также маневрирование в ограниченных пространствах. Симулятор также учитывает влияние внешних факторов, таких как погодные условия или время суток, что значительно повышает реализм и помогает пользователю более точно представлять себе условия работы на реальной строительной площадке.

Для разработки симулятора использовались технологии Unity 3D и C#, которые позволяют создавать высококачественные 3D-модели и реализовывать физику взаимодействия экскаватора с грунтом и другими объектами. Важным аспектом разработки стала оптимизация пользовательского интерфейса, который был спроектирован с учётом удобства и понятности. Это позволяет обучающимся быстро освоить систему и с комфортом выполнять различные задания. Также симулятор предоставляет подробную обратную связь по результатам выполнения упражнений, что помогает пользователю улучшать свои навыки и достигать лучших результатов.

Тестирование симулятора показало его высокую эффективность в процессе обучения. Основные преимущества включают:

- Безопасность – возможность отрабатывать маневры и техники работы без риска повреждения
- Экономичность – исключает необходимость использования дорогого оборудования для обучения
- Высокая мотивация обучающихся – обучение становится более интересным и доступным.

Таким образом, 3D-симулятор экскаватора позволяет значительно повысить качество подготовки специалистов, обеспечить их безопасность и снизить затраты на обучение, а также создать условия для более гибкого и интерактивного подхода в обучении.

УДК 004.056.55

Студ. Д.И. Пупко
Науч. рук. ассист. Д. В. Сазонова
(кафедра информационных систем и технологий, БГТУ)

АНАЛИЗ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИИ ПРИ АТАКАХ НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Современные информационные системы всё чаще становятся объектами атак, в которых злоумышленники применяют передовые технологии искусственного интеллекта (ИИ). Использование ИИ в кибератаках позволяет значительно повысить их эффективность, автоматизировать процессы взлома, сократить время на подготовку атак и обойти традиционные системы защиты.

В данной работе рассматриваются основные методы применения ИИ в атаках на информационные системы, а также возможные способы противодействия.

ИИ может значительно ускорить процесс взлома паролей с помощью нейросетей. Такие системы анализируют распространённые шаблоны, предсказывают вероятные пароли пользователей и адаптируются к механизмам защиты, таким как задержки при вводе пароля и системы CAPTCHA. Некоторые продвинутые модели даже способны подбирать пароли на основе анализа публичных данных о человеке, включая его профили в социальных сетях.

Алгоритмы машинного обучения анализируют поведение жертв, адаптируя сообщения так, чтобы они выглядели максимально достоверно. Чат-боты на основе ИИ могут вести переписку с жертвами, убеждая их раскрыть конфиденциальные данные, технологии deepfake позволяют подделывать голоса и даже видеоизображения, создавая иллюзию общения с реальными людьми, такими как коллеги или руководители. Это делает фишинг ещё более опасным, поскольку пользователи склонны доверять знакомым лицам и голосам.

Современные модели распознавания изображений, основанные на глубоких нейросетях, могут обходить традиционные системы CAPTCHA, что позволяет автоматизировать регистрацию фальшивых аккаунтов и выполнение вредоносных действий на сайтах. Более того, злоумышленники используют генеративные состязательные сети (GAN) для создания искусственных изображений и текстов, которые могут обходить даже сложные CAPTCHA, использующие поведенческий анализ или аудиофайлы. Новые методы атаки также включают использование ботов, имитирующих поведение реального пользователя, например, плавные движения мыши и задержки между нажатиями клавиш, что затрудняет их обнаружение системами защиты.

Злоумышленники могут применять методы атак на модели машинного обучения, включая внесение искажений в обучающие выборки (data poisoning) или создание противодействующих примеров (adversarial attacks), позволяющих обманывать системы распознавания лиц, текстов или вредоносного кода. Атаки типа data poisoning позволяют встраивать вредоносные данные в обучающие выборки, что приводит к неправильным решениям моделей. Это особенно опасно в системах, где ИИ используется для принятия критически важных решений, например, в финансовых или медицинских приложениях. Противодействующие примеры, создаваемые с помощью нейросетей, позволяют злоумышленникам заставить модель классифицировать объект

ошибочно, что может применяться для обхода систем биометрической аутентификации или обнаружения вредоносных программ.

ИИ может анализировать исходный код программ и сетевые протоколы, выявляя слабые места быстрее, чем это делают традиционные инструменты сканирования. Генеративные модели способны находить новые типы уязвимостей, которые ранее не были документированы. Например, алгоритмы машинного обучения могут обнаруживать логические ошибки в программном коде, предсказывать потенциальные точки входа для атак и даже генерировать эксплойты для использования обнаруженных уязвимостей.

Для защиты от атак, использующих искусственный интеллект, требуется комплексный подход:

– Развитие ИИ-систем для кибербезопасности. Использование машинного обучения для выявления подозрительной активности, анализа сетевого трафика и прогнозирования угроз.

– Многофакторная аутентификация. Введение биометрических и поведенческих факторов защиты снижает вероятность успешного взлома пароля.

– Обучение пользователей. Повышение цифровой грамотности помогает снижать риски успешных фишинговых атак.

– Совершенствование CAPTCHA. Внедрение динамических методов аутентификации и анализ поведения пользователя.

– Защита моделей машинного обучения. Разработка устойчивых архитектур, защита обучающих данных и применение методов детекции противодействующих атак.

Важно развивать передовые системы безопасности, повышать осведомлённость пользователей и применять комплексные стратегии защиты, чтобы минимизировать риски атак, использующих искусственный интеллект.

УДК 004.056.55

Студ. А.А. Бестемяникова
Науч. рук. ассист. Д. В. Сазонова
(кафедра информационных систем и технологий, БГТУ)

АНАЛИЗ ШИФРОВ, ИСПОЛЬЗУЕМЫХ В ЛИТЕРАТУРНЫХ ПРОИЗВЕДЕНИЯХ

Криптография играет важную роль в обеспечении конфиденциальности и целостности информации. В художественной литературе шифры используются как элемент сюжета, средство кодирования тайных посланий и способ демонстрации ума персонажей. Рассмотрены не