных и классификацию задач, при решении которых целесообразно с использованием технологий интеллектуального анализа данных и методов искусственного интеллекта	ПК-1.5 _{ПК-1}	+			Контрольная работа/Контрольное задание № 1. Классификация задач, решение которых целесообразно с использованием экспертных систем. Контрольное задание № 2. Принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений.
принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений	ПК-1.5 _{ПК-1}			+	Контрольная работа/Контрольное задание № 5. Практическое задание по использованию технологии Data Mining
статистические методы обработки данных большого объема	ПК-1.5 _{ПК-1}		+		Контрольная работа/Контрольное задание № 3. Практическое задание по использованию статистического метода обработки данных большого объема BigDate. 4. Контрольное задание № 4. Разработка систем проактивной информационной без-опасности на основе анализа событий в информационной системе.
Уметь:					
использовать технологию Data Mining и оболочки экспертных систем на практике	ПК-1.5 _{ПК-1}	+			Контрольная работа/Контрольное задание № 3. Практическое задание по использованию статистического метода обработки данных большого объема BigDate. 4. Контрольное задание № 4. Разработка систем проактивной информационной без-опасности на основе анализа событий в информационной системе.
разрабатывать систему проактивной информационной безопасности на основе анализа событий в информационной системе	ПК-1.5 _{ПК-1}		+		Контрольная работа/Контрольное задание № 1. Классификация задач, решение которых целесообразно с использованием экспертных систем. Контрольное задание

				<p>№ 2. Принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений.</p> <p>Контрольная работа/Контрольное задание № 6. Методы и технологии применения ИТ экспертных систем в профессиональной деятельности</p>
<p>применять методы и технологии применения ИТ экспертных систем в профессиональной деятельности</p>	ПК-1.5 _{ПК-1}		+	<p>Контрольная работа/Контрольное задание № 3.</p> <p>Практическое задание по использованию статистического метода обработки данных большого объема BigDate. 4.</p> <p>Контрольное задание № 4. Разработка систем проактивной информационной без-опасности на основе анализа событий в информационной системе.</p>

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

1 семестр

Форма реализации: Письменная работа

1. Контрольное задание № 1. Классификация задач, решение которых целесообразно с использованием экспертных систем. Контрольное задание № 2. Принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений. (Контрольная работа)
2. Контрольное задание № 3. Практическое задание по использованию статистического метода обработки данных большого объема BigDate. 4. Контрольное задание № 4. Разработка систем проактивной информационной без-опасности на основе анализа событий в информационной системе. (Контрольная работа)
3. Контрольное задание № 5. Практическое задание по использованию технологии Data Mining (Контрольная работа)
4. Контрольное задание № 6. Методы и технологии применения ИТ экспертных систем в про-фессиональной деятельности (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет (Семестр №1)

В диплом выставляется оценка за 1 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Маннинг, К. Д. Введение в информационный поиск : пер. с англ. / К. Д. Маннинг, П. Рагхаван, Х. Шютце . – М. : Вильямс, 2011 . – 528 с. - ISBN 978-5-8459-1623-5 .;
2. Дюк, В. Data Mining: Учебный курс / В. Дюк, А. Самойленко . – СПб. : Питер, 2001 . – 368 с. + CD-ROM . – (Учебный курс) . - ISBN 5-318-00227-7 .;
3. "Интеллектуальный анализ данных средствами MS SQL Server 2008", (2-е изд.), Издательство: "ИНТУИТ", Москва, 2016 - (337 с.)
<https://e.lanbook.com/book/100609>.

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. ЭБС Лань - <https://e.lanbook.com/>
2. ЭБС "Университетская библиотека онлайн" - http://biblioclub.ru/index.php?page=main_ub_red
3. Электронные ресурсы издательства Springer - <https://link.springer.com/>
4. База данных Web of Science - <http://webofscience.com/>
5. База данных Scopus - <http://www.scopus.com>
6. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
7. Журнал Science - <https://www.sciencemag.org/>
8. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
9. Портал открытых данных Российской Федерации - <https://data.gov.ru>
10. Информационно-справочная система «Кодекс/Техэксперт» - <Http://proinfosoft.ru;>
<http://docs.cntd.ru/>
11. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>
12. Открытая университетская информационная система «РОССИЯ» - <https://uisrussia.msu.ru>

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения промежуточной аттестации	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Интеллектуальный анализ данных и процессов

(название дисциплины)

1 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Контрольное задание № 1. Классификация задач, решение которых целесообразно с использованием экспертных систем. Контрольное задание № 2. Принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений. (Контрольная работа)
- КМ-2 Контрольное задание № 3. Практическое задание по использованию статистического метода обработки данных большого объема BigDate. 4. Контрольное задание № 4. Разработка систем проактивной информационной без-опасности на основе анализа событий в информационной системе. (Контрольная работа)
- КМ-3 Контрольное задание № 5. Практическое задание по использованию технологии Data Mining (Контрольная работа)
- КМ-4 Контрольное задание № 6. Методы и технологии применения ИТ экспертных систем в про-фессиональной деятельности (Контрольная работа)

Вид промежуточной аттестации – Зачет.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Технологии и средства интеллектуального анализа					
1.1	Термины и определения		+	+		
2	Теоретические основы техно-логий интеллектуального анализа и экспертных систем для оценки безопасности ИС					
2.1	Статистические методы обработки данных большого объема (BigDate): корреляционный, кластерный и регрессионный анализ		+	+		+
3	Практическое применение технологии Data Mining и экспертных систем					
3.1	Практическое использование технологии Data Mining и оболочек экспертных систем			+	+	
Вес КМ, %:			25	25	25	25