УДК 004.056.53

РАЗРАБОТКА МЕТОДА ГЕНЕРАЦИИ СЦЕНАРИЕВ КИБЕРАТАК НА ОСНОВЕ РЕСУРСНЫХ ЗАВИСИМОСТЕЙ

Кораблев В.И. (ИТМО)
Научный руководитель – кандидат физико-математических наук, доцент Комаров И.И. (ИТМО)

Введение. Переход кибератак от разрозненных событий к комплексным, многоэтапным сценариям создает качественно новый уровень вызовов для систем информационной безопасности. Реактивная парадигма, основанная на обнаружении и нейтрализации уже реализованных инцидентов, демонстрирует свою недостаточность, так как обнаружение часто происходит на поздних стадиях, когда злоумышленник уже достиг тактической цели и нанес ущерб. В отличие от данного подхода, проактивная безопасность направлена на предотвращение угроз, а не на реагирование на них. Не дожидаясь, пока что-нибудь случится, система проактивной безопасности выявляет, прогнозирует и предотвращает кибератаки еще до проникновения злоумышленников в системы организации [1].

Однако реализация проактивной защиты требует не просто смены парадигмы, а конкретных инструментов, позволяющих предвидеть возможные действия нарушителя. Необходимо формализованное представление о том, какими путями злоумышленник может достичь своей цели в заданной инфраструктуре. Одним из способов такого представления являются деревья атак, в которых этапы сценария атаки расписываются в виде древовидной структуры, где корневая вершина представляет собой цель атаки, а листья дерева - способы ее достижения [2].

Тем не менее, существующие подходы к построению деревьев атак либо требуют ручного труда эксперта, либо оперируют отдельными техниками без учета их взаимосвязей, что обуславливает актуальность разработки метода автоматической генерации сценариев кибератак на основе ресурсных зависимостей, позволяющего формально и исчерпывающе связывать разрозненные техники в целостные деревья атак без участия эксперта.

Основная часть. Предлагаемый метод генерации сценариев кибератак основан на формализации ресурсных зависимостей между техниками MITRE ATT&CK. Ключевая идея заключается в том, что выполнение некоторой техники становится возможным тогда и только тогда, когда все ресурсы, необходимые для ее реализации, имеются в распоряжении злоумышленника на текущем шаге. Данные ресурсы могут быть получены как в результате выполнения одной предшествующей техники, так и скомпонованы из результатов нескольких различных техник, выполненных ранее.

Для практической реализации метода разработана процедура автоматической разметки техник векторами ресурсных зависимостей. Поскольку исходные базы MITRE ATT&CK не содержат явного описания того, какие ресурсы требуются для выполнения техники и какие ресурсы приобретаются в результате, данная задача решена с применением больших языковых моделей. Модуль анализа на основе LLM для каждой техники на основе ее текстового описания определяет:

- какие ресурсы необходимы для ее реализации;
- какие ресурсы приобретаются злоумышленником в результате ее выполнения;
- является ли данная техника возможной точкой входа (началом атаки);
- является ли данная техника конечной целью (терминальной вершиной).

На выходе данного этапа каждая техника оказывается размеченной вектором ресурсных зависимостей, что позволяет передать их в модуль композиции сценариев, где автоматическое построение деревьев атак реализовано в виде двухфазного алгоритма, где на первом этапе формируется дерево возможных комбинаций техник на основе правил достижимости ресурсов, при этом модуль отслеживает платформенную совместимость техник и предотвращает зацикливание, исключая циклические зависимости. На втором этапе для

каждой целевой вершины вычисляется декартово произведение множеств достижимых путей, что позволяет обеспечить полноту покрытия всех вариантов развития атаки. Дополнительно реализован механизм минимизации провайдеров ресурсов, исключающий избыточные комбинации и сокращающий итоговое пространство сценариев без потери полноты.

Каждое дерево представляет собой полный граф переходов от начальных состояний (векторов входа) к целевой вершине, заданной оператором. Заключительным этапом работы системы является визуализация сгенерированных деревьев атак, обеспечивающая наглядное представление всех возможных путей реализации угрозы для дальнейшего анализа специалистом.

Выводы. В результате выполненной работы предложен метод автоматической генерации сценариев кибератак на основе ресурсных зависимостей и разработан прототип системы, реализующая данный метод посредством LLM-разметки техник MITRE ATT&CK по потребляемым и порождаемым ресурсам, а также двухфазного алгоритма композиции, обеспечивающего построение полных деревьев атак с учетом платформенной совместимости, исключения циклов и минимизации провайдеров ресурсов. Экспериментальная апробация подтвердила работоспособность предложенного метода: построенные деревья атак корректно отражают множественные зависимости между техниками и обеспечивают исчерпывающий перебор всех возможных траекторий достижения корневой вершины.

Список использованных источников:

1. Что такое проактивная безопасность? - [Электронный ресурс] // www.trendmicro.com: [сайт]. - Режим доступа: URL: https://www.trendmicro.com/ru_ru/what-is/proactive-security.html (Дата обращения: 11.02.2026).

2. Методы моделирования атак на графах - [Электронный ресурс] // habr.com: [сайт]. - Режим доступа: URL: https://habr.com/ru/companies/pt/articles/861072/ (Дата обращения: 12.02.2026).