Введение

В настоящее время общество находится в состоянии цифровой трансформации. Повсеместно проводится компьютеризация и интеграция локальных компьютерных сетей (КС) в единую структуру — сеть Интернет. Компьютеризации подвергаются как сети общего пользования — домашние локальные КС; корпоративные КС и т. д., так и специализированные — промышленные сети; сети, образованные устройствами Интернета вещей; государственные информационные сети.

Искусственный интеллект (ИИ) и связанные с ним машинное обучение и интеллектуальный анализ данных сегодня активно используют для продвижения нового поколения информационных систем. В контексте информационной безопасности (ИБ) искусственный интеллект — это методы, алгоритмы и их программная реализация (программное обеспечение, ПО), способное интерпретировать состояние среды, распознавать происходящие в ней события и самостоятельно принимать необходимые меры. В настоящее время технологии машинного обучения повсеместно применяются для решения множества задач классификации, прогнозирования и принятия решений. Все чаще в основе этих направлений лежат методы глубокого обучения.

В **первой главе** анализируются тенденции развития и использования искусственного интеллекта в сфере информационной безопасности, вводятся основные понятия интеллектуального анализа данных и машинного обучения (МО, *Machine Learning*). Анализируются методы обнаружения и классификации компьютерных атак и сетевых аномалий.

В условиях роста информационного пространства и необходимости автоматизации информационных процессов повышение эффективности существующих моделей и методов для построения систем классификации, анализ и управление текстовой информацией являются важными и актуальными научно-техническими задачами.

Применение технологии машинного обучения в области информационной безопасности крайне востребовано для специалистов. В частности, инструменты машинного обучения используются для выявления угроз сетевой безопасности и, соответственно, угроз конфиденциальным данным, которые в этих сетях хранятся, обрабатываются и передаются.

Необходимо обнаруживать и противостоять сетевым атакам, анализировать и устранять уязвимости, заниматься наполнением базы знаний о киберугрозах. Однако огромный объем данных (логов) и многочисленные задачи не позволяют провести анализ в реальном времени. Решить подобные задачи позволяют технологии МО и искусственного интеллекта.

МО, представляющее собой комплекс инструментальных и методических средств, позволяющих значительно сократить долю человеческого участия в создании систем искусственного интеллекта, в том числе средствами автоматической валидации результатов моделирования, является одним из ключевых инструментов для обеспечения кибербезопасности.

Во **второй, третьей и четвертой** главах рассмотрены вопросы классификации и кластеризации данных средствами МО, а также метрики оценки эффективности результатов их обработки. На основе математической постановки задачи классификации в **главах 2 и 3** рассматривается широкий ассортимент существующих методов и алгоритмов: линейный классификатор; логистическая регрессия; байесовский классификатор; наивный байесовский классификатор; KNN; алгоритмы на основе деревьев решений; CART; C4.5; CHAID; леса решений; случайный лес; ансамблевые алгоритмы. Рассматриваются методы композиции обучающихся алгоритмов: бустинг, бэггинг и стекинг.

С учетом направленности дальнейшего изложения в **третьей главе** анализируются классические методы МО, включая алгоритмы классификации с помощью нейронных сетей и сетей глубокого обучения. Анализируются сети глубокого обучения (Deep neural network, DNN); сверточные нейронные сети (convolutional neural network, CNN); рекурсивные (рекуррентные) нейронные сети (Recurrent Neural Network, RNN), построенные по принципу LSTM (Long Short-Term Memory) и GRU (Gated Recurrent Units); нейронные сети типа «автокодировщик»; нейронные сети типа «Трансформер».

Рассматриваемые архитектуры искусственных нейронных сетей не являются всеобъемлющими, поскольку рассматривае-

мая предметная область бурно развивается. Нейронные сети типа «Трансформер» появились в 2016 году, однако в настоящий момент являются лидерами в задачах обработки естественного языка (BERT, chatGPT); обработки и порождения изображений (Stable Diffusion, Midjourney).

Заметна тенденция к созданию гибридных искусственных нейронных сетей, включающих в свою архитектуру сразу несколько «базовых компонентов» — свертку, полносвязаные слои.

Рассмотрены особенности построения современных искусственных нейронных сетей, включая стратегии дообучения на существующих моделях; гиперсети; стратегия «Low-Rank Adaptation» (LoRA).

Важное место занимают вопросы обработки потоковых данных, включая алгоритмы Adaptive Random Forest и алгоритмы обнаружения смены дрейфа концепта.

Для обеспечения информационной и общественной безопасности большое значение имеет анализ в телекоммуникационных сетях контента, содержащего противоправную информацию (в том числе данные, связанные с терроризмом, наркоторговлей, подготовкой протестных движений или массовых беспорядков). В этой связи классификация текстов является одной из важных задач информационной безопасности, поскольку к ней сводится ряд других задач: определение тематической принадлежности текстов, автора текста, эмоциональной окраски высказываний и др. В главе рассматриваются основные этапы и алгоритмы классификации текстовой информации. Основное внимание уделено вопросам классификации текстов на основе искусственных нейронных сетей.

В **главе 4** анализируются наиболее распространенные методы кластеризации, включая иерархические, неиерархические и сетевые методы. Рассматриваются такие методы кластеризации, как: CURE, BIRCH, MST, k-means, PAM, CLOPE, самоорганизующиеся карты Кохонена, алгоритм HCM, Fuzzy C-means, Bath k-means, Online k-means. Рассматриваются метрики оценки качества алгоритмов кластеризации: полнота (Recall), точность (Precision), чистота (purity), индекс случайности (Rand index), F-мера (F-measure), индекс Жаккара (Jaccard index), индекс Dice (Dice index), индекс Fowlkes-Mallows, однородность (Homogeneity), полнота (completeness), V-мера, коэффициент силуэта (silhouette coefficient), индекс Калински-Харабаза (Calinski-Harabasz Index), индекс Ренда (Adjusted Rand Index).

Глава 5 посвящена программной реализация алгоритмов машинного обучения с использованием Python. Здесь рассмотрены вопросы практической программной реализации анализируемых алгоритмов МО на примере задач обнаружения компьютерных атак. Рассматривается работа с PyCharm, особенности настройки программной среды через интерпретатор Anaconda и через Python без сторонних интерпретаторов. Рассматриваются распространенные проблемы при создании проекта в среде PyCharm.

Работа в среде PyCharm выполняется посредством анализа данных, порожденных в результате реализации атаки типа Botnet. Выполняется предобработка входных данных — выполняется визуальная оценка данных; проводится проверка данных на наличие выбросов, нечисловых и отсутствующих значений; данные масштабируются; строится корреляционная диаграмма и диаграмма взаимного распределения атрибутов исследуемых экспериментальных данных. Данные разделяются на тестовую и обучающую части, выбирается функция потерь. Компьютерная атака обнаруживается при помощи четырех алгоритмов машинного обучения: многослойного персептрона, Random Forest, Gaussian NB, KNN. Приводится сравнительный анализ алгоритмов классификации.

В главе также рассматривается многозначная классификация в контексте ее применимости в задачах информационной безопасности и кибербезопасности.

В качестве приложения к пособию прикладывается Лабораторный комплекс, в котором приведен перечень некоторых лабораторных работ, реализуемых в программной среде Python на примере доступных в Интернете баз данных.

В основу пособия положены курсы лекций, читаемые авторами во МТУСИ для профиля 10.03.02 «Безопасность компьютерных систем» и 10.04.02 «Интеллектуальные технологии безопасности компьютерных систем».