УДК 004.852

РАЗРАБОТКА МОДЕЛИ ПРОГНОЗИРОВАНИЯ УРОВНЯ КРИТИЧНОСТИ ДЛЯ НОВЫХ УЯЗВИМОСТЕЙ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Грузиленков М.Д.[1], Исаев Н.Э.[1], Менисов А.Б.[1]
Научный руководитель – кандидат технических наук Менисов А.Б.[1],
оенно-космическая академия имени А.Ф. Можайского
e-mail: vka@mil.ru

Введение. Современные информационные системы сталкиваются с постоянным ростом числа уязвимостей. Процесс их оценки, основанный на стандартах, таких как Common System (CVSS), требует значительных временных и человеческих ресурсов. Это затрудняет своевременное принятие мер по устранению угроз. Использование методов машинного обучения, в частности трансформеров, позволяет автоматизировать и ускорить процесс оценки критичности уязвимостей. В рамках исследования был проведен анализ отечественного и зарубежного опыта, а также выявлены ключевые проблемы, связанные с текущими подходами к оцениванию уязвимостей.

Основная часть. Предлагаемое решение направлено на автоматизацию и ускорение оценки критичности новых уязвимостей с использованием методов машинного обучения. Проблема текущих подходов заключается в их зависимости как от человеческого ресурса, так и значительных временных затратах при анализе уязвимостей, что создает риски несвоевременной реакции на угрозы [1].

Для решения этих задач была разработана модель, основанная на архитектуре трансформера, которая способна эффективно работать с текстовыми данными и учитывать контекст описаний уязвимостей. Модель обучается на реальных данных из открытых источников, таких как Национальная база уязвимостей (NVD), включающих описание уже оцененных уязвимостей, их уровни критичности и числовые метрики. За основу была взята предобученная модель, которая была донастроена на указанном наборе данных объемом более 80 000 записей. Это позволило улучшить точность предсказаний для задач анализа описаний уязвимостей в области информационной безопасности. После обучения модели был проведен сравнительный анализ, в котором мы сопоставили ее с рекуррентными и сверточными нейронными сетями (RNN/CNN). Полученные значения стандартной метрики машинного обучения, такой как точность предсказания (Accuracy : 96,7%) показывает, что модель превосходит сверточные и реккурентные нейронные сети, точность которых (в равных условиях/параметрах обучения) достигает лишь 92%.

Основные преимущества предлагаемой модели:

1) Скорость и точность оценки: Модель автоматически анализирует текстовые описания уязвимостей и определяет их критичность, что позволяет минимизировать участие человека и сократить временные затраты.

2) Использование механизма внимания: Это улучшает понимание контекста и зависимостей между словами в описаниях уязвимостей, повышая точность прогнозирования [2].

3) Гибкость и масштабируемость: Модель легко адаптируется для работы с новыми типами уязвимостей, а также включает в себя работу с русскоязычным описанием.

4) Автоматизация процессов: Интеграция с базами данных позволяет автоматически собирать новые данные об уязвимостях и прогнозировать их критичность без необходимости дополнительной ручной обработки [3].

Новизна метода заключается в применении трансформеров для анализа описаний уязвимостей в области информационной безопасности, что является перспективным направлением исследований. Если говорить о перспективах развития, то можно использовать модель для предсказания не только уровня критичности уязвимостей,

но и возможных путей решения, что расширит функциональность разработки.

Выводы. Разработанная модель на основе трансформеров обеспечивает автоматизацию и повышение оперативности процесса оценки критичности новых уязвимостей. Это позволяет сократить временные затраты, повысить точность прогнозирования и минимизировать зависимость от человеческого ресурса

Список использованных источников:

1. Когай И. Е. и др. Архитектура трансформер для глубоких нейронных сетей //Цифровизация экономики: направления, методы, инструменты. – 2023. – С. 245-247.
2. Бусько Н. А., Федорченко Е. В., Котенко И. В. Автоматическое оценивание эксплойтов на основе методов глубокого обучения //Онтология проектирования. – 2024. – Т. 14. – №. 3 (53). – С. 408-420.
3. Васильев В. И., Вульфин А. М., Кучкарова Н. В. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров //Вопросы кибербезопасности. – 2022. – №. 2 (48). – С. 27-38.