DOI 10.36622/1682-7813.2025.28.1.005
УДК 349:004.056

МЕТОДИКИ И АЛГОРИТМЫ РИСК-АНАЛИЗА СЦЕНАРИЕВ РЕАЛИЗАЦИИ АТАК

Г.А. Остапенко, А.П. Васильченко, А.А. Остапенко, В.И. Белоножкин, П.Д. Федоров

В статье рассматривается проблема моделирования кибератак и предлагается новый подход, основанный на интеграции классификации MITRE ATT&CK с вероятностными микромоделями эксплуатации уязвимостей. Основная идея заключается в том, что для каждой тактики из MITRE ATT&CK можно создать микромодель, которая будет учитывать вероятности успешной эксплуатации уязвимостей, связанных с конкретными техниками. Данная методика позволяет формировать сценарии комплексных атак, анализируя взаимосвязи между базами данных MITRE ATT&CK, CAPEC, CWE и CVE. В статье подробно описываются этапы поиска соответствий между техниками атак и уязвимостями, а также алгоритмы для оценки рисков и ущерба от реализации различных сценариев атак. Кроме того, рассматривается программная реализация предложенной методики, которая включает в себя автоматизацию риск-анализа кибератак и оценку вероятностей и ущербов. Результаты исследования направлены на улучшение понимания динамики кибератак и на разработку более эффективных мер по защите информационных систем.

Ключевые слова: кибератака, моделирование, уязвимости, микромодели, риск-анализ.

Введение

Проблема моделирования кибератак [1] может получить новый импульс в своем разрешении при переводе проектной деятельности в пространство классификаций MITRE ATT&CK. Суть состоит в том, что для каждой тактики этой классификации можно построить вероятностную микромодель эксплуатации уязвимостей, используемых рассматриваемой тактикой, с оцифровкой данных с помощью многообразия риск-калькуляторов [2-5]. Стыковка таких микромоделей (по переходам смены тактик) позволит описать траекторию (сценарий) комплексной атаки на защищаемый объект и оценить ожидания успеха ее реализации через вероятности единичной эксплуатации уязвимостей каждой техникой в отдельности. К примеру, для описания наиболее правдоподобного случая достаточно в микромоделях задать наиболее ожидаемые в использовании уязвимости каждой техники (в цепочке применяемых тактик кибер-вторжения).

Формирование сценария реализации атаки

Одним из подходов к решению задачи формирования сценария реализации атаки является использование взаимосвязей между базами данных (БД) MITRE ATT&CK, CAPEC, CWE и CVE [1,6-9], каждая из которых содержит определенный набор данных о тактиках и техниках атак, а также о конкретных уязвимостях в программном обеспечении (ПО).

Методика поиска соответствий начинается с извлечения данных из БД MITRE ATT&CK, в которой каждая техника имеет уникальный идентификатор и сопутствующие метаданные, включающие описание, примеры использования и связанные уязвимости. Далее для каждой техники из MITRE осуществляется поиск соответствующих записей в базе CAPEC, которая классифицирует атаки и методы их реализации. Это позволяет установить связь между конкретными техниками и способами их применения.

Следующим шагом является сопоставление полученных данных с БД CWE, которая содержит информацию о типах уязвимостей (включая уникальный идентификатор и описание), что позволяет более глубоко понять, какие из них могут быть использованы в рамках определенной техники атаки. Важно отметить, что связи между CAPEC и CWE могут быть не всегда прямыми, и в некоторых случаях может

потребоваться дополнительный анализ для установления соответствий.

После того как установлены связи между MITRE, CAPEC и CWE, можно перейти к базе CVE, которая содержит записи о конкретных уязвимостях ПО (уникальный идентификатор, описание уязвимости, а также информация о программных продуктах, в которых она присутствует). На этом этапе методика позволяет сопоставить техники MITRE с конкретными уязвимостями CVE, что является ключевым моментом для оценки рисков и разработки мер по защите.

Таким образом, методика поиска соответствий между техниками MITRE и уязвимостями CVE основывается на многоуровневом анализе взаимосвязей между различными БД. Полученные связи делают возможным установление взаимно однозначного соответствия между любыми рассмотренными элементами (рис. 1).

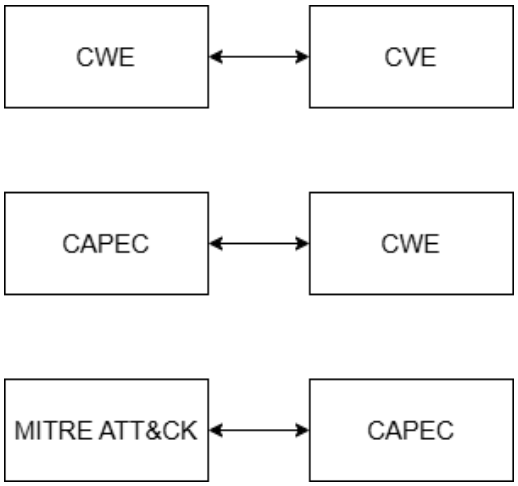

Рис. 1. Связи между базами данных

Для поиска соответствия техники MITRE и уязвимостями CVE последовательность операций будет следующая:

– по заданной уязвимости (CVE) выбираются программные ошибки (CWE);

– каждый элемент CWE позволяет установить получить шаблон атаки CAPEC;

– по полученному шаблону атаки CAPEC из базы данных MITRE становится возможным получить использующиеся техники.

Автоматизация описанной методики должна значительно ускорить и упростить анализ угроз и уязвимостей, а также повысить точность и полноту получаемых результатов.

Расчет вероятностей и ущербов для техник сценариев атак

Риск-анализ комплексных атак предполагает детальный анализ техник и векторов атак, а также возможных уязвимостей. Для оценки вероятности ущербов и выработки мер по минимизации рисков была выработана методика моделирования атак с использованием микромоделей техник, которая комбинирует графовые модели с вероятностным анализом и обеспечивает структурированный метод оценки рисков, связанный с эксплуатацией уязвимостей.

Микромодель техники представляет собой граф из уязвимостей, состоящий из вероятностей успеха и ущерба соответствующих единичных атак. Микромодель для m уязвимостей представлена на рис. 2.

При рассмотрении микромодели техники интерес представляют наиболее ожидаемые в эксплуатации уязвимости. Наиболее ожидаемую уязвимость можно определить как уязвимость с максимальным значением вероятности соответствующей единичной атаки:

$$P_{max} = ma\,x\{p_1, p_2, \dots, p_m\},$$

где: u_i – единичный ущерб при эксплуатации i-й уязвимости.

При этом ущерб определяется, как: $U = u_i$.

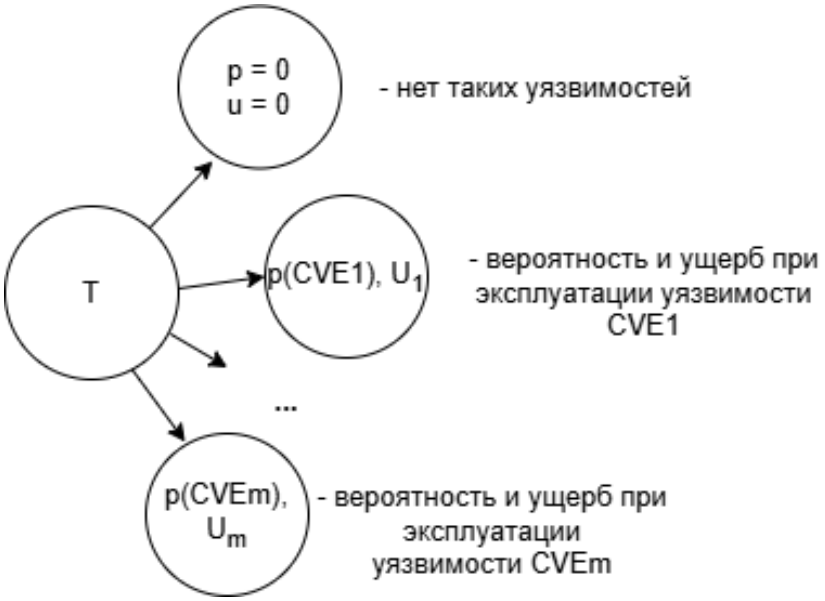

Рис. 2. Микромодель техники

Исходными данными выступают наборы техник в различных сочетаниях.

На основе микромоделей полученных техник строится граф, учитывающий альтернативы эксплуатации разных уязвимостей (рис. 3).

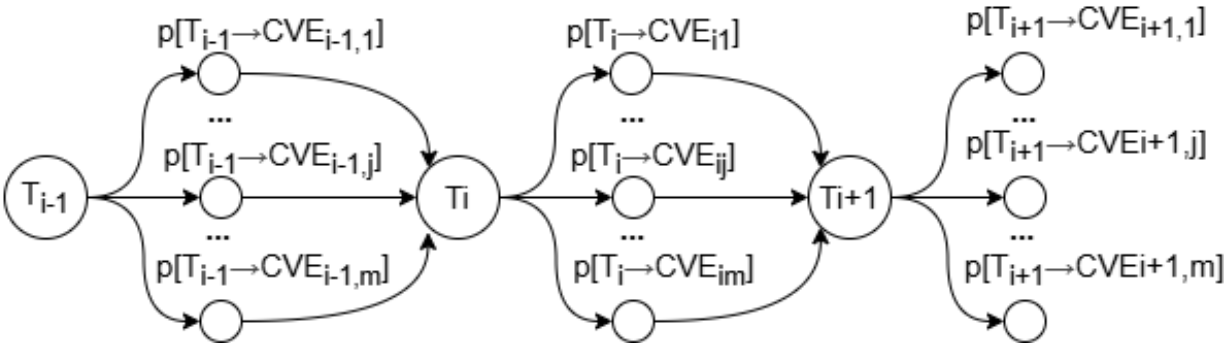

Рис. 3. Графовая микромодель реализации техник атаки

Для вычисления ущербов от реализации техник строится модель оценки ущерба (рис. 4), в которой:

$U[T_i \to CVE_j]$ - ущерб, наносимый атакуемой системе в результате эксплуатации уязвимости CVE_j в ходе реализации техники T_i. $\overline{U} = \frac{U}{C}$ – ущерб, наносимый системе, нормированный по ценности С её ресурса.

В этом случае общий ущерб вычисляется по формуле:

$$\overline{U_\Sigma} = \sum_i \sum_j U[T_i \to CVE_j].$$

Значение общего ущерба определяется как сумма значений ущербов, возникающих в результате эксплуатации всевозможных уязвимостей посредством реализации каждой техники атаки по ходу рассматриваемого сценария атаки.

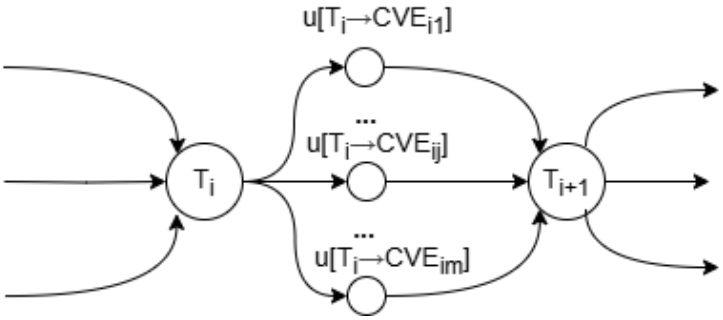

Рис. 4. Модель оценки ущерба

В контексте реализации тактик, можно представить полученные микромодели в виде последовательности тактик реализации атак (рис. 5). Выборка варианта реализации тактики возможна по нескольким критериям, таким, как:

– максимум вероятности (наиболее ожидаемый вариант);

– наибольший ущерб.

В результате получается величина риска, возникающего при реализации избранного сценария атаки, нормированная по ценности защищаемого ресурса:

$$\overline{Risk} = \prod_i p_i \times \sum_j \overline{U_j}\,. \qquad (1)$$

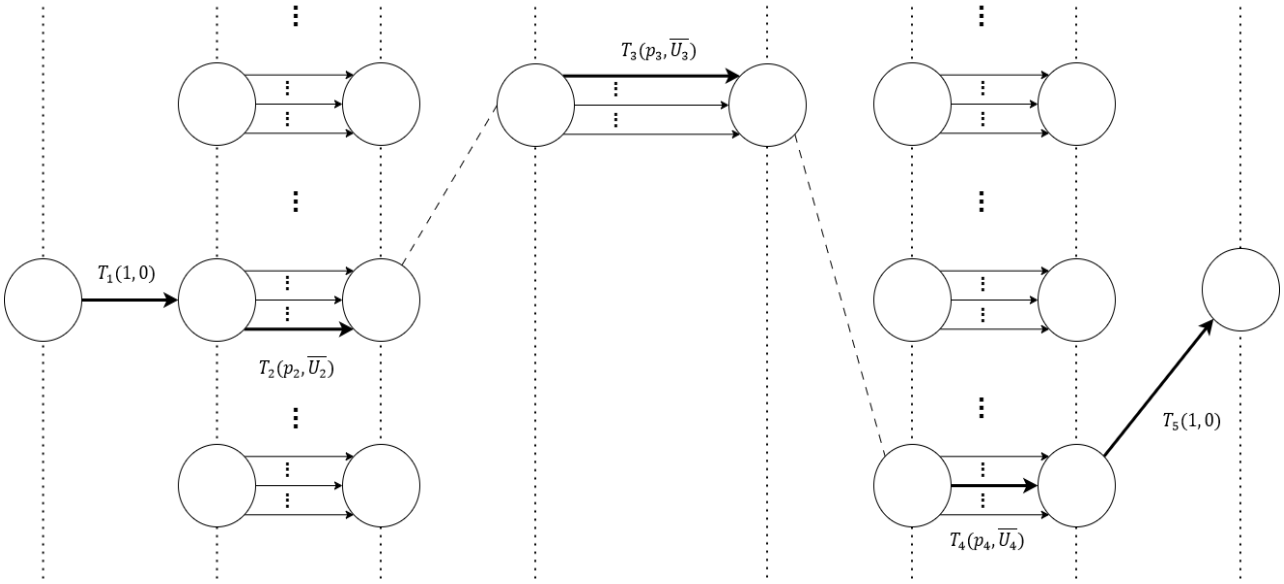

Рис. 5. Риск-модель реализации сценария атаки

Комплексная атака зачастую представляет собой сценарий, который включает последовательную реализацию нескольких техник, использующих различные векторы, что позволяет злоумышленникам эффективно обходить системы безопасности, комбинируя различные методы атаки для достижения своих целей.

Первым шагом в проведении риск-анализа такой атаки является анализ каждого вектора и составление списка микромоделей, соответствующих этим техникам. Векторы атаки могут включать в себя такие элементы, как фишинг, эксплуатация уязвимостей в программном обеспечении, атаки на сеть и другие. Каждая техника имеет свои особенности и способы реализации, которые необходимо учитывать при построении графа переходов. Микромодели представляют собой детализированные описания каждой техники атаки, включая условия успешного

выполнения техники, необходимые ресурсы и инструменты, а также возможные пути обхода систем защиты. Эти микромодели помогают понять, как различные техники могут взаимодействовать друг с другом и какие переходы между ними возможны. На основе анализа микромоделей строится граф с возможными прямыми переходами между техниками (рис. 6).

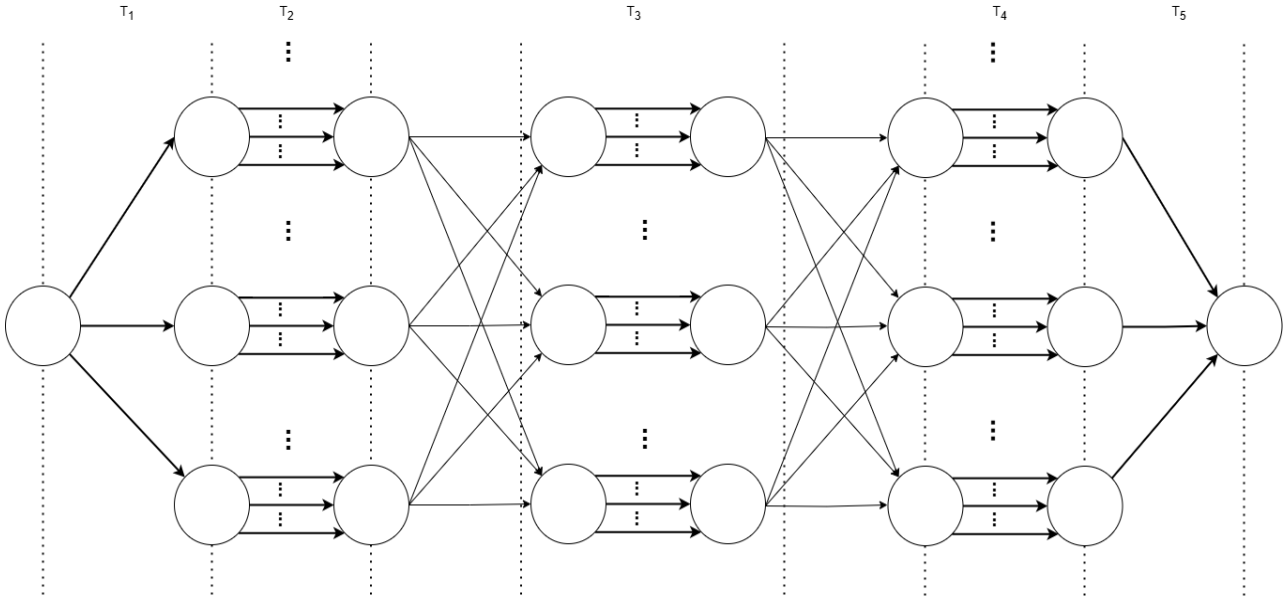

Рис. 6. Граф с переходами между техниками

Этот граф иллюстрирует связи между различными техниками, показывает, как одна техника может привести к другой, позволяет визуализировать все возможные сценарии атак и оценить их взаимосвязи

Вероятность реализации атаки на произвольном пути определяется следующей формулой:

$$P_\Sigma = \prod_j p_j,$$

где P_Σ – вероятность успешности комплексной атаки;

p_j - вероятность успешной реализации техники.

Эта формула позволяет оценить общую вероятность успешного завершения всей последовательности атакующих действий. Зная вероятности отдельных техник, можно оценить, насколько высока вероятность успешной атаки в целом. Ущерб, причиняемый комплексной атакой, определяется как сумма ущербов всех последовательных техник.

Ущерб определяется как сумма ущербов всех последовательных техник и определяется по формуле:

$$\overline{U_\Sigma} = \sum_i U_i,$$

где $\overline{U_\Sigma}$ – нормированный по ценности защищаемого ресурса ущерб от комплексной атаки;

U_i – ущерб при успешной реализации техники.

Риск, возникающий при реализации сценария комплексной атаки, нормированный по ценности защищаемого ресурса, определяется формулой (1), которая объединяет вероятность и ущерб, позволяя получить общее представление о рисках, связанных с атакой.

При анализе графа необходимо также рассмотреть сценарии с наибольшим ущербом и наибольшей вероятностью.

Наибольший ущерб определяется как сумма максимальных значений единичных ущербов.

В этом случае, наибольший ущерб определяется по формуле:

$$\overline{U_{max}} = \sum_j U_j, j: U_j = maxU_i, \qquad i = 1 \dots$$

где U_j – ущерб, возникающий при реализации техники с наибольшим ущербом;

$\overline{U_{max}}$ – наибольший ущерб от комплексной атаки, нормированный по ценности защищаемого ресурса;

Наибольшая вероятность определяется по формуле:

$$P_{max} = \prod_j p_j, j: p_j = maxp_i, \qquad i = 1 \dots n,$$

где p_j– вероятность реализации техники наиболее вероятной техники; P_{max} – вероятность успешности комплексной атаки.

Программная реализация методики

Созданная для реализации разработанной методики программа на первом шаге ищет соответствия техника-уязвимость на основе переданного шаблона CAPEC. Пример нахождения таких соответствий показан на рис. 7. Для дальнейшего расчета оценок критичности полученных уязвимостей создается соответствующая БД под управлением Postgresql. Программа получает из БД информацию об оценках каждого калькулятора (CVSS, EPSS, OWASP), производит расчет и генерирует csv-файл, пример которого показан на рис. 8.

Последним шагом является расчет вероятностей и ущерба для полученных уязвимостей. Для этого программа запрашивает в БД параметры для расчета ущерба, а вероятность вычисляется по полученным ранее оценкам критичности. В результате получается файл, каждая строка которого описывает микромодель техники (рис. 9).

Для расчета вероятностей и ущербов комплексных атак разработан соответствующий программный модуль, работа которого включает три основных этапа – парсинг данных, построение графа и вычисление максимального пути, который соответствует наибольшим вероятности и ущербу.

```
T1036.001; CVE-2018-8414, CVE-2009-0927,CVE-2023-22952
T1553.002; CVE-2018-8414, CVE-2009-0927,CVE-2023-22952
T1562.003; CVE-2018-8414, CVE-2020-0646, CVE-2009-0927,CVE-2021-22205, CVE-2023-22952
T1574.006; CVE-2018-8414, CVE-2020-0646, CVE-2009-0927,CVE-2021-22205, CVE-2023-22952
T1574.007; CVE-2018-8414, CVE-2020-0646, CVE-2009-0927,CVE-2021-22205, CVE-2023-22952
T1036; CVE-2018-20250
T1134; CVE-2018-20250, CVE-2020-0938, CVE-2021-22205
T1134.001; CVE-2018-20250, CVE-2020-0938, CVE-2021-22205
T1134.002; CVE-2018-20250, CVE-2020-0938, CVE-2021-22205
T1134.003; CVE-2018-20250, CVE-2020-0938, CVE-2021-22205
T1550.004; CVE-2018-20250, CVE-2020-0938, CVE-2021-22205
T1574.002; CVE-2018-20250
T1574.008; CVE-2018-20250
T1027; CVE-2020-0646, CVE-2009-0927, CVE-2021-22205, CVE-2023-22952
T1027.006; CVE-2021-22205
T1027.009; CVE-2021-22205
T1564.009; CVE-2021-22205
T1211; CVE-2023-38831
T1542.002; CVE-2023-38831
```

Рис. 7. Пример установления соответствия между вектором атаки и техниками- уязвимостями

```
Уязвимость, Критичность_уязвимости
CVE-2018-8414,0.80628
CVE-2018-20250,0.83796
CVE-2020-0646,0.89486
CVE-2020-0938,0.803
CVE-2021-1647,0.7656
CVE-2010-2568,0.748
CVE-2009-0927,0.8585
CVE-2021-22205,0.7261
CVE-2023-36884,0.6607
CVE-2023-38831,0.6561
CVE-2023-22952,0.7871
```

Рис. 8. Фрагмент файла с расчетом критичности уязвимостей

```
Техника;Уязвимость:Вероятность:Ущерб
T1134.001;CVE-2021-22205:0.307:0.5,CVE-2020-0938:0.339:0.5,CVE-2018-20250:0.354:0.5
T1134.002;CVE-2021-22205:0.307:0.5,CVE-2020-0938:0.339:0.5,CVE-2018-20250:0.354:0.5
T1134.003;CVE-2021-22205:0.307:0.5,CVE-2020-0938:0.339:0.5,CVE-2018-20250:0.354:0.5
T1528;CVE-2021-22205:0.307:0.5,CVE-2020-0938:0.339:0.5,CVE-2018-20250:0.354:0.5
T1606;CVE-2021-22205:0.307:0.5,CVE-2020-0938:0.339:0.5,CVE-2018-20250:0.354:0.5
T1562.003;CVE-2020-0646:0.220:0.2,CVE-2009-0927:0.211:0.5,CVE-2021-22205:0.178:0.5,CVE-2018-8414:0.198:0.2,CVE-2023-22952:0.193:0.2
T1027;CVE-2020-0646:0.274:0.2,CVE-2009-0927:0.263:0.5,CVE-2021-22205:0.222:0.5,CVE-2023-22952:0.241:0.2
T1564.009;CVE-2021-22205:1.000:0.5
T1036.001;CVE-2009-0927:0.350:0.5,CVE-2018-8414:0.329:0.2,CVE-2023-22952:0.321:0.2
T1553.002;CVE-2009-0927:0.350:0.5,CVE-2018-8414:0.329:0.2,CVE-2023-22952:0.321:0.2
T1574.006;CVE-2020-0646:0.220:0.2,CVE-2009-0927:0.211:0.5,CVE-2021-22205:0.178:0.5,CVE-2018-8414:0.198:0.2,CVE-2023-22952:0.193:0.2
T1083;CVE-2023-38831:1.000:0.7
T1574.005;CVE-2023-38831:1.000:0.7
T1040;CVE-2023-38831:1.000:0.7
T1574.008;CVE-2018-20250:1.000:0.5
T1574.007;CVE-2020-0646:0.220:0.2,CVE-2009-0927:0.211:0.5,CVE-2021-22205:0.178:0.5,CVE-2018-8414:0.198:0.2,CVE-2023-22952:0.193:0.2
T1557.002;CVE-2023-38831:1.000:0.7
T1574.002;CVE-2018-20250:1.000:0.5
T1036;CVE-2018-20250:1.000:0.5
T1134;CVE-2021-22205:0.307:0.5,CVE-2020-0938:0.339:0.5,CVE-2018-20250:0.354:0.5
T1211;CVE-2023-38831:1.000:0.7
T1565.002;CVE-2023-38831:1.000:0.7
T1027.006;CVE-2021-22205:1.000:0.5
T1539;CVE-2009-0927:0.214:0.5,CVE-2021-22205:0.181:0.5,CVE-2020-0938:0.200:0.5,CVE-2018-20250:0.209:0.5,CVE-2023-22952:0.196:0.2
T1027.009;CVE-2021-22205:1.000:0.5
T1556;CVE-2023-38831:1.000:0.7
T1611;CVE-2023-38831:1.000:0.7
T1542.002;CVE-2023-38831:1.000:0.7
T1574.010;CVE-2023-38831:1.000:0.7
T1550.004;CVE-2021-22205:0.307:0.5,CVE-2020-0938:0.339:0.5,CVE-2018-20250:0.354:0.5
```

Рис. 9. Фрагмент файла микромоделей техник

На первом этапе загружается информация из структурированного текстового файла с данными о тактиках и связанных техниках.

Каждая строка файла содержит идентификатор техники, вероятность ее реализации и ущерб

Далее создаются объекты, содержащие данные строк, и составляется их список для дальнейшего использования.

На втором этапе программа использует библиотеку NetworkX для построения направленного графа:

– инициализируется пустой граф;

– каждая техника добавляется как вершина графа;

– для каждой пары соседних строк (тактик) создаются ребра между техниками в одной тактике и техниками в следующей;

– вес ребра определяется как величина вероятности и ущерба, связанная с переходом от одной техники к другой.

На третьем этапе выполняется поиск максимального пути в графе:

– происходит перебор всех возможных пар начальных и конечных вершин;

– для каждой пары генерирует все возможные простые пути между ними,

программа ищет последовательности вершин, которые не повторяются;

– для каждого найденного пути вычисляется сумма весов ребер, что соответствует суммарному ущербу либо вероятности (в зависимости от режима работы программы).

По итогу суммы весов всех путей сравниваются и определяется путь с максимальным весом, который соответствует наиболее опасному сценарию.

После нахождения максимального пути программа выводит:

– идентификаторы техник, которые входят в максимальный путь;

– максимальную вероятность и суммарный ущерб, соответствующие этому пути.

Фрагмент входных данных, необходимых для построения графа показан на рис. 10.

```
Persistence;
    T1574.006:0.19796505632433387:0.2
    T1574.005:1.0:0.7
    T1574.008:1.0:0.5
    T1574.007:0.19796505632433387:0.2
    T1574.002:1.0:0.5
    T1556:1.0:0.7
    T1542.002:1.0:0.7
    T1574.010:1.0:0.7
Privilege Escalation;
    T1134.001:0.3540087703733746:0.5
    T1134.002:0.3540087703733746:0.5
    T1134.003:0.3540087703733746:0.5
    T1574.006:0.19796505632433387:0.2
    T1574.005:1.0:0.7
    T1574.008:1.0:0.5
    T1574.007:0.19796505632433387:0.2
    T1574.002:1.0:0.5
    T1134:0.3540087703733746:0.5
    T1611:1.0:0.7
    T1574.010:1.0:0.7
Defense Evasion;
    T1134.001:0.3540087703733746:0.5
    T1134.002:0.3540087703733746:0.5
    T1134.003:0.3540087703733746:0.5
    T1562.003:0.19796505632433387:0.2
    T1027:0.27394567985893414:0.2
    T1564.009:1.0:0.5
    T1036.001:0.32884154200042415:0.2
    T1553.002:0.32884154200042415:0.2
    T1574.006:0.19796505632433387:0.2
    T1574.005:1.0:0.7
    T1574.008:1.0:0.5
    T1574.007:0.19796505632433387:0.2
    T1574.002:1.0:0.5
    T1036:0.32884154200042415:0.2
    T1134:0.3540087703733746:0.5
    T1211:1.0:0.7
    T1027.006:1.0:0.5
Defense Evasion;
    T1134.001:0.3540087703733746:0.5
    T1134.002:0.3540087703733746:0.5
    T1134.003:0.3540087703733746:0.5
    T1562.003:0.19796505632433387:0.2
    T1027:0.27394567985893414:0.2
    T1564.009:1.0:0.5
    T1036.001:0.32884154200042415:0.2
    T1553.002:0.32884154200042415:0.2
    T1574.006:0.19796505632433387:0.2
    T1574.005:1.0:0.7
    T1574.008:1.0:0.5
    T1574.007:0.19796505632433387:0.2
    T1574.002:1.0:0.5
    T1036:0.32884154200042415:0.2
    T1134:0.3540087703733746:0.5
    T1211:1.0:0.7
    T1027.006:1.0:0.5
    T1027.009:1.0:0.5
    T1556:1.0:0.7
    T1542.002:1.0:0.7
    T1574.010:1.0:0.7
    T1550.004:0.3540087703733746:0.5
Credential Access;
    T1528:0.3540087703733746:0.5
    T1606:0.3540087703733746:0.5
    T1040:1.0:0.7
    T1557.002:1.0:0.7
    T1539:0.20882905603764085:0.5
    T1556:1.0:0.7
Discovery;
    T1083:1.0:0.7
    T1040:1.0:0.7
Lateral Movement;
    T1550.004:0.3540087703733746:0.5
Collection;
    T1557.002:1.0:0.7
Impact;
    T1565.002:1.0:0.7
```

Рис. 10. Фрагмент файла входных данных для построения графа

Заключение

В рамках предложенной модели сценарий комплексной атаки представляет собой последовательность микрографов реализации техник из различных используемых тактик. При этом теоретически возможны и циклы когда в ходе атаки одни и те же техники применяются неоднократно. Подобная формализация процесса также удобна для выявления наиболее опасных сценариев и предупреждения действий злоумышленников в отношении защищаемого объекта. Необходимо отметить, что применение предполагаемой схемы моделирования ограничивается лишь теми случаями, когда уязвимости и тактики, используемые злоумышленниками, априори неизвестны администратору безопасности. Во всех остальных проектных ситуациях предлагаемый подход уместен для защиты самых разнообразных киберсистем: нейросети (машинное обучение), беспроводные сети и т.п., где имеются соответствующие матрицы MITRE-ресурса, которые предлагают самую широкую фактуру (тактик, техник, мер реализации и др.). Спектр таких систем довольно широк (от интернета вещей до средств критической информационной инфраструктуры и др.), как и многообразие классов компьютерных атак (инъекция, социальная инженерия и др.), реализуемых в отношении перечисленных объектов.

Методика риск-анализа комплексных атак позволяет глубже понять взаимодействие между различными техниками и оценить риски, связанные с их реализацией, а также более эффективно реагировать на потенциальные угрозы и планировать меры безопасности.

Созданное методическое обеспечение риск-анализа кибератак позволяет систематизировать подходы к оценке рисков, что способствует более эффективному управлению киберугрозами и созданию адаптивных стратегий защиты, основанных на актуальных данных о рисках, тем самым снижая вероятность успешных атак.

Полученные сценарные риск-модели кибератак предоставляют инструменты для анализа и прогнозирования последствий комлексных атак, что позволяет заранее выявлять потенциальные уязвимости и разрабатывать стратегии защиты, повышая уровень готовности к киберугрозам и минимизируя возможные убытки.

Список литературы

1. MITRE ATT&CK. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения 25.01.25).

2. Exploit Prediction Scoring System (EPSS). – URL: https://www.first.org/epss/ (дата обращения 25.01.25).

3. Общая система оценки уязвимостей (CVSS). URL: https://www.first.org/cvss/specificationdocument/ (дата обращения 25.01.25).

4. Common Vulnerability Scoring System v3.1. URL: https://www.first.org/cvss/v3.1/specificationdocument (дата обращения 25.01.25).

5. Common Vulnerability Scoring System v4.0 – URL: https://www.first.org/cvss/v4.0 (дата обращения 25.01.25).

6. OWASP Risk Assessment Calculator. URL: https://javierolmedo.github.io/OWASPCalculator/ (дата обращения 25.01.25).

7. CVE. – URL: https://cve.mitre.org/ (дата обращения 25.01.25).

8. CWE. URL: https://cwe.mitre.org/index.html (дата обращения 25.01.25).

9. CAPEC. URL: https://capec.mitre.org/ (дата обращения 25.01.25).

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 28.01.25

Информация об авторах

Остапенко Григорий Александрович – д-р техн. наук, профессор, Финансовый университет при Правительстве Российской Федерации, e-mail: ost@fa.ru

Васильченко Алексей Павлович – аспирант, Финансовый университет при Правительстве Российской Федерации, e-mail: rainichek@yandex.ru

Остапенко Александр Алексеевич – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

Белоножкин Владимир Иванович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Федоров Павел Денисович – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

METHODS AND ALGORITHMS FOR RISK ANALYSIS OF ATTACK IMPLEMENTATION SCENARIOS

G.A. Ostapenko, A.P. Vasilchenko, A.A. Ostapenko, V.I. Belonozhkin, P.D. Fedorov

The article considers the problem of cyberattack modeling and proposes a new approach based on the integration of the MITRE ATT&CK classification with probabilistic micromodels of vulnerability exploitation. The main idea is that for each MITRE ATT&CK tactic, it is possible to create a micromodel that will take into account the probabilities of successful exploitation of vulnerabilities associated with specific techniques. This methodology allows one to form scenarios of complex attacks by analyzing the relationships between the MITRE ATT&CK, CAPEC, CWE, and CVE databases. The article describes in detail the stages of searching for correspondences between attack techniques and vulnerabilities, as well as algorithms for assessing the risks and damage from the implementation of various attack scenarios. In addition, the software implementation of the proposed methodology is considered, which includes automation of risk analysis of cyber attacks and assessment of probabilities and damages. The results of the study are aimed at improving the understanding of the dynamics of cyber attacks and developing more effective measures to protect information systems.

Keywords: cyber attack, modeling, MITRE ATT&CK, vulnerabilities, micromodels, risk analysis.

Submitted 28.01.25

Information about the authors

Grigory A. Ostapenko – Dr. Sc. (Technical), Professor, Financial University under the Government of the Russian Federation, e-mail: ost@fa.ru

Alexey P. Vasilchenko – graduate student, Financial University under the Government of the Russian Federation, e-mail: rainichek@yandex.ru

Alexander A. Ostapenko – graduate student, Voronezh State Technical University, e-mail: alexostap123@gmail.com

Vladimir I. Belonozhkin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Pavel D. Fedorov – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com