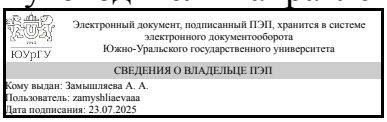
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления



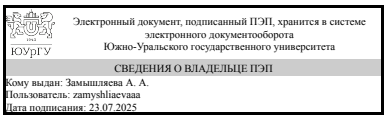
А. А. Замышляева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.31 Основы защиты данных в интеллектуальных системах
для направления 01.03.02 Прикладная математика и информатика
уровень Бакалавриат
форма обучения очная
кафедра-разработчик Центр ОП топ-уровня в сфере ИИ "ВиртУм"

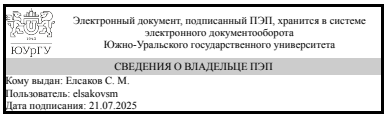
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 01.03.02 Прикладная математика и информатика, утверждённым приказом Минобрнауки от 10.01.2018 № 9

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



А. А. Замышляева

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



С. М. Елсаков

Челябинск

1. Цели и задачи дисциплины

Изучить основные методы и принципы защиты информации применительно к интеллектуальным системам. Овладение методикой построения комплексной защиты интеллектуальных систем. Сформировать умение работать с нормативными источниками, моделью системы и инструментами защиты данных для разных интеллектуальных систем.

Краткое содержание дисциплины

Основы организации защиты данных в интеллектуальных системах. Угрозы, атаки, риски, потери и инструменты защиты. Фреймворки и инструменты моделирования угроз. Современные инструменты сбора уязвимостей. Методики для оценки целевых акторов и техники атак. Определение поверхности атаки. Качественная и количественная оценка рисков, их приоритизация. Планирование реагирования на инциденты. Системы безопасные изначально. Проведение экспериментальных атак в песочнице. Состязательные атаки, атаки уклонения и методы защиты от них. Тестирование на проникновение в сервисы и модели. Проверка обнаруживаемости взлома. Метрики устойчивости к взлому. Инженерные методы проверки устойчивости системы. Повышение устойчивости систем с помощью дистилляции, сглаживания, подготовки данных, рандомизации, ансамблирования, калибровки, проверки диапазона выхода. Стеганография и цифровые водяные знаки. Методы предотвращение утечки данных. Симметричное, асимметричное, гомоморфное шифрование.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-9 Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	Знает: основные угрозы информационной безопасности (угрозы конфиденциальности, целостности и доступности данных) Умеет: выбрать адекватные средства защиты данных для каждого вида информационной системы Имеет практический опыт: установки и настройки защитных механизмов в информационных системах и базах данных
ОПК-12 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знает: основные модели и технологии защиты данных (идентификация, аутентификация, авторизация, шифрование, электронная подпись и др.) Умеет: использовать нормативные документы для построения защищенных ML-систем Имеет практический опыт: построения модели угроз для ML-систем
ОПК-13 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	Знает: основные стандарты в области информационной безопасности и искусственного интеллекта Умеет: разрабатывать подходы, согласно действующих норм, для создания доверенных

	обучающих наборов данных и доверенных систем искусственного интеллекта в задачах информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.15 Компьютерные сети	Не предусмотрены

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

Дисциплина	Требования
1.О.15 Компьютерные сети	Знает: принципы работы с сетевым оборудованием, принципы построения и функционирования компьютерных сетей, методы и технологии сетевой безопасности, общие характеристики коммуникационного оборудования (концентраторы, коммутаторы, маршрутизаторы), принципы организации, планирования и документирования компьютерных сетей, принципы коммутации в LAN сетях, принципы маршрутизации в LAN и WAN сетях, основные принципы построения и функционирования компьютерных сетей, сетевую модель взаимодействия открытых систем OSI, сетевую модель стека протоколов TCP/IP, протокол безопасной передачи данных https Умеет: настраивать сетевое оборудование для организации компьютерных сетей, -[И-1, БУ] организовать сетевые взаимодействия и передачу данных в рамках создания систем искусственного интеллекта, проектировать и настраивать компьютерные сети, обеспечивать безопасность и защиту сетей, планировать компьютерную сеть на основе требований, предъявляемых к сети, и технической документации оборудования, планировать модификацию (расширение) компьютерной сети на основе растущих требований к сети Имеет практический опыт: конфигурирования сетевого оборудования и организации компьютерных сетей, -[И-3, БУ] работы с основными средствами и методами, используемыми в индустрии ИТ для поддержания сетевой инфраструктуры промышленных систем искусственного интеллекта, планирования и организации, модификации и документирования компьютерной сети малого предприятия, настройки и конфигурирования VLAN и STP, настройки и конфигурирования статической и динамической маршрутизации, применения

	различных протоколов для поиска неисправностей в компьютерных сетях, настройки механизма NAT, настройки ACL списков

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 70,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		6
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	0	0
Лабораторные работы (ЛР)	32	32
Самостоятельная работа (СРС)	37,5	37,5
Подготовка к д. зачету	37,5	37.5
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 организации защиты данных в интеллектуальных системах	10	10	0	0
2	Криптография	24	12	0	12
3	Безопасность информационных систем	18	6	0	12
4	Безопасность интеллектуальных систем	12	4	0	8

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Основы организации защиты данных в интеллектуальных системах.	2
2	1	Нормативные требования в области безопасности интеллектуальных систем.	4
3	1	Моделирование угроз в области безопасности интеллектуальных систем.	2
4	1	Методы оценки рисков в области безопасности	2
5	2	Симметричные криптосистемы	2
6	2	Основы теории чисел	4
7	2	Асимметричные криптосистемы	4
8	2	Гомоморфные криптосистемы	2

9	3	Безопасность ОС	2
10	3	Безопасность в сетях	2
11	3	Безопасность в БД	2
12	4	Методы и инструменты обеспечения информационной безопасности интеллектуальных систем	4

5.2. Практические занятия, семинары

Не предусмотрены

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	2	Криптоанализ симметричной криптосистемы (статистический анализ)	2
2	2	Криптоанализ симметричной криптосистемы (полный перебор)	2
3	2	Криптоанализ RSA	2
4	2	Криптоанализ алгоритма Эль-Гамаля	2
5	2	Криптоанализ алгоритма на эллиптических кривых	4
6	3	Анализ защищенности ОС	4
7	3	Анализ защищенности Web-приложения	4
8	3	Реализация управления правами доступа в СУБД	4
9	4	Состязательные атаки	2
10	4	Отравление данных	2
11	4	Разработка модели угроз и системы безопасности	4

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	Гатченко, Н. А. Криптографическая защита информации : учебное пособие / Н. А. Гатченко, А. С. Исаев, А. Д. Яковлев. — Санкт-Петербург : НИУ ИТМО, 2012. — 142 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/40849 (дата обращения: 21.07.2025). — Режим доступа: для авториз. пользователей.	6	37,5

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-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	6	Текущий контроль	ЛР1	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей: - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла.	дифференцированный зачет
2	6	Текущий контроль	ЛР2	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл	дифференцированный зачет

						- выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла.	
3	6	Текущий контроль	ЛР3	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей: - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла.	дифференцированный зачет
4	6	Текущий контроль	ЛР4	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей: - приведены методики оценки	дифференцированный зачет

						технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла.	
5	6	Текущий контроль	ЛР5	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей: - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла.	дифференцированный зачет
6	6	Текущий контроль	ЛР6	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей:	дифференцированный зачет

						- приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла.	
7	6	Текущий контроль	ЛР7	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей: - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла.	дифференцированный зачет
8	6	Текущий контроль	ЛР8	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается	дифференцированный зачет

						из следующих показателей: - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла.	
9	6	Текущий контроль	ЛР9	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей: - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла.	дифференцированный зачет
10	6	Текущий контроль	ЛР10	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса).	дифференцированный зачет

						Общий балл при оценке складывается из следующих показателей: - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла.	
11	6	Текущий контроль	ЛР11	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей: - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла.	дифференцированный зачет
12	6	Проме-жуточная аттестация	Дифференцированный зачет	-	120	Контрольное мероприятие промежуточной аттестации (зачетная работа) включает устный ответ на билет и проводятся во время зачета При оценивании результатов мероприятия	дифференцированный зачет

						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.	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
дифференцированный зачет	Прохождение контрольных мероприятий промежуточной аттестации не обязательно. Дифференцированный 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	7	8	9	10	11	12
ОПК-9	Знает: основные угрозы информационной безопасности (угрозы конфиденциальности, целостности и доступности данных)	+	+	+	+	+	+	+	+	+	+	+	+
ОПК-9	Умеет: выбрать адекватные средства защиты данных для каждого вида информационной системы	+	+	+	+	+	+	+	+	+	+	+	+
ОПК-9	Имеет практический опыт: установки и настройки защитных механизмов в информационных системах и базах данных						+	+	+	+	+	+	+
ОПК-12	Знает: основные модели и технологии защиты данных (идентификация, аутентификация, авторизация, шифрование, электронная подпись и др.)	+	+	+	+	+	+	+	+	+	+	+	+
ОПК-12	Умеет: использовать нормативные документы для построения защищенных ML-систем	+	+	+	+	+	+	+	+	+	+	+	+
ОПК-12	Имеет практический опыт: построения модели угроз для ML-систем						+	+	+	+	+	+	+
ОПК-13	Знает: основные стандарты в области информационной безопасности и искусственного интеллекта									+	+	+	+
ОПК-13	Умеет: разрабатывать подходы, согласно действующих норм, для создания доверенных обучающих наборов данных и доверенных систем искусственного интеллекта в задачах 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. Методические указания

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Методические указания

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: 21.07.2025). — Режим доступа: для авториз. пользователей.
2	Основная литература	ЭБС издательства Лань	Безопасность систем искусственного интеллекта : учебное пособие / П. С. Ложников, А. Е. Самотуга, С. С. Жумажанова, А. Е. Сулавко. — 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: 21.07.2025). — Режим доступа: для авториз. пользователей.
3	Основная литература	ЭБС издательства Лань	Сергеева, Ю. С. Защита информации. Конспект лекций : учебное пособие / Ю. С. Сергеева. — Москва : А-Приор, 2011. — 128 с. — ISBN 978-5-9512-0397-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/3083 (дата обращения: 21.07.2025). — Режим доступа: для авториз. пользователей.
4	Основная литература	ЭБС 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 (дата обращения: 21.07.2025). — Режим доступа: для авториз. пользователей.
5	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: 21.07.2025). — Режим доступа: для авториз. пользователей.
6	Дополнительная литература	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: 21.07.2025). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

1. -Oracle VirtualBox(бессрочно)

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

Лабораторные занятия	333 (3б)	Компьютеры
Лекции	333 (3б)	Проектор