DOI 10.36622/1682-7813.2024.27.4.007
УДК 621.372.004

АКТУАЛЬНЫЕ ЗАДАЧИ И НЕКОТОРЫЕ ИХ РЕШЕНИЯ В ЧАСТИ РИСК-КАЛЬКУЛЯЦИИ УСПЕШНОСТИ РЕАЛИЗАЦИИ ЕДИНИЧНЫХ КИБЕРАТАК

А.А. Остапенко

Рассматривается насущная необходимость расчета параметров успешной эксплуатации уязвимостей со стороны заданных видов единичных атак. Осуществляется соответствующее целеполагание с конкретизацией задач риск-калькуляции, включая обзор известных калькуляторов, создание методического и иного обеспечения риск-анализа единичных кибератак. Предлагаются аналитические конструкции для расчета, использующие опыт эксплуатации калькуляторов опасности уязвимостей. В частности, обозначаются способы сокращения субъективности оценок на основе нормализации и усреднения данных разнообразных риск-калькуляторов для одной и той же уязвимости. Приводятся примеры практических расчетов вероятности единичной эксплуатации различных уязвимостей, используемых при разнообразных видах кибератак.

Ключевые слова: риск-анализ, уязвимость, вероятность, ущерб.

Введение

Предлагаемые ныне [1-7] риск-калькуляторы декларируют возможность численной оценки опасности, критичности, приоритезации и т.п. уязвимостей. Эти показатели созвучны вероятности эксплуатации исследуемой уязвимости и при определенной их обработке могут быть в дальнейшем использованы в этом качестве. Обилие калькуляторов также открывает перспективу снижения субъективности разброса их результатов путем некоторого усреднения значений, полученных для одной и той же уязвимости. В этом случае имеется возможность интеграции опыта разработчиков различных калькуляторов в интересах их пользователей в части вычисления вероятностных параметров единичных кибератак на интересующие уязвимости.

Вышеуказанные соображения позволили сформулировать целую серию задач, ориентированных на конструирование аналитических выражений для расчета вероятностей успеха единичных кибератак путем эксплуатации уязвимостей, критичность которых оценивается с использованием множества известных калькуляторов. Ниже перечисляются поставленные задачи исследования:

1. Мониторинг и анализ результатов создания и эксплуатации известных калькуляторов параметров кибератак и уязвимостей, включая:

- суммаризацию текущих сведений о создании и развитии методов и средств калькуляции параметров кибератак и уязвимостей;
- аккумуляцию и форматирование данных, используемых калькуляторами, с перспективой дальнейшего применения этой оцифровки в автоматизированном режиме калькуляции;
- тестирование рассматриваемых инструментов на реальных примерах проектной деятельности;
- построение таблицы их достоинств и недостатков;
- формирование частных технических заданий для совершенствования рассматриваемого инструментария и разрешения, выявленных в нем противоречий;
- менеджмент и комплексирование процессов реализации сформулированных заданий;
- сравнительная оценка полученных версий обновленного калькулятора в контексте удобства и адекватности выдаваемых им результатов для учебного процесса и проектной деятельности.

©Остапенко А.А., 2024

2. Разработка методического обеспечения для риск-анализа единичных кибератак, включая:

- формирование актуального множества метрик, необходимого и достаточного для практического использования создаваемого калькулятора;

- обоснование областей допустимых значений метрик, необходимых для экспертных оценок, образующих множество исходных данных риск-калькуляции;

- привязка метрического пространства к сущности риск-анализа, т.е. адаптация и предложение метрик с учетом получения на выходе калькулятора пары «ущерб и вероятность его наступления»;

- конструирование аналитических выражений и/или алгоритмов вычисления значений предлагаемых метрик;

- оценка адекватности результатов и удобства пользования для полученных аналитических конструкций в сравнении с аналогами риск-калькуляции.

3. Алгоритмизация и программная реализация предложенных аналитических конструкций в виде перспективных версий калькуляции параметров единичных атак, имея в виду:

- устранение недостатков в удобстве и адекватности риск-анализа пар «атака – уязвимость»;

- реализацию многовариантного расчета отдельных метрик и их интегральной оценки;

- подключение к многовариантному анализу модулей оптимизации параметров единичных атак в контексте управления рисками массированных кибер-вторжений;

- всестороннее тестирование разработанного инструментария автоматизированных оценки и регулирования рисков успешности единичных кибератак;

- отладка и внедрение полученного продукта в учебный процесс и проектную деятельности кафедры.

4. С использованием аппарата теории вероятностей и чувствительности, дальнейшее развитие методологии оценки и регулирования рисков успешности множественных кибератак, включая:

- совершенствование и обоснование подходов к созданию математического обеспечения в части калькуляции рисков множественных кибер-вторжений;

- развитие существующего методического обеспечения анализа массированных атак в части расчета линейки параметров ущерба и вероятности его наступления;

- регламентацию противодействия множественным кибератакам на основе предложенного инструментария риск-анализа;

- выработку рекомендаций и алгоритмов регулирования рисков с использованием теории чувствительности их параметров;

- программную реализацию предложенных алгоритмов оценки и регулирования рисков успешности массированных вторжений, ее тестирование и отладка в интересах внедрения в учебный процесс и проектную деятельности кафедры.

5. Расширение возможностей инструментария риск-калькуляции на ареал комплексных кибервторжений, активно реализуемых ныне хакерскими преступными группировками и спецслужбами недружественных государств.

6. Внедрение нейросетевых технологий в инструментарий автоматизированных оценок и регулирования рисков успешности единичных, множественных и комплексных кибератак.

7. На основе созданного инструментария риск-калькуляции, разработка методологии (и ее нейросетевая реализация) организационно-правовой защиты от массированных кибер-вторжений.

Представленный комплекс задач представляется весьма масштабным, и в настоящей работе будет акцентировано внимание на некоторые решения по первым двум позициям, где речь идет о риск-калькуляции единичных кибератак. Поэтому данную статью уместно считать началом исследований, открываемых в обозначенном направлении. Далее предлагается рассмотреть многообразие калькуляторов, ориентированных на оценку критичности (опасности и т.п.) уязвимостей, эксплуатируемых в ходе реализации кибератак.

Развитие методологии риск-калькуляции

Многочисленные сайты калькуляции параметров уязвимостей [1-7] предлагают пользователям оценки критичности, опасности и приоритетности в точке их устранения в ходе кибер-противоборства. Однако для защиты от атак, эксплуатирующих данные уязвимости, практический и теоретический интерес представляет расчет вероятности реализации таких вторжений. Рассмотрим особенности решения этой **задачи**.

Пусть в системе классификации CAPEC [8] идентифицирована кибератака шаблона i. Тогда представляется возможным (через базу данных CWE) установить множество уязвимостей $\mathrm{CVE}_j, j = 1(1)n$ мощностью n. С использованием одного или нескольких калькуляторов можно рассчитать критичность K_j каждой из установленных уязвимостей. Предполагая, что при атаке может быть проэксплуатирована только одна из рассматриваемых уязвимостей, вероятность успеха такой атаки можно определить в виде:

$$p_i = \frac{K_i}{\sum_{i=1}^{n} K_i}, \quad (1)$$

где для данной каждой группы событий очевидно имеем:

$$\sum_{i=1}^{n} p_i = 1, \quad (2)$$

Фактически гипотеза (1) исходит из того, что всякая уязвимость привлекает внимание злоумышленника и имеет возможность своей эксплуатации им, пропорционально ее критичности, которая учитывает множество особенностей и факторов, присущих именно рассматриваемой уязвимости.

Уместно также заметить, что анализируемое множество уязвимостей способно включать не все элементы базы данных CVE, теоретически подходящие для эксплуатации рассматриваемой CAPEC-атакой. Данное множество может быть ограничено теми из них, которые наличествуют в атакуемой системе.

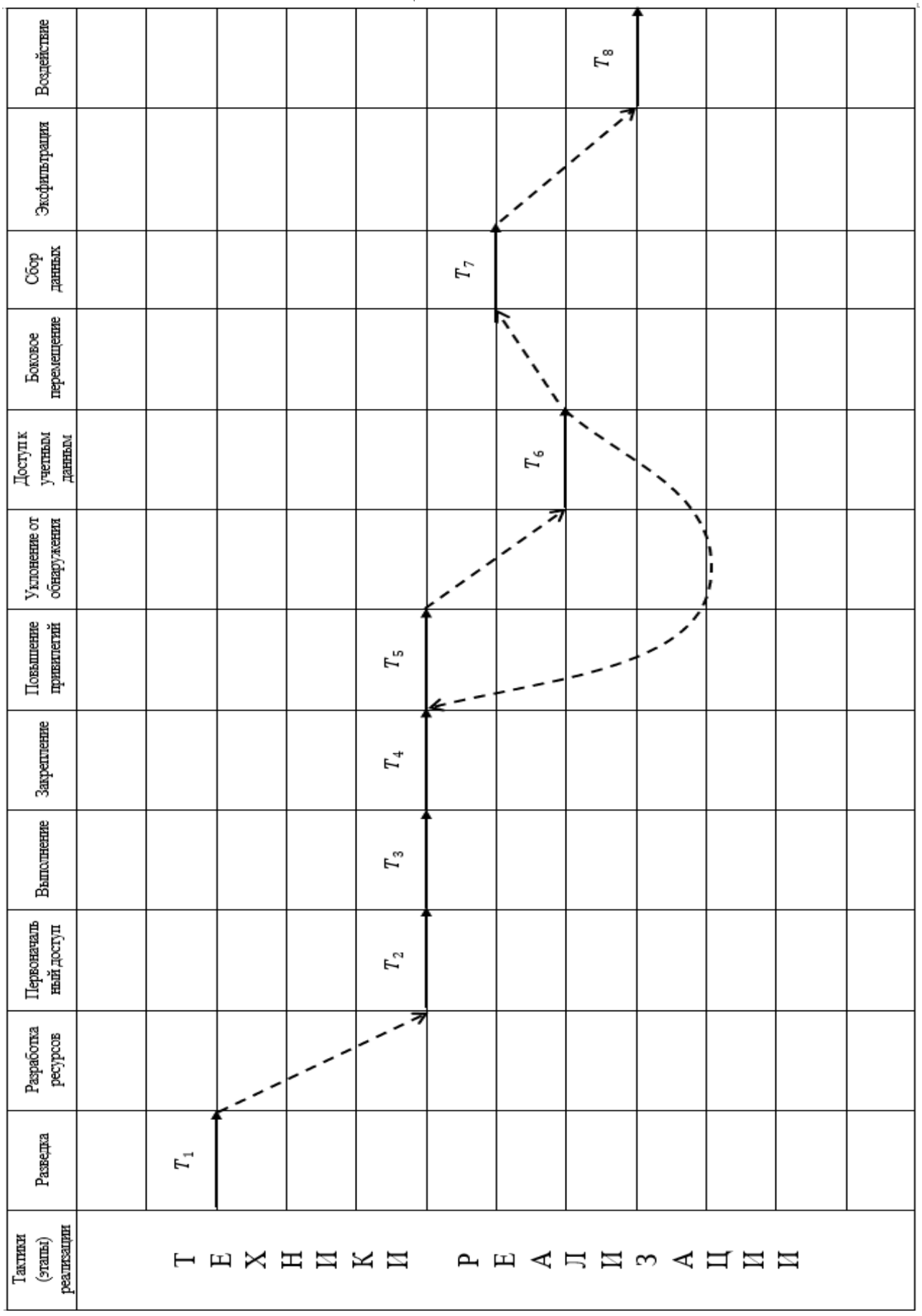
Есть еще один интересный нюанс, который требует своего исследования и моделирования. Разные по своей CAPEC-классификации атаки теоретически могут эксплуатировать одну и туже уязвимость.

Кроме вышеизложенного стоит рассмотреть следующий уровень детализации процесса реализации кибератак. Дело в том, что база данных MITRE ATT&CK [9] предложить разложить сценарии атак на последовательность техник. Такая процедура качественно иллюстрируется в таблицу 1, где по мере реализации определённых (матрицами сайта) тактик (от разведки до воздействия) включаются избранные злоумышленниками техники $T_1 - T_3$. Очевидно, такой сценарий не обязательно должен быть прямоточным. Возможны и циклы, что отражено в примере (табл. 1) на стадии повышения привилегий (пунктирная линия возврата к технике T_s)

Вышеизложенное ставит **задачу** поиска соответствия между элементами множества уязвимостей и совокупностью техник. То есть с уровня CAPEC- классификации потребуется опустить к детализации в пространстве MITRE-техник, поставив последние в соответствие CVE-элементы, эксплуатируемые этими техниками. При этом следует графовая иллюстрация примера сценария CAPEC-атаки в виде последовательности реализации.

Таблица 1

Таблица MITRE-техник



Заметить, что далеко не все техники связаны с уязвимостями (к примеру, T_1 на этапе разведки может не иметь таковых). К тому же, возможны варианты с выбором техник в рамках реализации одной и той же тактики сценария для заданного вида атаки.

Таким образом требуется разработка (и их автоматизация) методик установления соответствия техник и уязвимостей с соответствующей оценкой вероятностей их эксплуатации. Эта задача актуальна не столько для моделирования единичных кибератак, сколько в отношении комплексных и CAPEC-комбинированных вторжений, где, конечно, сценарии (табл. 1) будут куда более масштабными. Такие атаки становятся все более популярными даже в среде организованной преступности, не говоря уже о спецслужбах недружественных государств.

Поэтому поставленная задача приобретает весьма важное значение в современных реалиях.

Если говорить о вероятностных оценках комплексных атак, то они также возможны на основе поиска передаточных функций от входа (разведка) до выхода (воздействие) процесса реализации сценария (табл. 1). Однако для этого нужно построить ранее предложенные (1) микромодели возможной эксплуатации набора уязвимостей, уже соответствующих техникам.

Ещё одной актуальной задачей следует считать оценку величины ущерба, наносимого рассматриваемой атакой. Здесь уместно прибегать к нормированию по ценности защищаемого ресурса. Это позволит абстрагироваться от ненужной для сравнительного анализа конкретики и сделать безразмерными величины ущерба. При этом углубление в специфику эксплуатации уязвимостей даст адекватные оценки ущербности.

Опираясь на изложенные в настоящем разделе соображения, рассмотрим далее более конкретно некоторые актуальные направления практического применения предлагаемого методического подхода.

Направления практического использования предлагаемого методического подхода

В этой связи ниже рассмотрим вопросы формализации противодействия кибератакам с акцентом на автоматизацию этого процесса как в части моделирования вторжения, так и в плане регламентации мер реагирования на них.

Проблема моделирования кибератак [9] может получить новый импульс в своем разрешении при переводе проектной деятельности в пространство классификаций MITRE ATT&CK. Суть вкратце 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 [1-7]. 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 (рис. 1, 2). На рис. 1 обозначено:

T_i – MITRE – техника с идентификационным номером i;

CVE_j – уязвимость с идентификационным номером j из множества уязвимостей, которые может проэксплуатировать нарушитель в ходе реализации техники T_i;

$p[T_i \rightarrow CVE_j]$ – вероятность эксплуатации j-ой уязвимости посредством реализации техники T_i;

$\sum_j p[T_i \rightarrow CVE_j] = 1$ – полная группа событий по множеству эксплуатируемых в ходе реализации T_i уязвимостей;

$\max p[T_i \rightarrow CVE_j]$ – наиболее ожидаемый вариант реализации техники T_i.

На рис. 2 обозначено:

$U[T_i \rightarrow CVE_j]$ – ущерб, наносимый атакуемой системе в результате эксплуатации уязвимости CVE_j в ходе реализации техники T_i;

U = U/C – ущерб, наносимый системе, нормированный по ценности C её ресурса;

$U_{\sum}$ $\sum i \sum j$ U[Ti → CVEj] – общий ущерб, наносимый атакуемой системе, вычисляемый в качестве суммы ущербов, которые могут возникнуть в результате эксплуатации всевозможных уязвимостей посредством реализации каждой техники атаки по ходу рассматриваемого сценария атаки.

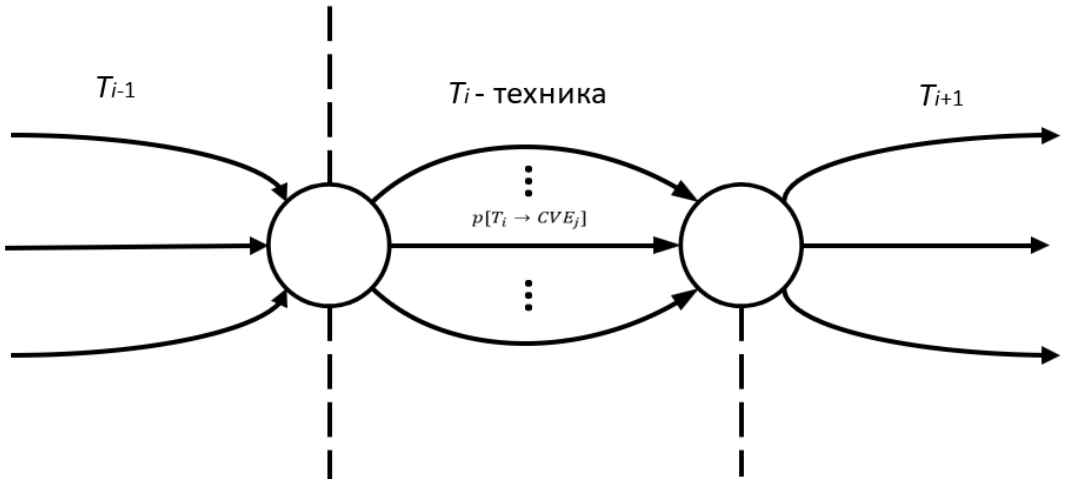


Рис. 1. Графовая микромодель реализации MITRE-техники атаки в альтернативах эксплуатации уязвимостей

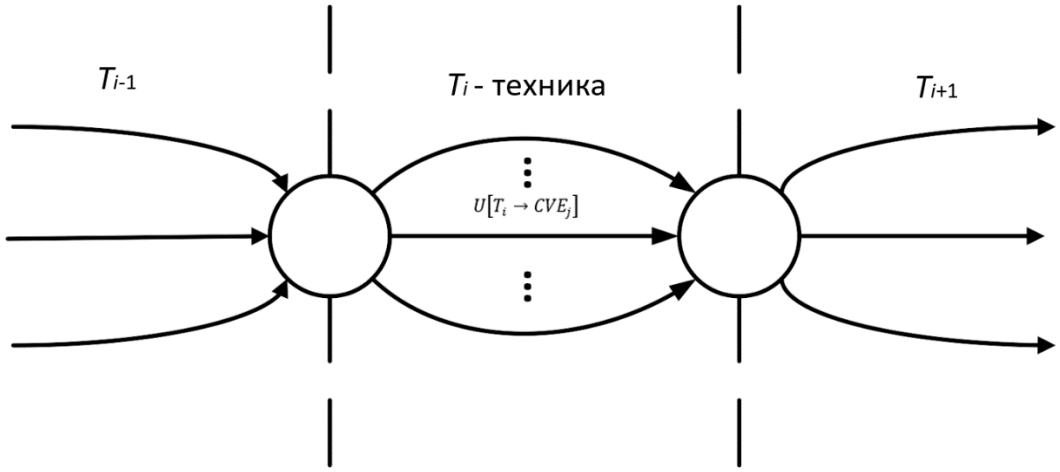


Рис. 2. Модели оценки ущербов атакуемой системы в совокупности реализуемых техник атаки

Для описания наиболее правдоподобного случая достаточно в микромоделях задать наиболее ожидаемые в использовании уязвимости каждой техники в цепочке применяемых тактик кибер-вторжения (рис. 3, 4).

На рис. 3 жирной стрелкой обозначена выборка варианта реализации тактики по необходимому критерию:

- максимума вероятности (наиболее ожидаемый вариант),
- минимум ущерба и т.д.

Risk = $\prod i$ pi × $\sum j$ Uj – нормированный по ценности защищаемого ресурса риск, возникающий при реализации избранного сценария атаки.

На рис. 4 показано развитие риск-модели, представленной на рис. 3.

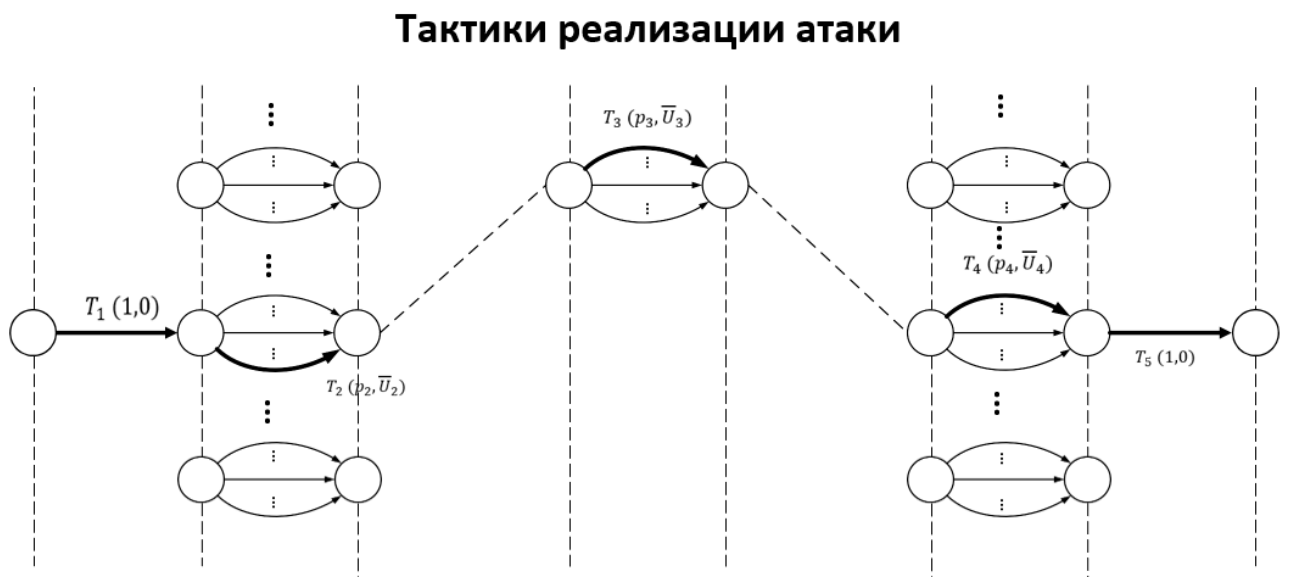


Рис. 3. Риск-модель для примера реализации сценария атаки

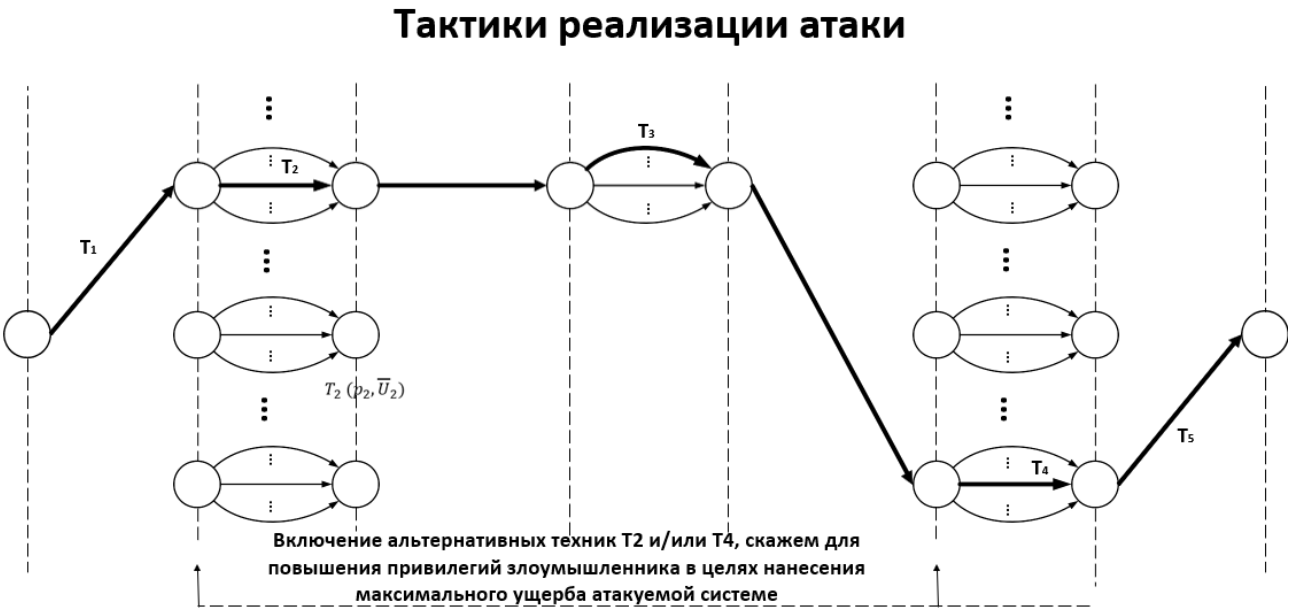


Рис. 4. Развитие риск-модели для примера переключения тактик с использованием обратной связи в сценарии

В рамках предлагаемой 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 (коррекции множества уязвимостей и пр.).

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.) [9].

По прежнему актуальной остается проблем автоматизации регламентов противодействия кибератакам [10]. При этом, ставка только на базу данных CAPEC [8] в решении этой проблемы оказалась неоправданной. Поэтому следует акцент сделать на MITRE ATT&CK [9], обеспечив установленные соответствия техник реализации атак и уязвимостей, эксплуатируемых ими. В случае, когда такую задачу автоматизировано удалось решить, открывается возможность поиска в вышеупомянутых базах данных рекомендаций по идентификации видов атак, реагирования на них, которые составят основу искомых регламентов противодействия.

Фактически, речь идет об оперативной автоматической выдаче рекомендаций администратору безопасности и его команде по организации мер смягчения ущербов в случае регистрации инцидента кибервторжения (т.е. обнаружения применения некоторой тактики атаки). При этом, чаще всего обсуждается реагирование на единичные деструктивные воздействия.

Однако, современные вторжения все более напоминают целые информационные операции, когда тактики чередуются и даже повторяются во времени по сценарию злоумышленников. Такие атаки стали называться комплексными, и они представляют особую опасность для множества киберсистем, которые сегодня во многом не готовы защищаться от подобных вторжений.

Поэтому особую активность будут иметь (в ближайшей обозримой перспективе) автоматизированные средства оперативного реагирования по ходу реализации комплексных кибератак (с опорой на соответствующие регламенты) на защищаемые системы. Вручную такую работу выполнять уже не представляется возможным (сотни техник и десятки тысяч соответствующих им уязвимостей).

Вместе с тем, сканирование известных баз данных формирование специализированных ресурсов позволит создать основу для решения поставленной выше задачи, которая отнюдь не представляется безнадежной в плане обеспечения кибербезопасности.

Обилие эпидемических моделей, к сожалению, пока не учитывает возможности эксплуатации многообразия уязвимостей посредством кибератак класса “Инъекция” [8]. При этом, имеются методические успехи вычисления вероятностей использования уязвимостей (1). В этом контексте представляется целесообразным рассмотреть каждый узел вирусно-атакуемой сети при его переходе из незараженного в противоположное состояние в результате эксплуатации серии наличествующих в узле уязвимостей, подверженных деструктивной инъекции. Если множество таких инъекций задано, то с помощью баз данных CAPEC, MITRE ATT&CK и CWE представляется возможным определить интересующие уязвимости CVE. Далее с помощью соответствующих калькуляторов можно найти вероятности успешной эксплуатации определенных уязвимостей. Совокупность таких моделей (для каждого узла сети) открывает перспективу моделирования сетевой эпидемии через матрицу инциденции узлов сети. Отбор для рассмотрения наиболее вероятных (для эксплуатации) уязвимостей позволит описать наихудший случай инъекции. При соответствующей модификации модели уместно осуществлять виде графовых структур. В этом случае можно оценивать вероятности общего исхода в тех или иных зонах сети посредством расчета соответствующих передаточных функций. Наглядность топологических представления атакуемой сетевой структуры открывает также перспективы управления эпидемических процессом (блокировка, локализация и т.п.) с учетом кластеризации сети и наличия в ее узлах тех или иных уязвимостей (по отношению к рассматриваемым техникам инъекции вредоносов). Совокупность вышеперечисленных соображений может лечь в основу целеполагания настоящего исследования, которое в данном случае

уместно развить и на комплексные кибератаки, где под внешним управлением злоумышленников устанавливается интенсивность и локация вбросов вредоносов в атакуемую сеть (задача противодействия таким атакам заслуживает особого внимания с точки зрения обеспечения сетевой кибербезопасности).

Заключение

Развитие обозначенных направлений исследования имеет существенное значение для обеспечения кибербезопасности, вместе с тем, предлагаемый методический подход может быть распространен и на другие отрасли знаний. Дело в том, что АИС и ТКС человек создавал по своему образу и подобию, что открывает перспективу использования сгенерированных им формализмов в разрешении социальных проблем, например, в отношении задач обеспечения информационно-психологической безопасности. В этой связи ниже формулируются соответствующие предложения.

Современные масс-медиа, особенно социальные сети и/или подобные информационные ресурсы достигли такой степени популярности, что фактически сейчас уже реализуют (в интересах их обладателей и регуляторов) массовое (можно сказать, машинное) обучение населения планеты. При этом, со множеством позитивов (оперативное и многоплановое информирование, удобство использования интересующих контентов и т.п.), вышеуказанные структуры несут обществу и ощутимые негативы (идеологемы, противные человеческому существу, и др.). В последнем случае, машинное обучение генерирует маргинальные группы индивидуумов (ЛГБТ, чайлдфри и пр.) в рамках либерально-порочной повестки глобалистов, рассчитывающих через эти группы достичь мирового господства.

Обозначенная выше угроза объективно требует осуществления риск-моделирования деструктивных процессов внедрения указанных идеологем в массовое сознание. Фактически, речь идет об обеспечении информационной безопасности общества, личности и даже государства в условиях реализации тактик и техник атак через психологические уязвимости.

Поскольку все существующие киберсистемы человек невольно создает по своему образу и подобию, то вполне уместно использование метода аналогий в решении поставленной задачи. Достаточно обратиться к ресурсу MITRE ATLAS [9], где применительно к машинному обучению формализованы тактики и техники деструктивных воздействий. Если при этом удастся установить соответствие техник и уязвимостей, а также – оцифровать вероятность их эксплуатации (в контексте обозначенной угрозы), то в решении поставленной задачи можно существенно продвинуться вперед.

Мало того, появится возможность моделирования комплексных информационно-психологических операций, внедряющих деструктивные идеологемы в сознание граждан и даже целых социальных групп. Здесь важно, прежде всего, сформировать матрицы тактик, техник и уязвимостей, статистику динамики множеств адептов, рассматриваемых идеологем, способствующих вероятностной оценке и прогнозированию динамики исследуемого процесса.

Список литературы

1. SSVC Calculator. – URL: https://www.cisa.gov/ssvc-calculator (дата обращения 30.10.2024).

2. EPSS. – URL: https://www.tist.org/epss/ (дата обращения 30.10.2024).

3. CVSS. – URL: https://tirst.org/cvss/specification-document (дата обращения 30.10.2024).

4. VISS. – URL: https://viss.zoom/com/calculator (дата обращения 30.10.2024).

5. BVSS. – URL: https://www.halbor.com/bvss/ (дата обращения 30.10.2024).

6. HVSS. – URL: https://hvss.online (дата обращения 30.10.2024).

7. OWASP. – URL: https://javierolmedo.github.io (дата обращения 30.10.2024).

8. CAPEC. – URL: https://capec.mitre.org/ (дата обращения 30.10.2024).

9. MITRE ATT&CK. – URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения 30.10.2024).

10. Организационно-правовая защита сетей / А. Г. Остапенко, Д. В. Щербакова, А. О. Калашников и др.; Под ред. Академика РАН Д. А. Новикова. – М.: Горячая линия – Телеком, 2023. -228с.

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 12.11.2024

Информация об авторах

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

CURRENT PROBLEMS AND SOME OF THEIR SOLUTIONS IN PART OF RISK CALCULATION OF THE SUCCESS OF IMPLEMENTING SINGLE CYBER-ATTACKS

A.A. Ostapenko

The urgent need for calculating the parameters of successful exploitation of vulnerabilities by specified types of single attacks is considered. The corresponding goal-setting is carried out with specification of the tasks of risk calculation, including a review of known calculators, creation of methodological and other support for risk analysis of single cyber-attacks. Analytical constructions for calculation are proposed, using the experience of operating vulnerability danger calculators. In particular, methods for reducing the subjectivity of assessments based on normalization and averaging of data from various risk calculators for the same vulnerability are designated. Examples of practical calculations of the probability of single exploitation of various vulnerabilities used in various types of cyber-attacks are given.

Keywords: risk analysis, vulnerability, probability, damage.

Submitted 12.11.2024

Information about the authors

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