ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколинский Л. Б.
Пользователь: leonid.sokolinsky
Дата подписания: 26.05.2023

Л. Б. Соколинский

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.03 Защита информации методами искусственного интеллекта
для направления 09.04.04 Программная инженерия
уровень Магистратура
форма обучения очная
кафедра-разработчик Системное программирование

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.04.04 Программная инженерия, утверждённым приказом Минобрнауки от 19.09.2017 № 932

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

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколинский Л. Б.
Пользователь: leonid.sokolinsky
Дата подписания: 26.05.2023

Л. Б. Соколинский

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Никольская К. Ю.
Пользователь: nikolskaiaki
Дата подписания: 26.05.2023

К. Ю. Никольская

Челябинск

1. Цели и задачи дисциплины

Целью преподавания дисциплины является изучение основных концепций и практических аспектов в сфере защиты информации с использованием методов искусственного интеллекта. Задачами изучения дисциплины являются: 1. Ознакомить с основными задачами защиты информации, кейсами применения методов ИИ в защите информации. 2. Познакомить студентов с определением, классификацией и характеристиками сетевых атак и способов защиты, способами анализа сетевого трафика методами ИИ; 3. Рассмотреть основные технологические принципы устройства антивирусов, анализа вредоносной активности методами ИИ; 4. Разобрать на практике методы и способы противодействия мошенничеству, реализации антиспам-фильтров и антифрод-систем.

Краткое содержание дисциплины

В рамках дисциплины изучаются основные направления применения методов искусственного интеллекта в задачах защиты информации: противодействие сетевым атакам путем интеллектуального анализа данных о сетевом трафике, обнаружение вредоносной активности на вычислительных узлах, особенности реализации антивирусных программ с использованием ИИ, противодействие мошенничеству в прикладных сервисах и фильтрация спам-рассылок в почтовых сервисах.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
УК-91 Способен понимать фундаментальные принципы работы современных систем искусственного интеллекта, разрабатывать правила и стандарты взаимодействия человека и искусственного интеллекта и использовать их в социальной и профессиональной деятельности	Знает: содержание нормативно-правовых документов в сфере информационных технологий, искусственного интеллекта и информационной безопасности Умеет: использовать нормативно-правовые документы в сфере информационных технологий, искусственного интеллекта и информационной безопасности при разработке стандартов, норм и правил Имеет практический опыт: анализа сетевого трафика методами искусственного интеллекта
ОПК-1 Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте	Знает: основные типы сетевых атак и способы защиты, типы вредоносной активности, способы противодействия мошенничеству Умеет: применять наиболее подходящие алгоритмы машинного обучения и инструменты для задач защиты информации Имеет практический опыт: сбора данных в различных форматах; предварительной обработки данных; анализа и визуализации данных в задачах защиты информации
ОПК-4 Способен применять на практике новые научные принципы и методы исследований	Знает: методы искусственного интеллекта для решения задач защиты информации Умеет: применять алгоритмы машинного

	обучения и инструменты для задач защиты информации Имеет практический опыт: решения задачи защиты информации методами искусственного интеллекта
ПК-7 Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	Знает: новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях; особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях Умеет: разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях; модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

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., 38,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		1
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	32	32
Лекции (Л)	16	16

Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	69,75	69,75
Изучение основной и дополнительной литературы по защите информации	33,75	33.75
Подготовка к зачету	36	36
Консультации и промежуточная аттестация	6,25	6,25
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Введение в защиту информации	4	2	2	0
2	Сетевые атаки и способы защиты. Анализ сетевого трафика методами ИИ	14	8	6	0
3	Типы вредоносной активности. Антивирусы. Анализ вредоносной активности методами ИИ	6	2	4	0
4	Противодействие мошенничеству. Антиспам. Анализ контента на примере почтовых сервисов	8	4	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Введение в защиту информации. Основные задачи. Кейсы применения методов ИИ в защите информации.	2
2-3	2	Сетевые атаки и способы защиты	4
4-5	2	Анализ сетевого трафика методами ИИ	4
6	3	Типы вредоносной активности. Антивирусы. Анализ вредоносной активности методами ИИ	2
7	4	Противодействие мошенничеству. Антиспам.	2
8	4	Анализ контента на примере почтовых сервисов	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Семинар по кейсам применения методов ИИ в защите информации	2
2-5	2	Практические занятия по анализу сетевого трафика методами ИИ. Выявление аномалий по признаковому описанию трафика. Профилизация трафика на основе методов машинного обучения.	6
6	3	Семинар по кейсам выявления вредоносной активности методами ИИ	4
7-8	4	Практические занятия по выявлению спама в почтовых сервисах. Реализация спам-фильтров методами интеллектуального анализа текста.	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
Изучение основной и дополнительной литературы по защите информации	Основная литература 1-2 Дополнительная литература 1.	1	33,75
Подготовка к зачету	Основная литература 1, 2. Дополнительная литература 1	1	36

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-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	1	Текущий контроль	ПЗ-1. Доклады по кейсам применения методов ИИ в защите информации	5	3	3 балла: текст доклада тесно увязан с заявленной темой; актуальность представляемого материала обоснована и доказательна; доклад дополняется наглядной, информативной презентацией; материал доклада представляется эмоционально, громко и разборчиво; докладчик приводит конкретные примеры, подтверждающие те или иные факты из предметной области вопроса, акцентируя внимание на наиболее важные моменты материала; 2 балла: содержание доклада в основных моментах пересекается с заявленной темой; студент представляет материал доклада понятно и доступно; докладчик приводит конкретные примеры, подтверждающие те или иные факты из предметной области вопроса; 1 балла: текст доклада лишь частично отражает содержание заявленной темы; в ходе доклада студент практически всегда читает материал с листа; докладчик не приводит конкретных примеров,	зачет

						подтверждающих те или иные факты из предметной области вопроса, 0 баллов: доклад не подготовлен	
2	1	Текущий контроль	ПЗ-2. Анализ сетевого трафика методами ИИ. Выявление аномалий по признаковому описанию трафика. Профилизация трафика на основе методов машинного обучения.	2	3	3 балла: задание выполнено полностью, 2 балла: задание выполнено выполнено полностью, но допущены незначительные ошибки, или задание выполнено более, чем 50%, 1 балла: задание выполнено выполнено полностью, но допущены серьезные ошибки, или задание выполнено менее, чем 50%, 0 баллов: задание не выполнено	зачет
3	1	Текущий контроль	ПЗ-3. Доклады по кейсам выявления вредоносной активности методами ИИ	5	3	3 балла: текст доклада тесно увязан с заявленной темой; актуальность представляемого материала обоснована и доказательна; доклад дополняется наглядной, информативной презентацией; материал доклада представляется эмоционально, громко и разборчиво; докладчик приводит конкретные примеры, подтверждающие те или иные факты из предметной области вопроса, акцентируя внимание на наиболее важные моменты материала; 2 балла: содержание доклада в основных моментах пересекается с заявленной темой; студент представляет материал доклада понятно и доступно; докладчик приводит конкретные примеры, подтверждающие те или иные факты из предметной области вопроса; 1 балла: текст доклада лишь частично отражает содержание заявленной темы; в ходе доклада студент практически всегда читает материал с листа; докладчик не приводит конкретных примеров, подтверждающих те или иные факты из предметной области вопроса,	зачет
4	1	Текущий контроль	ПЗ-4. Реализация спам-фильтров методами интеллектуального анализа текста	8	3	3 балла: задание выполнено полностью, 2 балла: задание выполнено выполнено полностью, но допущены незначительные ошибки, или задание выполнено более, чем 50%, 1 балла: задание выполнено выполнено полностью, но допущены серьезные ошибки, или задание выполнено менее, чем 50%, 0 баллов: задание не выполнено	зачет
5	1	Проме-жуточная	Итоговый тест	-	20	Компьютерный тест состоит из 20 вопросов, позволяющих оценить	зачет

		аттестация				сформированность компетенций. На ответы отводится 1 час. 20 баллов: задание полностью выполнено без ошибок 1-19 баллов: задание выполнено частично или выполнено с ошибками 0 баллов: задание не выполнено	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (Положение о БРС утверждено приказом ректора от 24.05.2019 г. № 179, в редакции приказа ректора от 10.03.2022 г.No 25-13/09). Оценка за дисциплину формируется на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля. Зачтено: Величина рейтинга обучающегося по дисциплине 60…100 %. Незачтено: Величина рейтинга обучающегося по дисциплине 0…59 %. Если студент не согласен с оценкой, полученной по результатам текущего контроля, студент проходит мероприятие промежуточной аттестации в виде тестирования. Тестирование проводится в системе edu.susu.ru. Тест содержит 20 вопросов. На выполнение теста дается 60 минут. В этом случае оценка за дисциплину рассчитывается на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации. Фиксация результатов учебной деятельности по дисциплине проводится в день зачета при личном присутствии студента.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5
УК-91	Знает: содержание нормативно-правовых документов в сфере информационных технологий, искусственного интеллекта и информационной безопасности				+	+
УК-91	Умеет: использовать нормативно-правовые документы в сфере информационных технологий, искусственного интеллекта и информационной безопасности при разработке стандартов, норм и правил	+				+
УК-91	Имеет практический опыт: анализа сетевого трафика методами искусственного интеллекта		+		+	+
ОПК-1	Знает: основные типы сетевых атак и способы защиты, типы вредоносной активности, способы противодействия мошенничеству		+			+
ОПК-1	Умеет: применять наиболее подходящие алгоритмы машинного обучения и инструменты для задач защиты информации		+			+
ОПК-1	Имеет практический опыт: сбора данных в различных форматах; предварительной обработки данных; анализа и визуализации данных в задачах защиты информации		+			+
ОПК-4	Знает: методы искусственного интеллекта для решения задач защиты			+	+	+

	информации					
ОПК-4	Умеет: применять алгоритмы машинного обучения и инструменты для задач защиты информации			+	+	+
ОПК-4	Имеет практический опыт: решения задачи защиты информации методами искусственного интеллекта			+		+
ПК-7	Знает: новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях; особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях	+				+
ПК-7	Умеет: разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях; модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях	+				+

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. Метод.указания Защита информации методами искусственного интеллекта

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Метод.указания Защита информации методами искусственного интеллекта

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

			https://e.lanbook.com/book/156401. — Режим доступа: для авториз. пользователей.
2	Основная литература	Электронно-библиотечная система издательства Лань	Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2012. — 592 с. — ISBN 978-5-94074-637-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/3032. — Режим доступа: для авториз. пользователей.
3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Защита информации в центрах обработки данных : учебно-методическое пособие / И. А. Ушаков, В. А. Десницкий, А. А. Чечулин, Т. Е. Захарова. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2019. — 44 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180094. — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Зачет,диф.зачет	114-1 (2)	Компьютерный класс, имеется выход в интернет
Практические занятия и семинары	114-1 (2)	Компьютерный класс, имеется выход в интернет
Лекции	114-1 (2)	Компьютер и проектор