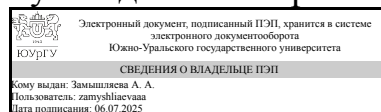


ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления



А. А. Замышляева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.11 Информационная безопасность интеллектуальных систем
для направления 02.04.02 Фундаментальная информатика и информационные технологии

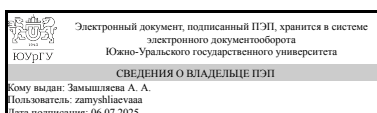
уровень Магистратура

форма обучения очная

кафедра-разработчик Прикладная математика и программирование

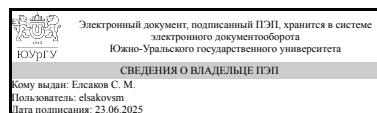
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 02.04.02 Фундаментальная информатика и информационные технологии, утверждённым приказом Минобрнауки от 23.08.2017 № 811

Зав.кафедрой разработчика,
д.физ.-мат.н., проф.



А. А. Замышляева

Разработчик программы,
к.физ.-мат.н., доцент



С. М. Елсаков

1. Цели и задачи дисциплины

Дисциплина «Информационная безопасность интеллектуальных систем» направлена на формирование у студентов теоретических знаний и практических навыков по обеспечению безопасности в условиях функционирования интеллектуальных систем, включая системы на основе искусственного интеллекта (ИИ), машинного обучения и больших данных. Задачи: Изучить современные угрозы и уязвимости, характерные для интеллектуальных систем. Освоить методы и технологии защиты данных, алгоритмов и архитектур ИИ. Разработать практические навыки применения инструментов обеспечения безопасности в реальных сценариях.

Краткое содержание дисциплины

1. Основы информационной безопасности интеллектуальных систем. 2. Нормативные требования в области безопасности интеллектуальных систем. 3. Моделирование угроз в области безопасности интеллектуальных систем. 4. Безопасность жизненного цикла ML/AI-систем. 5. Методы и инструменты обеспечения информационной безопасности интеллектуальных систем.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-4 Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	Умеет: использовать криптографические сервисы для проверки и обеспечения безопасности интеллектуальных систем Имеет практический опыт: комбинировать существующие информационно-коммуникационные технологии с учетом требований информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Нет

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 38,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		3
Общая трудоёмкость дисциплины	108	108
<i>Аудиторные занятия:</i>	32	32
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	69,5	69,5
Подготовка к д. зачету	69,5	69,5
Консультации и промежуточная аттестация	6,5	6,5
Вид контроля (зачет, диф.зачет, экзамен)	-	диф.зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основы информационной безопасности интеллектуальных систем.	4	4	0	0
2	Нормативные требования в области безопасности интеллектуальных систем.	4	4	0	0
3	Моделирование угроз в области безопасности интеллектуальных систем.	8	4	4	0
4	Методы и инструменты обеспечения информационной безопасности интеллектуальных систем.	16	4	12	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Основы информационной безопасности интеллектуальных систем.	4
2	2	Нормативные требования в области безопасности интеллектуальных систем.	4
3	3	Моделирование угроз в области безопасности интеллектуальных систем.	4
4	4	Методы и инструменты обеспечения информационной безопасности интеллектуальных систем.	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	3	Моделирование угроз в области безопасности интеллектуальных систем.	4
2	4	Состязательные атаки	4
3	4	Реализация атак data poisoning, evasion attacks, model inversion, model stealing.	4
4	4	Реализация безопасного ML/AI процесса	4

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к д. зачету	Талипов, Н. Г. Интеллектуальные системы обеспечения информационной безопасности : учебное пособие / Н. Г. Талипов, А. С. Катасёв, Д. В. Катасёва. — Казань : КНИТУ-КАИ, 2022. — 156 с. — ISBN 978-5-7579-2596-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/366533 (дата обращения: 21.06.2025). — Режим доступа: для авториз. пользователей.	3	69,5

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-мestr	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учитывается в ПА
1	3	Текущий контроль	ПР1	1	20	Студентом предоставляется оформленный отчет. Оценивается качество оформления, соответствие нормативным документам. Общий балл при оценке складывается из следующих показателей: Есть постановка задачи ML/AI (предпочтительно диплом) - 2 балла. Подготовлен датасет - 3 балла. Сформированы метрики - 1 балла. Есть решение задачи - 5 баллов. Есть полное описание развертывание модели - 1 балла. Смоделированы угрозы - 5	дифференцированный зачет

						баллов. Разработаны предложения по безопасному развертыванию - 3 балла. Максимальное количество баллов – 20. Весовой коэффициент мероприятия – 1.	
2	3	Текущий контроль	ПР2	1	20	Студентом предоставляется оформленный отчет. Оценивается качество оформления, соответствие нормативным документам. Общий балл при оценке складывается из следующих показателей: Применены 5 состязательных атак - 10 баллов. Найдены примеры и шумы - 5 баллов. Продемонстрировать стойкость к подобным атакам - 5 баллов. Максимальное количество баллов – 20. Весовой коэффициент мероприятия – 1.	дифференцированный зачет
3	3	Текущий контроль	ПР3	1	20	Студентом предоставляется оформленный отчет. Оценивается качество оформления, соответствие нормативным документам. Общий балл при оценке складывается из следующих показателей: Реализовать 4 атаки - 12 баллов . Проверить качество данных - 4 балла. Реализовать защиту от атак - 4 балла. Максимальное количество баллов – 20. Весовой коэффициент мероприятия – 1.	дифференцированный зачет
4	3	Текущий контроль	ПР4	1	20	Студентом предоставляется оформленный отчет. Оценивается качество оформления, соответствие нормативным документам. Общий балл при оценке складывается из следующих показателей: Реализована своя задача в виде безопасного процесса - 15 баллов.	дифференцированный зачет

						Включить моделирование угроз и защиту от них - 3 балла. Исследовать метрики безопасного процесса - 2 балла. Максимальное количество баллов – 20. Весовой коэффициент мероприятия – 1.	
5	3	Промежуточная аттестация	Д. зачет	-	120	онтрольное мероприятие промежуточной аттестации (зачетная работа) включает устный ответ на билет и проводятся во время зачета При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов. В билете два вопроса. Критерии оценивания выполнения зачетной работы: - ответ на один вопрос из билета без замечаний – 30 баллов; - ответ на один вопрос из билета с недочетами – 20 баллов; - ответ на один вопрос из билета с грубыми замечаниями – 10 баллов; - нет ответа на один вопрос из билета – 0 баллов; - ответ на один дополнительный вопрос без замечаний – 30 баллов; - ответ на один дополнительный вопрос с недочетами – 20 баллов; - ответ на один дополнительный вопрос с грубыми замечаниями – 10 баллов; - нет ответ на один дополнительный вопрос – 0 баллов; Максимальное количество баллов за промежуточную аттестацию – 120.	дифференцированный зачет
6	3	Текущий контроль	Доклад	1	20	Студентом предоставляется оформленная презентация. Оценивается качество оформления, соответствие нормативным документам, количество вопросов. Общий балл при оценке	дифференцированный зачет

					складывается из следующих показателей: Каждый вопрос - 1 балл, но не более 10 баллов. Полнота раскрытия вопроса - 5 баллов. Актуальность темы - 5 баллов. Максимальное количество баллов – 20. Весовой коэффициент мероприятия – 1	
--	--	--	--	--	---	--

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
дифференцированный зачет	Прохождение контрольных мероприятий промежуточной аттестации не обязательно. Зачет проводится по билетам. В билете два вопроса. Билет выбирается случайным образом. Студенту дается 30 минут на подготовку. После этого он рассказывает ответы на вопросы билета. Студенту задается дополнительный вопрос по каждому вопросу.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ					
		1	2	3	4	5	6
ОПК-4	Умеет: использовать криптографические сервисы для проверки и обеспечения безопасности интеллектуальных систем	+	+	+	+	+	+
ОПК-4	Имеет практический опыт: комбинировать существующие информационно-коммуникационные технологии с учетом требований информационной безопасности	+	+	+	+	+	+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) *основная литература:*

Не предусмотрена

б) *дополнительная литература:*

Не предусмотрена

в) *отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:*

Не предусмотрены

г) *методические указания для студентов по освоению дисциплины:*

1. Самостоятельная работа

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Самостоятельная работа

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	ЭБС издательства Лань	Талипов, Н. Г. Интеллектуальные системы обеспечения информационной безопасности : учебное пособие / Н. Г. Талипов, А. С. Катасёв, Д. В. Катасёва. — Казань : КНИТУ-КАИ, 2022. — 156 с. — ISBN 978-5-7579-2596-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/366533 (дата обращения: 21.06.2025). — Режим доступа: для авториз. пользователей.
2	Основная литература	ЭБС издательства Лань	Безопасность систем искусственного интеллекта : учебное пособие / П. С. Ложников, А. Е. Сомотуга, С. С. Жумажанова, А. Е. Сулаво. — Омск : ОмГТУ, 2023 — Часть 2 : Доверенный искусственный интеллект — 2023. — 74 с. — ISBN 978-5-8149-3731-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/421598 (дата обращения: 21.06.2025). — Режим доступа: для авториз. пользователей.
3	Дополнительная литература	ЭБС издательства Лань	Данилов, В. В. Нейронные сети : учебное пособие / В. В. Данилов. — Донецк : ДонГУ, 2020. — 158 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/179953 (дата обращения: 21.06.2025). — Режим доступа: для авториз. пользователей.
4	Методические пособия для самостоятельной работы студента	ЭБС издательства Лань	Платонов, В. В. Технологии машинного обучения в кибербезопасности : учебное пособие / В. В. Платонов. — Вологда : Инфра-Инженерия, 2024. — 140 с. — ISBN 978-5-9729-2048-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/427904 (дата обращения: 21.06.2025). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)
2. Python Software Foundation-Python (бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№	Основное оборудование, стенды, макеты, компьютерная техника,
-------------	---	--

	ауд.	предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	333 (36)	Проектор
Практические занятия и семинары	333 (36)	Проектор, компьютеры