АННОТАЦИЯ рабочей программы дисциплины

Б1.В.02 Математические модели защиты информации

Объем трудоемкости: 2 з.е.

Цели дисциплины:

Целью освоения дисциплины «Математические модели защиты информации» является формирование у будущих специалистов в области прикладной информатики и искусственного интеллекта систематизированных знаний о математическом аппарате, лежащем в основе современных методов защиты информации, и выработка навыков его применения для обеспечения конфиденциальности, целостности и доступности данных и моделей на всех этапах жизненного цикла AI-систем.

Задачи дисциплины: в соответствии с поставленной целью состоят в следующем:

- Сформировать у студентов понимание фундаментальных математических моделей, используемых в криптографии.
- Научить формализовывать угрозы информационной безопасности для данных и алгоритмов в системах аналитики и ИИ, используя математический аппарат.
- Дать представление о принципах работы и области применения основных криптографических алгоритмов (симметричных, асимметричных, хеш-функций) с точки зрения лежащих в их основе сложных математических задач.
- Освоить на практическом уровне методы реализации базовых криптографических примитивов и протоколов.
- Показать взаимосвязь между защитой информации и технологиями ИИ, в частности, рассмотреть математические основы методов обеспечения конфиденциальности при обучении моделей (дифференциальная приватность) и противодействия атакам на ML-системы.

Место дисциплины в структуре ООП ВО

Дисциплина «Математические модели защиты информации» относится к «Части, формируемая участниками образовательных отношений» Блока 1 «Дисциплины (модули)» учебного плана.

Данная дисциплина тесно связана с дисциплинами: «Математический анализ», «Основы программирования», «Дифференциальные уравнения», «Математические модели нейронных сетей».

Материал курса является связующим звеном между математикой, программированием и прикладными задачами обеспечения безопасности данных. Знания, полученные в данной дисциплине, являются основой для преддипломной практики и ВКР.

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Роль 1: Data Analyst (Аналитик данных)

Задачи:

1. Статистический анализ, визуализация данных, предварительная обработка.
2. Создание прогнозных моделей
3. Построение аналитических моделей для поддержки бизнес-решений.

Роль 2: MLOps (Специалист по эксплуатации ИИ)

Задачи:

1. DevOps для ML.
2. Автоматизация, мониторинг ML-систем.
3. Операционное управление жизненным циклом ML-моделей.

Роль 3: AI PM (Менеджер проектов ИИ)

Задачи:

1. Управление ИИ-проектами от идеи до внедрения
2. Анализ бизнес-требований и постановка задач
3. Оценка эффективности и ROI ИИ-решений

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и содержание компетенции	Индикаторы	Уровни освоения индикаторов компетенции
ПК-1 Способен анализировать предметную область для выявления угроз информационной безопасности и формулировать требования к защите данных.	ПК-1.1 Анализирует компоненты информационной системы (данные, модели, каналы связи) с точки зрения потенциальных угроз конфиденциальности, целостности и доступности.	Проводит анализ конвейера данных и AI-модели для выявления уязвимых мест.
	ПК-1.2 Выбирает и обосновывает применение конкретных криптографических алгоритмов и методов для парирования выявленных угроз в рамках проектируемой системы.	Проводит сравнительный анализ cryptographic примитивов для решения конкретной прикладной задачи.
ML-6 Способен применять алгоритмы обучения с подкреплением.	ML-6.1 Применяет методы повышения устойчивости, надежности, безопасности алгоритмов обучения с подкреплением для проверки разведочных гипотез и подготовки данных к применению современных методов ИИ.	Применяет готовые RL-библиотеки и базовые методы контроля надежности (ограничение наград, настройка гиперпараметров) для обучения и тестирования моделей в простых симулированных средах.
AI S-1 Способен управлять рисками в разработке систем ИИ, выстраивать управление безопасностью ИИ в компании с учетом этики ИИ	AI S-1.1 Выявляет и моделирует угрозы на всём жизненном цикле ИИ-систем, оценивает и приоритизирует риски	Понимает основные категории рисков и атак на ИИ. Применяет типовые методики по готовым шаблонам. Знает международные фреймворки и стандарты.
	AI S-1.2 Обеспечивает соответствие нормативным требованиям и принципам доверенного/этичного ИИ.	Знаком с Кодексом этики в сфере ИИ РФ (2021), базовых принципах Responsible AI, законом 152-ФЗ «О перс. данных» и основами GDPR. Может описать процесс Data Impact Assessment.

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Введение. Математические основы и модели угроз.	15,8	2		2	11,8
2.	Математические модели симметричного шифрования.	10	2		2	6
3.	Математические модели хеширования и аутентификации.	8	2		2	4
4.	Математические модели асимметричного шифрования.	10	2		2	6
5.	Криптографические протоколы: математические модели доверия.	8	2		2	4
6.	Математические модели защиты	12	2		2	8

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
	конфиденциальности в AI: дифференциальная приватность.					
7.	Математические модели атак на AI-системы и защиты от них.	8	2		2	4
ИТОГО по разделам дисциплины		**69,8**	**14**		**14**	**41,8**
Контроль самостоятельной работы (КСР)		2				
Промежуточная аттестация (ИКР)		0,2				
Подготовка к текущему контролю						
Общая трудоемкость по дисциплине		**72**				

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет.

Автор: В.О. Осипян, профессор кафедры, д-р. ф.-м. н., доцент