Системы, использующие методы машинного обучения, становятся всё более автономными. Нейроморфные процессоры, имитирующие работу человеческого мозга, позволят создавать устройства, которые смогут анализировать потоковые данные на аппаратном уровне. Это обеспечит минимальную задержку обработки и снижение энергозатрат.

Заключение: Искусственный интеллект и машинное обучение стали неотъемлемой частью анализа больших данных, особенно в задачах, требующих обработки потоков информации в реальном времени. Эти технологии позволяют быстро и точно выявлять аномалии, тренды и паттерны. Повышать производительность систем и снижать затраты. Создавать новые решения для сложных задач в таких областях, как финансы, здравоохранение, интернета вещей и безопасность.Однако остаются вызовы, связанные с высокими вычислительными требованиями, качеством данных и интерпретацией моделей. Тем не менее, дальнейшее развитие технологий, таких как квантовые вычисления и нейроморфные системы, открывает огромные перспективы для более эффективного использования искусственного интеллекта и машинного обучение.

ЛИТЕРАТУРА

1. Goodfellow I., Bengio Y., Courville A. “Deep Learning”, MIT Press, 2016.

2. Chollet F. “Deep Learning with Python”, Manning Publications, 2021.

3. McKinsey & Company: "Big Data and AI: Future Trends", 2023.

4. Apache Kafka Documentation: https://kafka.apache.org/

5. Apache Flink Documentation: https://flink.apache.org/

УДК 004.92

С.А. Евдокимова, доц., канд. техн. наук
(ВГУИТ, г. Воронеж, Россия)

УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ КОМПЬЮТЕРНОГО ЗРЕНИЯ

Компьютерное зрение – это область искусственного интеллекта, которая занимается разработкой алгоритмов и методов для анализа и интерпретацией визуальной информацией (изображения и видео) [1].

Компьютерное зрение и машинное (техническое) зрение часто используются как взаимозаменяемые термины, но между ними есть небольшие различия, хотя оба направления связаны с анализом и интерпретацией визуальных данных. Машинное зрение чаще всего при-

меняется в условиях контролируемой среды, где условия освещения, фон и положение объектов заранее известны, что упрощает задачу разработки алгоритмов и повышает надежность системы. Машинное зрение используют для поддержки производственного процесса, его автоматизации и уменьшения количества брака. Примерами применения технического зрения являются контроль качества, когда проверка деталей на наличие дефектов выполняется автоматически, определение положения и ориентации деталей, с которыми взаимодействуют промышленные роботы [2].

Компьютерное зрение предназначено для решения задач нахождения объектов на изображении, которые делятся на следующие виды:

– классификация – входное изображение пытаются отнести к одной определенной категории в зависимости от присутствия на нем характерных признаков;

– обнаружение объектов (или классификация с локализацией) – дополнительно к задаче классификации решается задача определение рамки, ограничивающей местоположение объекта на исходном изображении;

– сегментация – входное изображение делится на значимые сегменты или области, которые могут соответствовать отдельным объектам или их частям. Семантическая сегментация определяет принадлежность каждого пикселя какому-то классу, а сегментация экземпляров позволяет выделить отдельные экземпляры объектов;

– детекция объектов – находит объекты на исходном изображении посредством поиска координат ограничивающих рамок и классификации содержания рамок на множестве заданных ранее классов. При этом количество объектов на изображении заранее неизвестно.

Главную роль в компьютерном зрении играют нейронные сети, которые применяются для решения задач распознавания лиц, в робототехнике, автономном вождении, медицинской диагностике и т.д.

В компьютерном зрении используются следующие виды нейронных сетей:

– полносвязные нейронные сети (Fully Connected Neural Networks, FCNN) – каждый нейрон связан с каждый нейроном в следующем слое. Используются для решения задач классификации и прогнозирования;

– сверточные нейронные сети (Convolutional Neural Networks, CNN) – используют сверточные слои для автоматического излучения признаков из входных данных, представляют собой алгоритм глубокого изучения, который применяется для обработки изображений;

– реккурентные нейронные сети (Recurrent Neural Networks, RNN) - используют свою внутреннюю память для обработки последовательностей произвольной длины;

– генеративно-состязательные сети (Generative Adversarial Networks, GAN) - способны генерировать реалистичные образцы данных.

Успехи в области компьютерного зрения связаны с появлением и развитием архитектуры сверточных сетей [1]. В начале вручную проводилось выделение характерных признаков объектов, однако при изменении ракурса, освещенности и масштаба изображений качество распознавания ухудшалось. Сверточные нейронные сети (CNN) являются разновидностью нейросетей для обработки данных с сеточной структурой, которая имеется у изображений и видео, и автоматически извлекают признаки из входного изображения за счет применения фильтрации. CNN анализируют пиксели, которые находятся близко друг к другу и содержат непрерывную визуальную информацию – яркость и цвет.

Примерами сверточных нейронных сетей являются AlexNet, ImageNet, ResNet, U-Net и другие.

Однако системы компьютерного зрения имеют ряд уязвимостей информационной безопасности, связанных с использованием нейронных сетей и моделей искусственного интеллекта [3, 4]. Наиболее популярными атаками являются состязательные атаки (Adversarial Attacks), которые вносят небольшие изменения в исходные данные для принятия неправильного решения. Они делятся на модели, называемые «белым ящиком», когда злоумышленник полностью знаком с архитектурой и параметрами модели. Имея знания о внутренних слоях, их количестве, весовых коэффициентов, злоумышленник может рассчитать оптимальные возмущения для неправильного вывода.

Атаки «черного ящика» проводятся без прямого доступа к параметрам модели. В этом случае злоумышленник не знаком с моделью, поэтому он использует методы подбора, отправку запросов для поиска подходящих параметров, а затем обучает похожую копию модели для генерации враждебных примеров. Данные атаки менее эффективны, но чаще используются.

Атаки типа «серый ящик» являются промежуточным вариантом, когда злоумышленник имеет частичную информацию о модели.

Также атаки бывают целенаправленные, когда преследуется цель изменения вывода модели на требуемое решение, и нецеленаправленные, когда важно любое нарушение правильной работы модели.

Существует ряд популярных примеров входных данных, которые используются, чтобы обмануть модель [3-5]. Например, метод быстрого градиентного распознавания (Fast Gradient Sign method – FGSM) – простой метод атаки на основе градиента функции потерь, который генерирует враждебные примеры с минимальным отличием от исходного изображения путем незначительного изменения пикселей по всему изображению.

Атаки по глубокой ошибке (Deepfool attack) направлены на создание выборки, которая имеет минимальное евклидово расстояние от исходного изображения, и возмущения добавляются к изображению итеративно.

Состязательные атаки предоставляют существенный риск для систем компьютерного зрения, поскольку даже мелкие модификации входного набора данных могут радикально изменить поведение модели нейронной сети [5]. Для противодействия им следует применять методы обучения устойчивого восприятия, основой которых является создание моделей, нечувствительных к малым изменениям входных данных.

Метод состязательной подготовки (Adversarial Training) включает дополнительное обучение модели нейронной сети на специально подготовленных примерах, чтобы модель постепенно адаптировалась к подобным искажениям и демонстрировала повышенную устойчивость.

Другим способом улучшения устойчивости модели является метод Data Augmentation with Noise Injection, который использует для обучения слегка зашумленные данные. Реальные графические изображения могут иметь разные уровни цвета, яркости, несовершенства, поэтому более широкий диапазон данных для обучения позволяет сделать модель машинного обучения менее чувствительной к небольшим колебаниям или искажениям в данных.

Таким образом, для повышения безопасности систем компьютерного зрения необходимо использовать методы состязательной тренировки для повышения устойчивости к атакам, не применять открытые наборы данных для обучения, проводить регулярные аудиты данных и моделей, контролировать доступ к входным данным и параметрам модели.

ЛИТЕРАТУРА

1. Шапиро, Л. Компьютерное зрение / Л. Шапиро. – М. : Бином. Лаборатория знаний, 2013. – 752 с.

2. Евдокимова, С.А. Интеллектуальные технологии, применяемые для автоматизации процесса сборки изделий / С.А. Евдокимова, Д.В. Аверьянов // Моделирование информационных систем и техно-

логий : сборник материалов Международной научно-практической конференции. – Воронеж, 2024. – С. 297-303.

3. Survey of adversarial attacks and defense against adversarial attacks / A. Jain, S. Agarwal, A. Pareek, V. Singh // Darpan International Research Analysis. – 2024. – Т. 12, № 3. – С. 535-542.

4. Исследование и статистический анализ атак на нейронные сети в задачах компьютерного зрения / Л.И. Капитонова, А.А. Ушакова, Н.А. Шална, А.А. Сторожева // Политехнический молодежный журнал. – 2019. - № 2(31). – С. 5.

5. Data reduction for black-box adversarial attacks against deep neural networks based on side-channel attacks / H. Zhou [et al.] // Computers & Security. – 2025. – Т. 153. – С. 104401.

УДК 004.7:004.05

М.Х. Нурлыева, преподаватель, кафедры информационных технологий
(Государственный энергетический институт Туркменистана, г. Мары, Туркменистан)

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ И ОБРАБОТКИ ДАННЫХ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

В условиях активного развития цифровых технологий передача и обработка данных становятся базовыми элементами функционирования современных информационных систем. Практически все сферы деятельности – промышленность, экономика, наука, образование и государственное управление – опираются на эффективный обмен данными и их аналитическую обработку.

Рост объемов информации, усложнение информационных потоков и повышение требований к скорости и надежности передачи данных обусловливают необходимость внедрения новых технологических решений. В связи с этим исследование современных технологий передачи и обработки данных является актуальной научно-технической задачей.

Роль передачи и обработки данных в цифровых системах

Передача и обработка данных образуют основу цифровой инфраструктуры. Они обеспечивают взаимодействие между распределенными элементами информационных систем и позволяют преобразовывать исходные данные в полезную управленческую и аналитическую информацию.

Эффективность цифровых систем напрямую зависит от:

- пропускной способности каналов связи;
- надежности передачи данных;