DOI 10.36622/1682-7813.2025.28.2.012
УДК 004.056

РИСКИ РЕАЛИЗАЦИИ КИБЕРАТАК: ГРАФОВАЯ ФОРМАЛИЗАЦИЯ РИСК-АНАЛИЗА

Г.А. Остапенко, А.А. Остапенко, М.В. Кондратьев, Ю.М. Малежик, Д.Н. Герасимова

Основная идея статьи заключается в том, что необходимо разработать методологию и реализовать системы автоматизированной генерации мер и сценариев противодействия кибератакам на основе графового анализа. Кроме того, рассматривается программная реализация предложенной системы, которая включает в себя автоматизацию генерации мер и сценариев противодействия кибератакам и разработку алгоритмов динамического анализа рисков и алгоритма динамической генерации мер противодействия. Результаты исследования направлены на повышение устойчивости информационных систем к постоянно эволюционирующим угрозам, а также на снижение времени обнаружения и реагирования на возникающие инциденты кибербезопасности.

Ключевые слова: кибератака, моделирование, уязвимости, риск-анализ, графовая модель.

Введение

В условиях, когда цифровые технологии развиваются стремительными темпами вместе с повсеместным внедрением автоматизированных информационных систем, которые значительно облегчают работу в информационном пространстве ключевых секторов экономики, образования, здравоохранения, государственного управления и многих других секторов, обеспечение кибербезопасности становится стратегически важным направлением. Современный киберландшафт показывает не только стремительный рост числа атак в нем, но и значительное усложнение самих кибератак. Так, первый квартал 2025 года был ознаменован резким ростом числа кибератак во всем мире. По сравнению с данным за предыдущий год количество атак на организации в неделю увеличилось на 47 процентов, в среднем они подвергались примерно 1925 атакам еженедельно. Особенно возросла активность вымогателей: число атак с использованием программ-вымогателей увеличилось на 126 процентов по сравнению с началом 2024 года [1]. Эта информация, несомненно, указывает на то, что киберпреступники продолжают адаптироваться и усложнять техники своих атак, атакуя даже хорошо защищенные системы.

В результате анализа тенденции развития кибератак становится очевидным, что традиционные методы обеспечения информационной безопасности, основанные на статических базах данных об уязвимостях, сигнатурном анализе и фиксированных правилах реагирования, оказываются все менее эффективными против современных киберугроз. Кроме того, рост продолжительности атак указывает на то, что многие системы не способны обнаруживать угрозу, пока она не нанесен ущерб системе, что указывает на то, что текущие подходы к обеспечению безопасности не способны адаптироваться к эволюции кибератак и вовремя обнаруживать и реагировать на угрозы.

В данный момент одним из перспективных направлений в решении выявленных проблем обеспечения информационной безопасности является применение графовых моделей анализа киберугроз. Графы, в которых узлы представляют компоненты кибератак, а ребра – связи между ними, позволяют моделировать сложные сценарии атак. Но существующие подходы сильно ограничены в работе с динамично развивающимися угрозами информационной безопасности, а также с анализом различных абстрактных уровней кибератак. Для решения данной проблемы необходимо использовать граф, который

отражает все абстрактные уровни кибератаки, начиная от от паттернов, описывающих сценарии кибератаки и заканчивая уязвимостями в конкретном информационном активе. Реализация такой модели будет обеспечивать гибкость за счет учета всего множества вариаций реализации атаки. Например, если обнаруживается новая уязвимость, граф динамически обновится, вычислив новые опасные сценарии кибератак и рекомендуя приоритетные меры противодействия по обнаружению, реагированию и ликвидации последствий возникших угроз.

Целью настоящей работы является разработка методологии и реализация системы автоматизированной генерации мер и сценариев противодействия кибератакам на основе графового анализа. Для достижения цели решаются следующие задачи:

1) формализация модели графа, интегрирующей данные об уязвимостях, слабостях архитектуры, техниках и шаблонах реализации сценариев кибератак;

2) разработка алгоритмов динамического анализа рисков с учетом влияния на доступность, целостность и конфиденциальность информации;

3) разработка алгоритма динамической генерации мер противодействия кибератакам.

Научная новизна работы заключается в объединении методов теории графов, машинного обучения и анализа рисков для создания адаптивной системы, способной противостоять непрерывно развивающимся кибератакам в режиме реального времени.

Практическая значимость выражается в возможности внедрения разработанной системы в автоматизированные информационные системы для повышения их устойчивости к постоянно эволюционирующим киберугрозам, а также для снижения времени обнаружения и реагирования на возникающие инциденты кибербезопасности, тем самым минимизируя ущерб от атак.

1. Формализация модели графа, интегрирующая данные об уязвимостях, слабостях архитектуры, техниках и шаблонах реализации сценариев кибератак

Вследствие того, что современные угрозы кибербезопасности все чаще характеризуются высокой сложностью, многоуровневостью и динамичностью. Традиционные подходы к анализу уязвимостей, основанные только на статических метриках вроде CVSS, часто не учитывают контекст реальных атак и вероятность эксплуатации уязвимостей злоумышленниками. Для того, чтобы избежать данных ограничений одним из лучших вариантов является реализация системы на основе графовой модели, что позволяет объединить данные разных уровней абстракции в единую структуру, которая сможет отразить важные взаимосвязи между различными компонентами, составляющими кибератаку.

1.1. Модель графа

В данной работе представлено решение, которое включает в себя ориентированный мультиграф G = (N,E), где множество узлов N включает элементы следующих типов: интегрирующий наиболее популярные стандарты в области кибербезопасности:

- **CVE (Common Vulnerabilities and Exposures)** – уязвимости информационных активов. Одна из основных метрик узла - вероятность успешной эксплуатации уязвимости во время кибератаки [4]. Для расчета данной метрики используется система EPSS (Exploit Prediction Scoring System) [7], предназначенная для прогнозирования вероятности эксплуатации уязвимости в реальных условиях. Данная система основана на машинном обучении и учитывает исторические данные о реальных эксплойтах уязвимостей, опубликованных через такие платформы по кибербезопасности как: ExploitDB (одной из самых больших баз данных эксплоитов), Metasploit (самом популярном и поддерживаемом фреймворке для тестирования на проникновение и разработки эксплойтов) и данных об

инцидентах кибербезопасности от организации, занимающейся кибербезопасностью, реагированием на инциденты и анализом уязвимостей, CERT (Computer Emergency Response Team). Из-за того, что EPSS фокусируется на реальной вероятности эксплуатации уязвимости, а не только на ее технической серьезности, данная система является приоритетной для определения вероятности эксплуатации уязвимостей.

- **CWE (Common Weakness Enumeration)** – классификация слабостей программного обеспечения и архитектуры системы, которые могут быть использованы для реализации атаки [9]. Поскольку CWE порождает множество CVE, то вероятность успешной реализации кибератаки через данную слабость архитектуры будет рассчитываться как вероятность того, что любая, но только одна из связанных CVE будет проэксплуатирована в ходе атаки. Предполагая независимость эксплуатаций отдельных CVE (что справедливо при отсутствии корреляции между уязвимостями), для этого найдем вероятность эксплуатации только одной CVE, что реализуется как вероятность эксплуатации CVE ($EPSS(CVE)$) умноженная, на вероятность того, чтобы другие CVE не будут проэксплуатированы ($1 - EPSS(CVE)$). Тем самым получим основную формулу:

$$P_{CWE} = \sum_{i=1}^{N}[EPSS(CVE_i) * \prod_{j=1,j\neq i}^{N}(1 - EPSS(CVE_j)],$$

где N – количество дочерних уязвимостей (CVE).

На рис. 1 изображены узлы CWE интегрированные в граф в количестве 986 штук, где цвет узлов тем темнее, чем вероятность эксплуатации CVE через данную CWE выше:

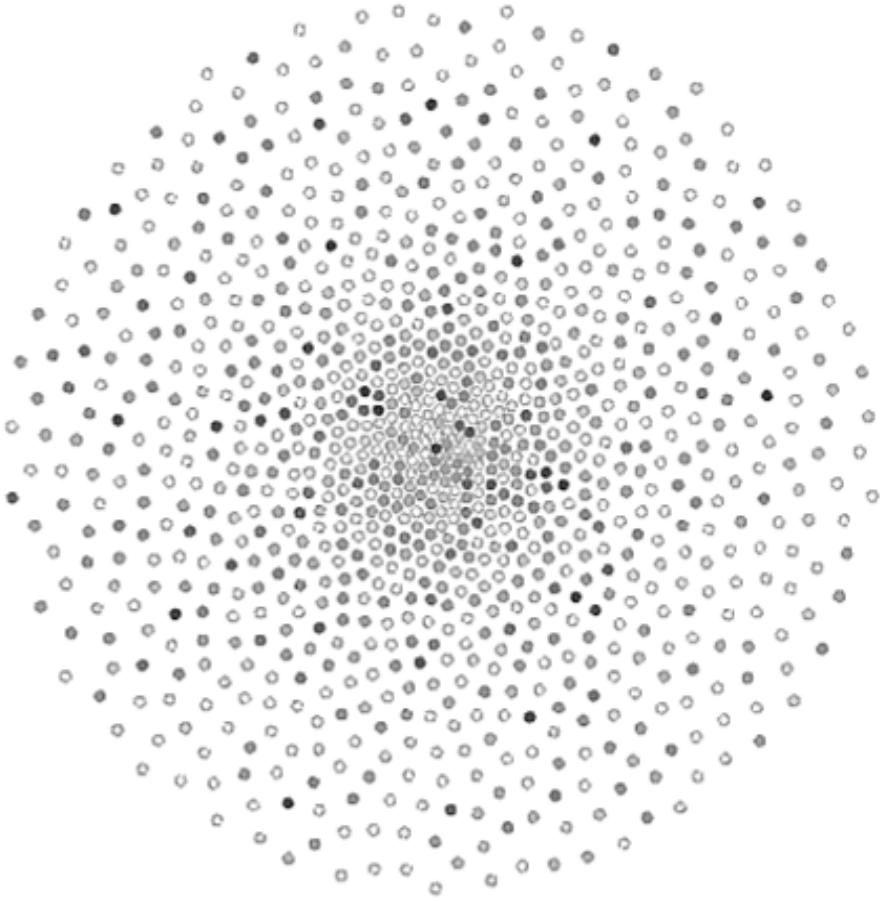


Рис. 1. Узлы CWE в графе компонентов кибератак

- **техника MITRE ATT&CK** – техники, применяемые на этапах жизненного цикла кибератаки. Чтобы найти вероятность успешного использования техники в кибератаке, нужно найти вероятность того, что атака будет успешно реализована через одну из слабостей архитектуры атакуемой системы, которые соответствуют данной технике, так как в вероятностях CWE уже учтены вероятности уязвимостей, то данная вероятность также будет означать и вероятность того, что в ходе атаки, использующей определенную технику, будет проэксплуатирована одна из уязвимостей, которые относятся непосредственно к данной технике. В результате формула нахождения вероятности для такого узла графа будет следующей:

$$P_T = \sum_{i=1}^{N}[P_{CWE_i} * \prod_{j=1, j\neq i}^{N}(1 - P_{CWE_j})],$$

где N количество дочерних CWE у техники.

На рис. 2 изображены узлы техник интегрированные в граф в количестве 823 штук, где цвет узлов тем темнее, чем вероятность эксплуатации CVE в ходе атаки через использование данной техники выше:

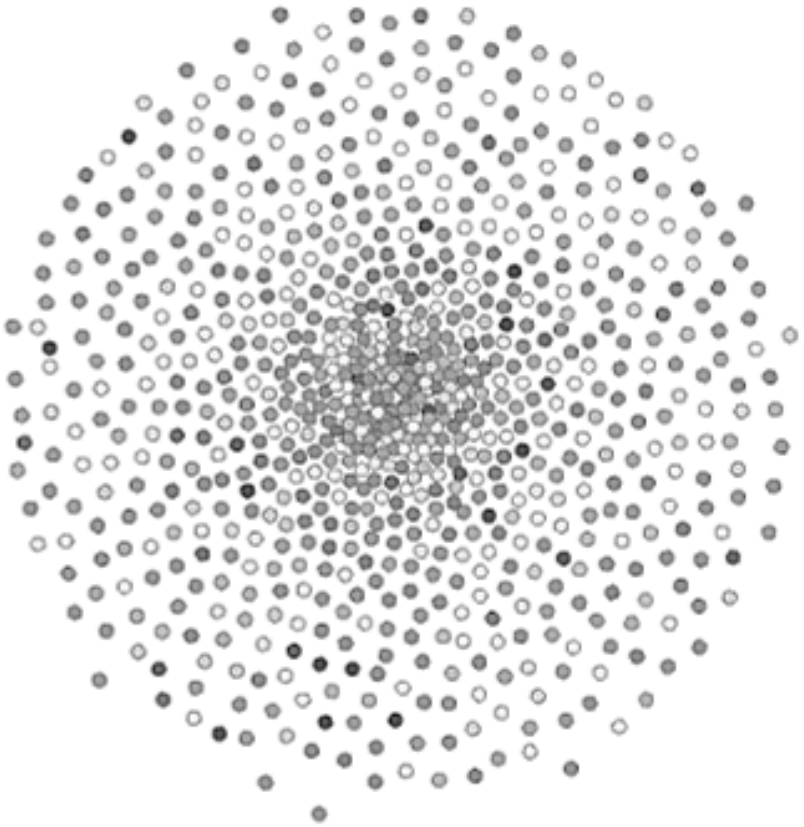


Рис. 2. Узлы техник в графе компонентов кибератак

- **CAPEC (Common Attack Pattern Enumeration and Classification)** – шаблоны атак, описывающие типовые сценарии кибератак [10];

Ребра E определяют отношения между узлами:

- **CAPEC → MITRE ATT&CK** – указывает какие техники могут быть реализованы в сценариях кибератаки (рис. 3). Данная связь не имеет веса и используется исключительно для выделения техник в контексте определенной кибератаки;

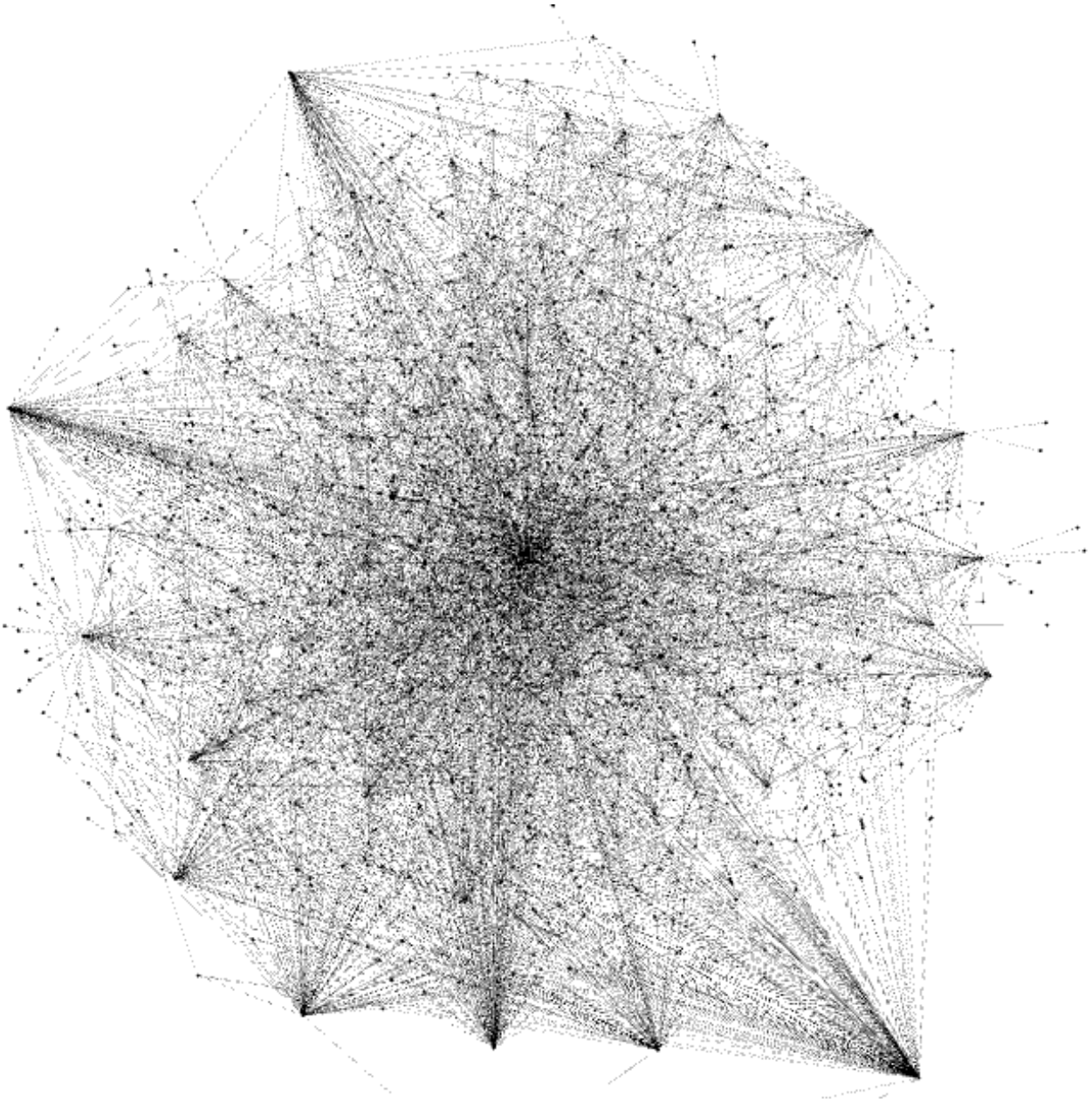


Рис. 3. Взаимосвязи между узлами CAPEC и техниками в графе компонентов кибератак

- **MITRE ATT&CK → CWE** – связь указывает какие слабости в архитектуре могут использоваться для реализации атаки определенной техникой. Данная связь имеет вес, равный вероятности использования определенной техникой в ходе кибератаки конкретной слабости в архитектуре атакуемой системы. Она рассчитывается на основе гипотезы, что злоумышленник будет предпочтительнее использовать для кибератаки техникой те слабости архитектуры, которые с наибольшей вероятностью принесут ему успех. Исходя из данной гипотезы становится очевидным, что во время атаки определенной техникой, вероятность использования слабости будет прямо пропорциональна вероятности успешной эксплуатации одной из уязвимостей, которые относятся к данной CWE, также данный тип связи подразумевает, что с вероятностью 100 процентов будет избрана одна из соответствующих CWE, так как других вариантов в ходе кибератаки выбранной техникой у злоумышленника нет. На основе данной информации, вес связи должен быть прямо пропорционален P_{CWE} и сумма всех таких связей, исходящих из определенной техники, должна быть равна 1, из чего можно выделить следующую формулу для таких ребер:

$$W_{T \to CWE_i} = \frac{P_{CWE_i}}{\sum_{j=1}^{N} P_{CWE_j}},$$

где N – количество CWE которые могут быть использованы в ходе кибератаки через технику T. На рис. 4 изображен граф со взаимосвязями между техниками и CWE, которые могут использовать во время атаки, где чем шире выглядит связь, тем больше вероятность выбора CWE в контексте определенной техники.

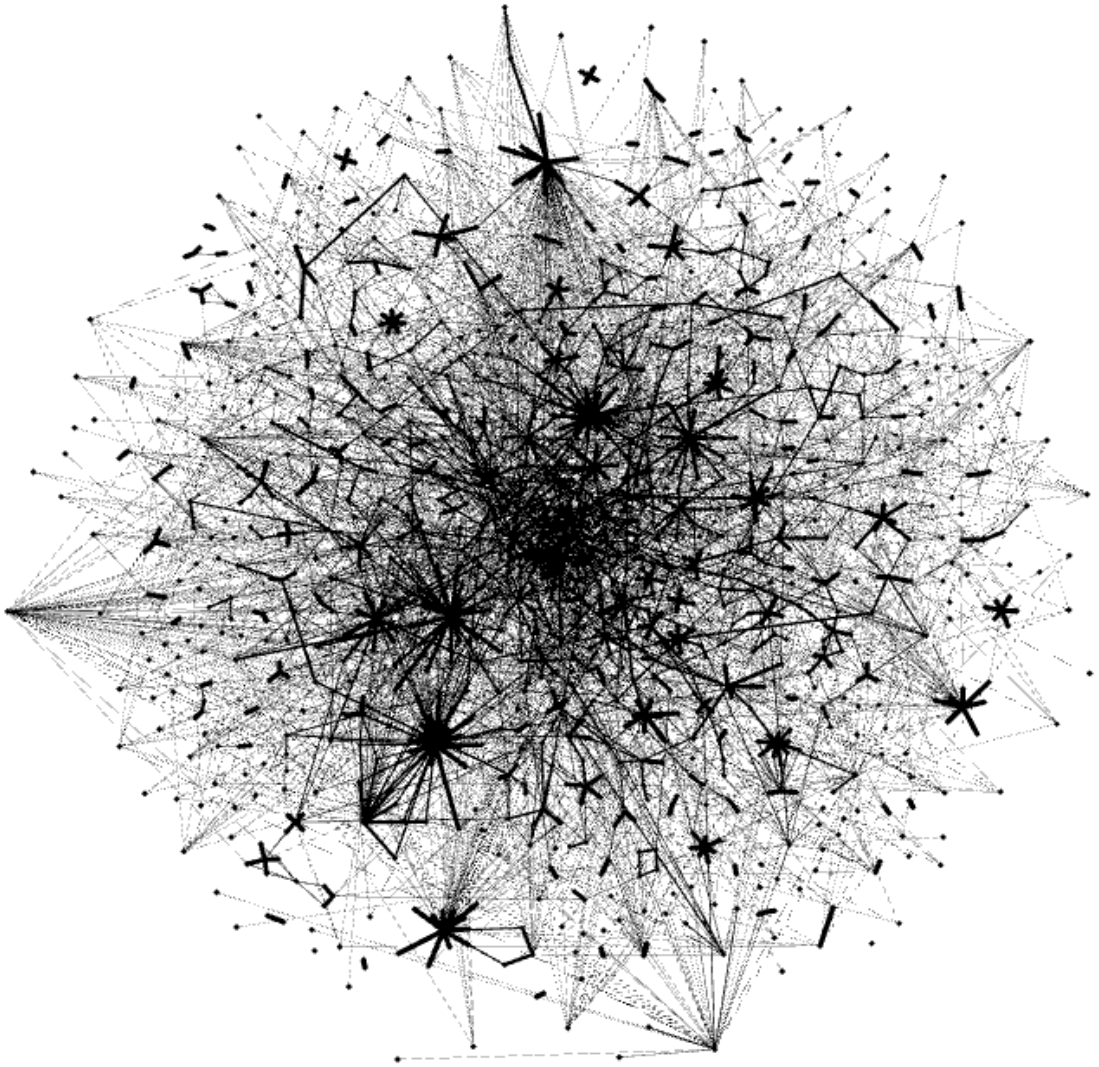


Рис. 4. Взаимосвязи между узлами техник и CWE в графе компонентов кибератак

- **CWE → CVE** – связь указывает с какой вероятностью в ходе атаки, использующей определенную слабость архитектуры системы, злоумышленник проэксплуатирует определенную уязвимость. Данная вероятность, аналогично предыдущей гипотезе, будет прямо пропорциональна метрике EPSS конкретной уязвимости и сумма весов таких дуг, исходящих из опредленной CWE будет равна 1, означая, что злоумышленник, избрав опредленную слабость архитектуры во время атаки обязательно примет попытку эксплуатировать одну из уязвимостей. В результате, формула расчета вероятности для данного типа ребра будет следующая:

$$W_{CWE \to CVE} = \frac{P_{CVE}}{\sum_{i=1}^{N} P_{CVE_i}},$$

где N – количество CVE порожденных данной слабостью в архитектуре.

На рис. 5 представлен граф, на котором изображены узлы CWE и CVE со связями между ними.

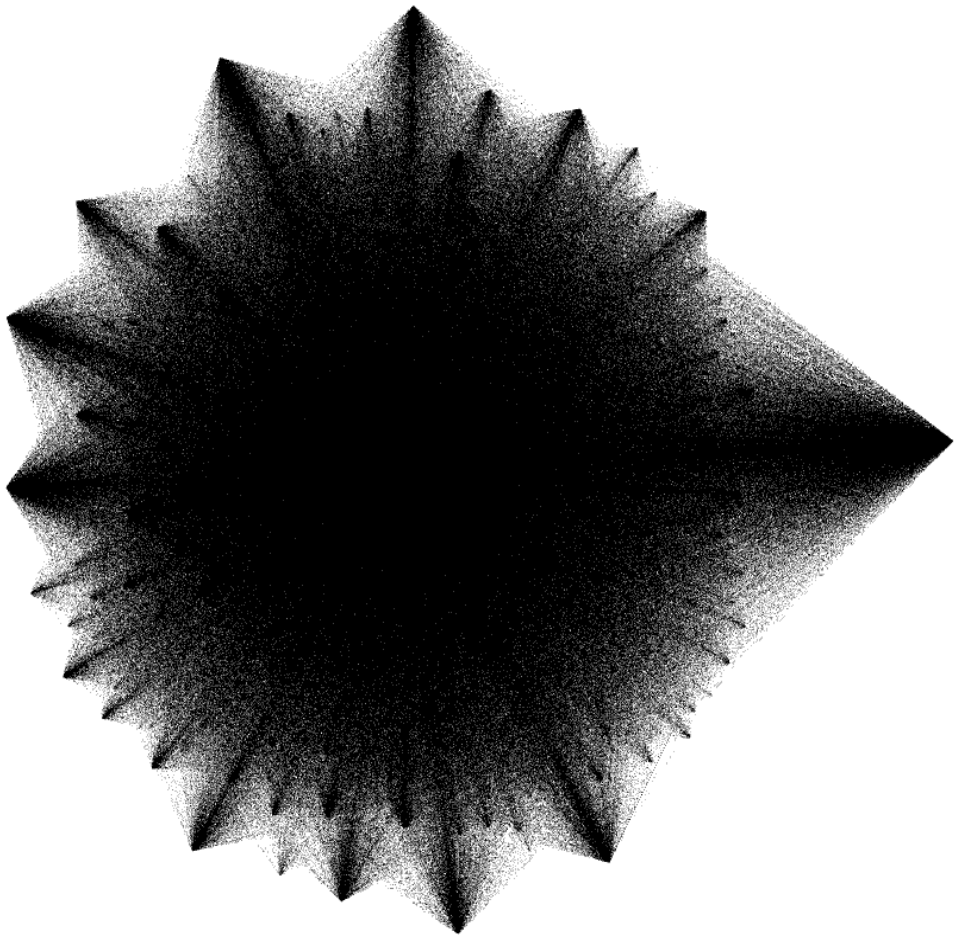


Рис. 5. Взаимосвязи между узлами CWE и CVE в графе компонентов кибератак

Такая структура графа реализует комплексный подход к моделированию атаки на различных уровнях, начиная от более абстрактных CAPEC и техник MITRE ATT&CK до более конкретных уязвимостей (CVE) и их обобщенных классов (CWE), а также позволяет моделировать сценарии для кибератак. На рис. 6 изображен полностью граф, включающий в себя узлы CAPEC, техники, CWE и CVE, а также ребра между ними.

1.2. Нейросетевая модель генерации связей в графе

Для успешного анализа кибератак, используя описанный выше граф, необходимы качественные данные, а из-за непрерывного роста числа атак, а также увеличивающейся сложности привычные методы ручного сопоставления уязвимостей, техник и шаблонов атак становятся все менее действенными в силу дефицита специалистов в сфере информационной безопасности. Основным решением данной проблемы избрано машинное обучение, так как правильно разработанные и обученные современные нейросетевые модели показывают высокую точность и скорость работы в сравнении с человеком. Главной архитектурой был выбран ансамблевый подход, состоящий из моделей CySecBERT с TF-IDF. Для того, чтобы более подробно разобраться в качестве такого подхода, необходимо рассмотреть комбинируемые модели по отдельности.

CySecBERT является специализированной версией модели BERT, которая относится к классу архитектур на основе трансформеров и предназначена для глубокого анализа естественного языка в сфере кибербезопасности. Для более глубокого понимания стоит рассмотреть основу этой архитектура, а именно модель BERT. Она стала большим прорывом в области анализа текстов благодаря

способности учитывать двусторонний контекст, что позволяет модели одновременно анализировать слова как в прямом, так и в обратном направлении, для того чтобы понимать семантическую связь между элементами предложения. Такой подход дал возможность BERT выявлять смысловые отношения между текстами. Из-за того, что BERT основан на трансформерах - нейросетевой структуре, в которой каждый элемент входной последовательности взаимодействует с каждым элементом выходной последовательности через механизмы внимания, что дает данной модели следующие ключевые преимущества [2]:

- параллелизм – данная особенность дает возможность обработки всех слов в тексте одновременно, что позволяет значительно ускорить вычисления;
- обработка длинных текстов – механизмы внимания позволяет данной модели эффективно улавливать зависимости даже между далеко удаленными элементами анализируемого текста;
- поддержка предобучения – у BERT есть возможность заранее обучиться на больших наборах текста, после чего свободно использоваться под конкретные задачи.

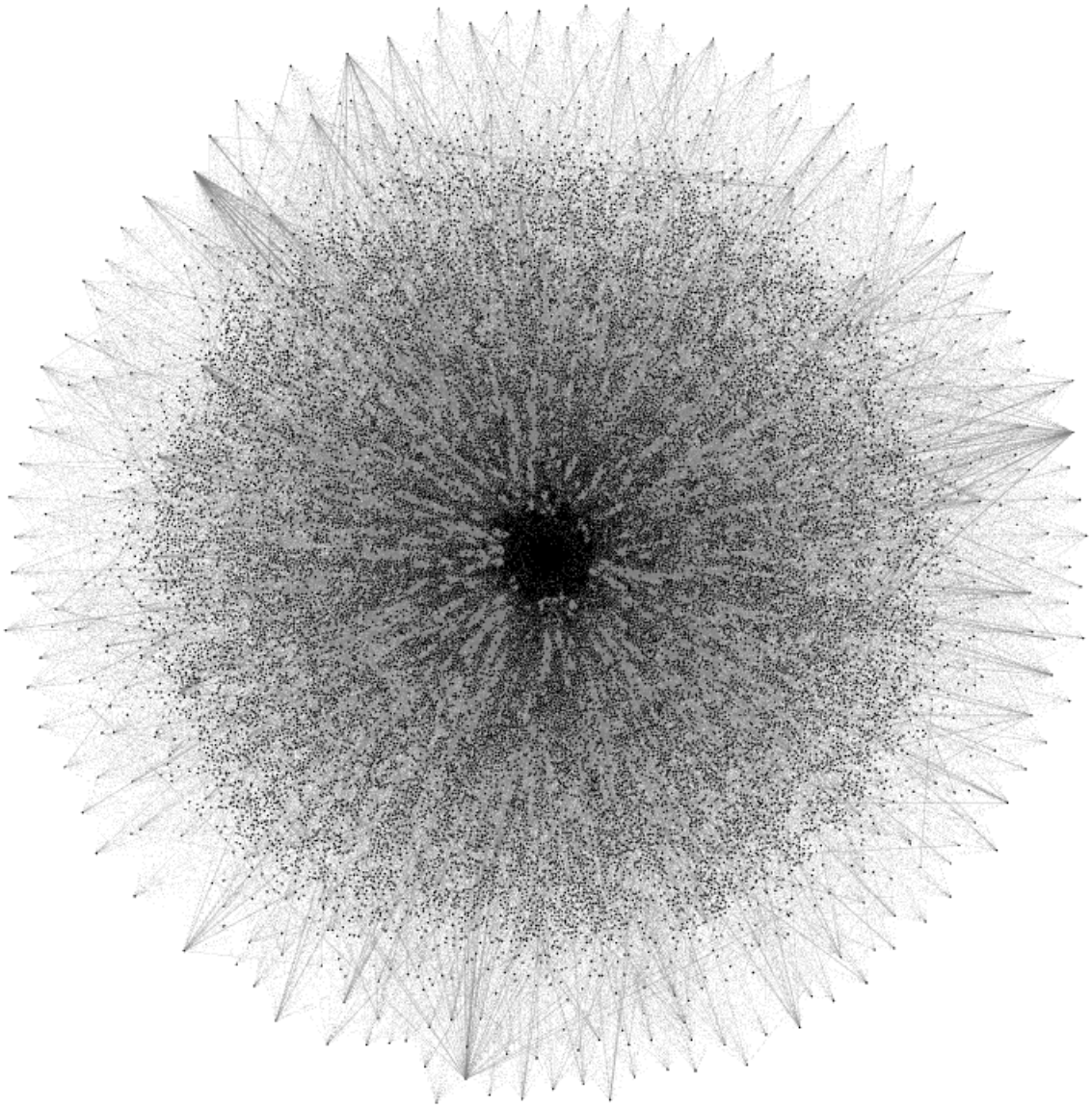


Рис. 6. Узлы CAPEC, техник, CWE и CVE и взаимосвязей между ними в графе компонентов кибератак

CySecBERT также включает в себя все основные преимущества BERT, но важен из-за того, что фокусируется именно на кибербезопасности. Данная модель предобучена на уникальном наборе данных, содержащем 4,3 миллиона записей, связанных с угрозами, уязвимостями и инцидентами кибербезопасности. Такая узконаправленная специализация позволяет CySecBERT лучше понимать конкретные термины, вроде «APT-атака» или «zero-day», а также сложные описания, характерные для отрасли обеспечения информационной безопасности [3].

В свою очередь, **TF-IDF (Term Frequency-Inverse Document Frequency)** – это статистическая модель, которая так же, как и BERT широко используемая в анализе и обработке текстов. Основная задача данной модели заключается в том, чтобы определять, какие термины наиболее значимы для конкретного текста или набора текстов, учитывая при этом как локальную частоту термина в документе, так и глобальное распространение во всем наборе, что позволяет выделять ключевые слова, игнорируя общие и малоинформативные термины. Для TF-IDF можно выделить следующие основные компоненты:

- частота термина (TF) измеряет частоту появления слова в конкретном документе. В большинстве случаев данный компонент рассчитывается как отношение количества вхождений термина к общему числу слов в документе:

$$TF(t,d) = \frac{\text{количество вхождений термина } t \text{ в документ } d}{\text{количество всех слов в документе } d},$$

- обратная частота документа (IDF) – измеряет, насколько редко термин встречается во всей коллекции документов:

$$IDF(t,D) = \frac{\text{количество документов в наборе } D}{\text{количество документов, содержащих термин } t}.$$

В результате общий вес данной модели равен произведению TF на IDF:

$$TF\ IDF(t,d,D) = TF(t,d) \times IDF(t,D).$$

Высокий вес в TF-IDF получают часто встречающиеся слова в конкретном документе, но редкие в общем наборе документов. Например, в какой-либо статье о кибератаках слово «APT» будет иметь высокий общий вес TF-IDF, если оно достаточно часто упоминается в данной статье, но очень редко упоминается в других текстах.

Данная модель была выбрана из-за следующих ключевых преимуществ:

- простота реализации,
- вычислительная эффективность при работе с большими наборами текстов,
- успешное применение в задачах, где важна частотность терминов.

Таким образом, обобщая описанные модели, можно сделать вывод, что данный подход позволяет получить наиболее релевантные связи между различными текстами за счет комбинации преимущества CySecBERT в нахождении семантической связи и преимущества TF-IDF в нахождении ключевых слов в тексте.

В итоге, становится возможным дать описание работы модели генерации связей между узлами в контексте текущего графа кибератак. Подход заключается в том, чтобы сопоставлять описание узла, со всем множеством описаний узлов другого типа (например CWE с CVE). Данные описания передаются в модель, после чего происходит их преобразования и вычисление конечных метрик сходства, которые дают итоговый результат в виде взвешенной суммы метрик моделей CySecBERT и TF-IDF в соотношении 70% к 30 %. Данное соотношение дает лучшую точность на

основе множества проведенных экспериментов, где поиск лучшего соотношения велся с помощью методики GridSearch (составлялась таблица всевозможных ансамблевых сопоставлений BERT и TF-IDF и происходил расчет точности по каждой ячейке таблицы). Также при реализации такой модели применяется распространенный прием, идея которого заключается в предобработке сравниваемых текстов перед их помещение в модель, что позволяет исключить лишние слова без определенной смысловой нагрузки на текст, тем самым ускоряя обработку и повышая точность метрик сходства.

Стоит выделить, что при использования данной модели появляется возможность интеграции любых доступных баз знаний, которые охватывают различные составляющие компоненты кибератак. Наибольшее преимущество же заключается в появившейся способности к оперативному обновлению в случае появления новых составных компонент кибератаки или обновления информации о старых компонентах, как только появляются новые данные – они сразу же могут быть проанализированы и интегрированы в существующий граф, благодаря чему модель остаётся адаптированной к быстро меняющейся киберобстановке, что гарантирует высокое качество данных, а соответственно и наиболее точные показатели риска.

2. Разработка алгоритмов динамического анализа рисков с учетом влияния на доступность, целостность и конфиденциальность информации

Основные меры противодействия кибератакам являются комплексом действий и стратегически важных подходов, которые направлены на защиту информационных систем. Такие меры противодействия включают в себя следующие ключевые этапы: обнаружение инцидентов, оперативное реагирование на них, а также ликвидация последствий после завершенной кибератаки. Все три компонента являются обязательной основой, без которой практически невозможно снижение уровня рисков до минимальных значений. В результате можно сделать вывод, что такие важные и затратные меры необходимо применять только для важных атак, который действительно могут нанести ущерб системе, для этого необходим точный и глубокий анализ рисков, возможных кибератак.

Таким образом, эффективная генерация мер противодействия невозможна без системного подхода к анализу рисков, что делает этот процесс неотъемлемой частью современной стратегии обеспечения информационной безопасности.

На основе полученной графовой базы данных вычисляются основные веса узлов графа, а именно: риск для конфиденциальности, риск для целостности и риск для доступности защищаемой информации.

По основному определению, риск – это потенциальная возможность причинения вреда в результате реализации какой-либо угрозы к какому-либо активу через существующую уязвимость. Поэтому риск в контексте данного анализа будет считать именно потенциальным ущербом от реализации кибератаки. В результате получим формулу риска:

$$Risk = P \times \underline{U} \times C,$$

где P – вероятность реализации угрозы через уязвимость,

$\underline{U}$ – нормированный ущерб активу в результате реализации угрозы,

C – ценность актива.

Так как ценность актива зависит от архитектуры информационной системы, то очевидно, что создание универсальной и гибкой системы на основе данной формулы риска становится затруднительным, поэтому ценность актива можно временно сократить, оставив только нормированный ущерб, тем самым полив нормированный риск, что даст системе универсальность и гибкость. В результате получим формулу нормированного риска, на основе которой будет строиться весь подход к анализу:

$$\underline{Risk} = P \times \underline{U}.$$

На основании определения риска в данной системе, фундаментальной единицей атаки являются уязвимости, используя взаимосвязи, с которыми можно будет получить более расширенный риск, связанный с CWE, техниками и сценариями кибератак. Необходимо подробнее рассмотреть главные свойства уязвимостей, которыми являются:

- вероятность эксплуатации уязвимости в ходе кибератаки, данное свойство узла рассчитывается в ходе интеграции данных в граф, использую систему EPSS;
- нормированный ущерб активу в результате эксплуатации уязвимости, данное свойство для уязвимости CVE одним из основных подходов принято определять на основе двух показателя CVSS.

CVSS (Common Vulnerability Scoring System) [5, 6] – это один из наиболее используемых и признанных в области кибербезопасности стандартов оценки серьезности уязвимостей в системах информационной безопасности. Значение серьезности уязвимости, вычисленное при помощи данной системы используется в качестве нормированного ущерба в ряде известных подходов к анализу рисков, таких как FAIR, NIST SP 800-30 и OCTAVE. Данная система оценки подходит унифицировано к количественной оценке уязвимостей, что уже позволяет организациям наладить эффективный анализ и управление рисками, выстраивая приоритеты реагирования на атаки. Базовый показатель CVSS состоит из двух основных групп метрик:

- метрики атаки характеризуют условия и возможности для реализации уязвимости;
- метрики воздействия указывают на последствия, которые могут быть вызваны при успешной эксплуатации уязвимости, влияющие на три базовые характеристики актива: конфиденциальность, целостность и доступность.

Основной недочет системы CVSS заключается в том, что предоставляется общий ущерб активу в результате эксплуатации уязвимости, что не дает возможности оценить влияние на каждое из перечисленных свойств безопасности информации, что важно для эффективного управления рисками и принятия обоснованных решений по защите информации, на основе осведомленности в том, какую именно часть инфраструктуры и какие конкретные аспекты безопасности затрагивает та или иная уязвимость.

В результате подробного изучения структуры и формул расчета базовой оценки в различных версиях CVSS, было сделано заключение о возможности ее декомпозиции на метрики, соответствующие каждому из базовых свойств безопасности информации, а именно: конфиденциальности, целостности и доступности, что даст возможность учитывать какой из компонентов безопасности будет подвергаться наибольшему риску.

Для реализации такого подхода к декомпозиции базовой оценки CVSS был избран метод распределения вклада каждой компоненты безопасности в базовую оценку, основанный на теории кооперативных игр, в точности на методе Шепли, так как именно данный метод используется для справедливого распределения общего вклада в результат между участниками, делая выводы исходя из маргинальных вкладов участников во всех возможных комбинациях. Рассмотрим данный метод подробнее. Пусть $v(S)$ – функция расчета Base Score при заданных метриках $S \subseteq N$, где N = {К, Ц, Д}. Тогда становится возможным рассчитать значения Шепли по следующей формуле:

$$\phi_i(v) = \frac{1}{n!}\sum_{p \in (\text{перестановки } N)}[v(S_p(i) \cup \{i\}) - v(S_p(i))],$$

где $\phi_i(v)$ – вклад метрики $i \in \{К, Ц, Д\}$ в CVSS Base Score;

$S_p(i)$ – множество метри, добавленных до i в перестановке p;

$v(S)$ – функция расчета Base SCore при наличии только метрик из S.

В результате чего Base Score рассматривается как характеристическая функция кооперативной игры, где игроки – это метрики конфиденциальности, целостности и доступности.

Используя данную формулу, рассчитываются маргинальные вклады в CVSS Base Score для каждой из метрик К, Ц, Д. Зная эти значения Шепли, необходимо их нормализовать, для этого необходимо рассчитать суммарное влияние по формуле:

$$\phi_{\text{кцд}} = \phi_{\text{к}} + \phi_{\text{ц}} + \phi_{\text{д}}.$$

После вычисления суммарного влияния на Base Score можно получить веса для каждой метрики по следующей формуле:

$$w_{\text{К,Ц,Д}} = \frac{\phi_{\text{к,ц,д}}}{\phi_{\text{кцд}}}.$$

В итоге, с помощью весов для каждой метрики появляется возможность рассчитать CVSS для каждой отдельной метрики по следующей формуле:

$$CVSS_{\text{К,Ц,Д}} = CVSS_{Base\ Score} \times w_{\text{К,Ц,Д}}.$$

Но из-за того, что оценка CVSS является статическим показателем потенциального ущерба, то появляется потребность в подкреплении данного значения динамической информацией, которая позволила бы адаптироваться к изменяющемуся киберпространству. Такой информацией можно считать наличие уязвимости в базе данных CISA KEV, что указывает на её высокую степень серьезности и потенциальную опасность для информационной безопасности из-за приоритетности ее выбора злоумышленником [8]. К тому же, CISA KEV (Catalog of Known Exploited Vulnerabilities) является официальной базой данных об уязвимостях, которые в действительности уже были эксплуатированы злоумышленниками в ходе кибератак. Данный каталог ведётся Агентством кибербезопасности и инфраструктурной безопасности США (CISA) и предназначен для повышения защищенности организаций. Выбор данной базы данных как одного из факторов потенциального ущерба уязвимости обусловлен тем, что CVE в нем имеют высокую релевантность и актуальность, гарантируя, что все уязвимости, были подтверждены в реальных кибератаках. Также исследования показали, что уязвимости, включенные в базу данных CISA KEV, устраняются в среднем в 3.5 раза быстрее, чем другие известные уязвимости, не входящие в этот список. Такая динамика объясняется повышенным вниманием как со стороны специалистов по безопасности, так и со стороны злоумышленников, поскольку наличие уязвимости в CISA KEV сигнализирует о реальной угрозе компрометации систем.

Также вследствие того, что наполняет базы CISA KEV не всегда оптимальна одним из важных коэффициентов является относительная критичность уязвимости, которая определяется как отношение критичности CVE к сумме критичность всех CVE, которые могут быть проэксплуатированы в ходе рассматриваемой атаки. Это значение учитывает вес уязвимости в контексте всего множества возможных CVE, что важно для эффективной оценки с целью реализации качественных мер противодействия кибератакам.

В результате, становится возможным составить итоговую формулу нахождения нормированного ущерба для уязвимости:

$$\underline{U_{\text{К,Ц,Д}}} = CVSS_{\text{К,Ц,Д}} \times K_{CISA\ KEV} \times \left(1 + \frac{CVSS(CVE)}{\sum_{i=1}^{N} CVSS(CVE_i)}\right) \times \frac{1}{70},$$

где К, Ц, Д – означают влияние на конфиденциальность, целостность или доступность информации;

$K_{CISA\ KEV}$ – коэффициент значение которого равно 1, если уязвимость не находится в базе CISA,

1.75 – если уязвимость находится в базе данных;

3.5 – если уязвимость находится в базе CISA KEV и просрочены сроки исправления, указанные в ней, тем самым данные коэффициенты учитывают текущие тенденции в киберпространстве;

$\frac{1}{70}$ – значение, которое используется для нормировки ущерба в пределах от 0 до 1 и вычисляется как частное единицы к

произведению максимального значения CVSS (10), на максимальное значение $K_{CISA\,KEV}$ (3.5) и на максимальное значение относительной критичности (2).

Теперь, получив главные свойства уязвимости для нахождения потенциального ущерба при эксплуатации уязвимости, становится возможным описать итоговую формулу расчета потенциального ущерба целостности, доступности или конфиденциальности информации в ходе эксплуатации уязвимости:

$$\underline{Risk_{CVE}^{\text{К,Ц,Д}}} = EPSS * \underline{U_{\text{К,Ц,Д}}}.$$

Данный подход позволяет создавать многомерные графы, учитывающие потенциальный нормированный ущерб для целостности доступности и конфиденциальности, что можно увидеть на рис. 7, где узлы CVE тем темнее, чем выше риск.

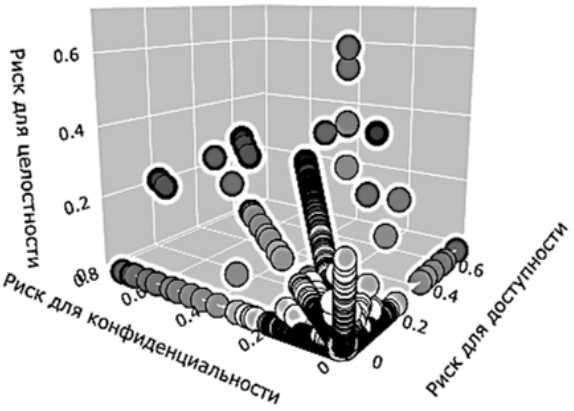


Рис. 7. Многомерный граф рисков для узлов CVE

Теперь, зная риски узлов CVE в графе и имея взаимосвязи, характеризующие вероятность выбора злоумышленником, между уязвимости и порождающими их CWE, становится возможным расчет нормированного риска (потенциального нормированного ущерба) кибератаки, использующей определенную слабость архитектуры системы при эксплуатации уязвимости. Данный риск вычисляется по следующей формуле:

$$\underline{Risk_{CWE}^{\text{К,Ц,Д}}} = \sum_{i=1}^{N} \underline{Risk_{CVE_i}^{\text{К,Ц,Д}}} * W_{CWE \to CVE_i},$$

где N – количество CVE связанных с CWE,

$W_{CWE \to CVE_i}$ – вероятность выбора CVE злоумышленником, рассчитанная при создании графа.

На рис. 8 изображен многомерный граф, учитывающий потенциальный нормированный ущерб для целостности доступности и конфиденциальности в ходе реализации атаки с использованием определенных слабостей архитектуры, где узлы тем темнее, чем выше риск:

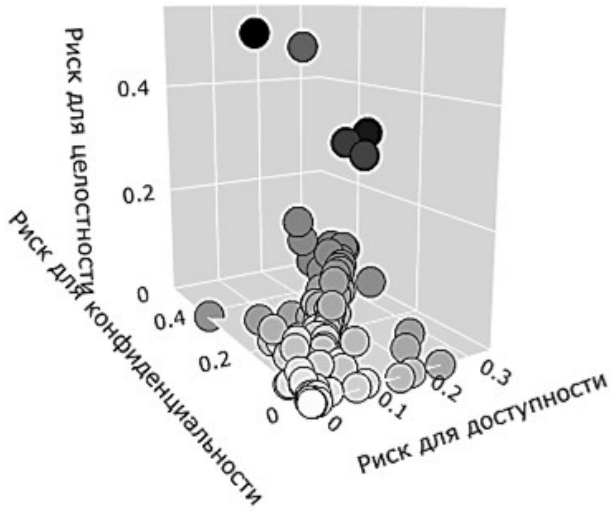


Рис. 8. Многомерный граф рисков для узлов CWE

Получив нормированные риски кибератак, использующих слабости в архитектуре, которые учитывают в себе риски кибератак эксплующих определенные уязвимости, можно рассчитать потенциальный нормированный ущерб, наносимый в результате реализации кибератак, выполненных определенными техниками Mitre Attack, что выполняется по следующей формуле:

$$\underline{Risk_{T}^{\text{К,Ц,Д}}} = \sum_{i=1}^{N} \underline{Risk_{CWE_i}^{\text{К,Ц,Д}}} * W_{T \to CWE_i},$$

где N – количество CWE связанных с техникой;

$W_{T \to CWE_i}$ – вероятность выбора CWE злоумышленником, рассчитанная при создании графа.

На рис. 9 изображен многомерный граф, учитывающий потенциальный нормированный ущерб для целостности доступности и конфиденциальности в ходе

реализации атаки с использованием определенной техники, где узлы тем темнее, чем выше риск:

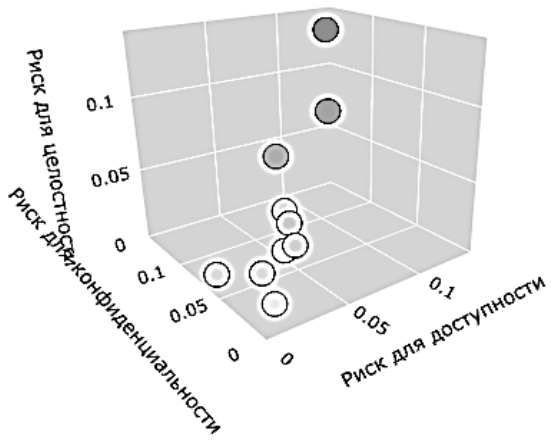


Рис. 9. Многомерный граф рисков для узлов техник

Для расчета рисков сценариев кибератак используются последовательности техник Mitre Attack, найденные через специально разработанный граф, реализующий цепи Маркова, который состоит из техник, относящихся к определенным тактикам Mitre Attack, а также дополнительных узлов СТАРТ и СТОП, которые показывают начало и конец любого сценария кибератаки. На рис. 10 изображен граф, учитывающий всевозможные сценарии кибератак, на основе 823 техник и 236449 взаимосвязей между ними:

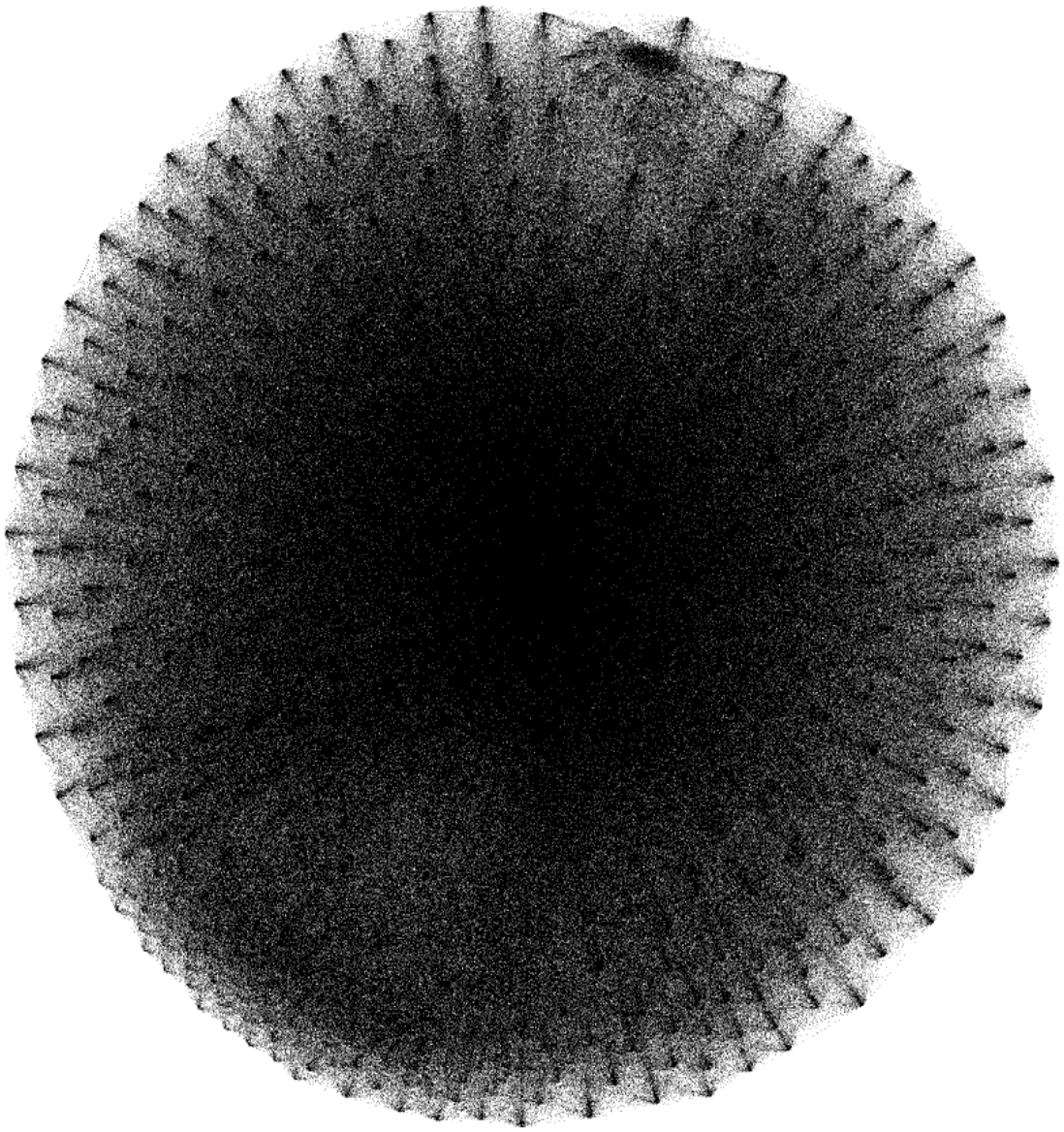


Рис. 10. Граф сценариев кибератак

Для реализации такого графа используется отдельный вид ребра “техника → техника”, которое указывает какая техника в сценарии будет использоваться следующей в ходе реализации кибератаки. Данное ребро имеет вес равный вероятности перехода от одной техники к другой, что рассчитывается на основе предположения, что злоумышленник будет выбирать технику с наиболее вероятным успехом ее завершения. В результате вес данной связи рассчитывается по следующей формуле:

$$W_{T \to T_i} = \frac{P_{T_i}}{\sum_{j=1}^{N} P_{T_j}},$$

где T_i – техника, вес ребра между которой рассчитывается от текущей техники T,

N – количество техник, в которые текущая техника имеет возможность перейти в ходе атаки;

Техники в графе соединены между собой в определенной последовательности, которая сформирована на основе соответствующих им тактик, взаимосвязи между которыми можно увидеть в табл. 1.

Таблица 1

Взаимосвязи между тактиками Mitre Attack

Текущая тактика	Следующая тактика	Описание
СТАРТ	Разведка	Атакующий начинает с разведки
	Первоначальный доступ	Атакующий сразу пытается получить доступ к системе, предполагая наличие минимальной информации о цели
	Выполнение	Атакующий запускает вредоносный код на целевой системе без явного этапа получения доступа
	Получение учетных данных	Атакующий начинает с попыток добычи учетных данных, предполагая, что у него есть базовая информация о структуре системы или пользователях
Разведка	Подготовка ресурсов	На основе собранной информации атакующий готовит необходимую инфраструктуру
	Первоначальный доступ	Атакующий использует собранную информацию первоначального доступа
	СТОП	Атакующий завершил разведку
Подготовка ресурсов	Первоначальный доступ	Подготовленная инфраструктура используется для реализации начального доступа к целевой системе
	СТОП	Подготовка ресурсов завершена, но атакующий сменил цель
Первоначальный доступ	Выполнение	После получения доступа атакующий запускает вредоносный код
	Закрепление	Атакующий закрепляется в системе сразу после получения доступа
	СТОП	После получения доступа атака остановлена
Выполнение	Повышение привилегий	После запуска вредоносного кода атакующий пытается повысить свои привилегии для расширения возможностей внутри системы
	Предотвращение обнаружения	Запущенный код модифицируется или маскируется для обхода систем безопасности
	СТОП	Вредоносный код выполнен, атака достигла цели

Продолжение табл. 1

Текущая тактика	Следующая тактика	Описание
Закрепление	Повышение привилегий	Используя механизмы закрепления, атакующий пытается получить более высокие привилегии
	Предотвращение обнаружения	Механизмы закрепления адаптируются для скрытия от антивирусов и систем обнаружения вторжений
	Обнаружение	После закрепления атакующий начинает исследование системы, чтобы найти дополнительные возможности для перемещения или добычи данных
	СТОП	После закрепления в системе атака остановлена, так как атакующий сменил цель
Повышение привилегий	Перемещение внутри периметра	С повышенными правами атакующий получает возможность перемещаться по внутренней сети
	Получение учетных данных	Высокие привилегии позволяют атакующему добраться до защищённых хранилищ учетных данных
	Предотвращение обнаружения	Атакующий использует свои полномочия для отключения систем мониторинга, изменения журналов событий или установки доверенных модулей
	СТОП	Привилегии повышены, операция временно прекращена до подходящего момента
Предотвращение обнаружения	Закрепление	Для обеспечения долгосрочного доступа атакующий использует скрытые или легитимные методы закрепления, чтобы избежать обнаружения
	Повышение привилегий	Атакующий использует обход защиты для выполнения действий, направленных на повышение привилегий
	Обнаружение	Атакующий продолжает исследование системы, используя техники, которые трудно обнаружить
	СТОП	Техники уклонения успешно применены, атака остановлена
Обнаружение	Получение учетных данных	Во время исследования атакующий находит места хранения учетных данных
	Перемещение внутри периметра	Полученная информация о системе, пользователях и сетевых соединениях позволяет атакующему двигаться дальше по инфраструктуре
	Сбор данных	Атакующий начинает собирать данные, найденные во время исследования
	СТОП	Исследование системы завершено, операция остановлена, для продажи данных
Получение учетных данных	Перемещение внутри периметра	Полученные учетные данные используются для доступа к другим системам или сервисам в рамках внутренней сети
	Сбор данных	Учетные данные собираются и сохраняются для дальнейшего использования или передачи
	СТОП	Добыча учетных данных завершена, атака остановлена для продажи данных

Окончание табл. 1

Текущая тактика	Следующая тактика	Описание
Перемещение внутри периметра	Обнаружение	При перемещении по сети атакующий исследует новые системы, службы и пользовательские данные
	Сбор данных	Атакующий собирает данные с новых систем, к которым получил доступ после перемещения
	Предотвращение обнаружения	Атакующий использует скрытные способы перемещения, чтобы избежать обнаружения
	СТОП	Перемещение по сети завершено
Сбор данных	Организация управления	Собранные данные отправляются на удалённый сервер управления (C2)
	Перемещение внутри периметра	Собранные данные используются для планирования следующих этапов перемещения по сети
	СТОП	Сбор данных завершён, атака остановлена для реализации данных
Организация управления	Эксфильтрация данных	Через канал управления (C2) атакующий начинает извлечение данных из сети
	Предотвращение обнаружения	Атакующий использует сложные или легитимные C2-каналы, чтобы избежать блокировки или обнаружения
	СТОП	Канал управления временно не используется, атака остановлена
Эксфильтрация данных	Деструктивное воздействие	После извлечения данных атакующий наносит ущерб: шифрует данные, изменяет их или полностью удаляет для максимального деструктивного воздействия
	Организация управления	Атакующий продолжает использовать C2-канал для контроля над системой и координации дальнейших действий
	Сбор данных	Продолжается сбор данных для дальнейшего извлечения или анализа
	Перемещение внутри периметра	Атакующий перемещается по сети, чтобы найти дополнительные данные для извлечения
	СТОП	Извлечение данных завершено, атака остановлена
Деструктивное воздействие	Обнаружение	После нанесения ущерба атакующий снова исследует систему, чтобы понять, какие данные были затронуты или какие последствия вызвало воздействие
	Сбор данных	Атакующий собирает информацию о результате воздействия
	Предотвращение обнаружения	Атакующий маскирует последствия воздействия, чтобы избежать обнаружения или восстановления системы
Деструктивное воздействие	Закрепление	После воздействия атакующий оставляет точки закрепления для повторного доступа, если система будет восстановлена
	СТОП	Атака завершена после ненанесения ущерба
СТОП	-	Конечная точка атаки

Поиск сценариев ведется через поиск всевозможных путей в графе от узла СТАРТ до узла СТОП. Вероятность бесконечных циклов избегается путем применения пороговых значений вероятности реализации сценария. Вероятность сценария, в свою очередь, рассчитывается по формуле:

$$P_{\text{сценар.}} = P_{T_1} \times \prod_{i=2}^{N} P_{T_i} \times W_{T_{i-1} \to T_i},$$

где N – количество техник в сценарии.

Нормированный риск сценария же определяется как сумма произведений нормированного риска техники во время ее выполнения на вероятность сценария в момент, когда, эта техника была последней техникой этого сценария:

$$Risk_{\text{сценар.}} = \sum_{i=1}^{N} Risk_{T_i} * P_{\text{сценар.}i},$$

где N – количество техник в сценарии.

В результате получены наиболее опасные сценарии, с наибольшим суммарным риском, которые можно увидеть на рис. 11:

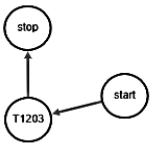
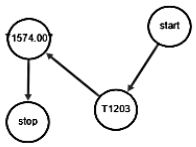
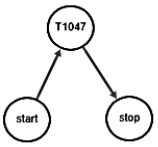
Сценарий	Риск для конфиденциальности	Риск для целостности	Риск для доступности	Общий риск	Граф сценария
сценарий_2	0.04505	0.04316	0.04298	0.13119	
сценарий_11	0.01614	0.01368	0.01376	0.04358	
сценарий_3	0.01343	0.0135	0.01306	0.04	

Рис. 11. Сценарии кибератаки

При нажатии на узел техники конкретного сценария становится доступным список уязвимостей, которые могут быть поэксплуатировать данной техникой.

3. Динамическая генерации мер противодействия кибератакам

Для наиболее эффективного противодействия возникающим кибератакам особую важность имеет подход в разработке комплексных мер противодействия кибератакам, которые охватывают различные фазы жизненного цикла инцидента. Всего выделяется три базовых свойства защиты информации:

- меры обнаружения – действия, которые должны быть направлены на своевременное выявление кибератак в информационных системах. Целью данных мер является обеспечение максимально раннего реагирования на кибератаки для минимизации ущерба,
- меры реагирования – действия, которые предпринимаются после обнаружения инцидента, данные меры направлены на наиболее быструю минимизацию ущерба и предотвращение дальнейшего развития сценария кибератаки,
- меры ликвидации последствий – действия, которые направлены на восстановление нормального функционирования систем и минимизацию

негативных последствий кибератаки. Эти меры важны в процессе повышения устойчивости системы к будущим атакам.

Для качественной генерации мер противодействия кибератакам был разработан подход, основанный на анализе существующих данных о мерах противодействия, содержащихся в патчах к уязвимостям и рекомендациях сообщества информационной безопасности, а также гибкой адаптации существующих патчей ко всем остальным уязвимостям, а именно были предприняты следующие шаги к достижению задачи:

- была создана обобщённая база данных, включающая информацию о мерах противодействия, которые ранее применялись для устранения последствий различных уязвимостей. Эти данные были собраны из открытых источников, так NVD (National Vulnerability Database) и отчёты CERT.

- за основу генератора мер противодействия была взята модель на основе CySecBERT, которая используется для анализа уязвимостей и патчей на основе семантического соответствия описания типовой уязвимости из базы данных мер противодействия кибератакам с другими уязвимостями в графе.

На рис. 12 показан пакет сгенерированных мер противодействия для определенной CVE.

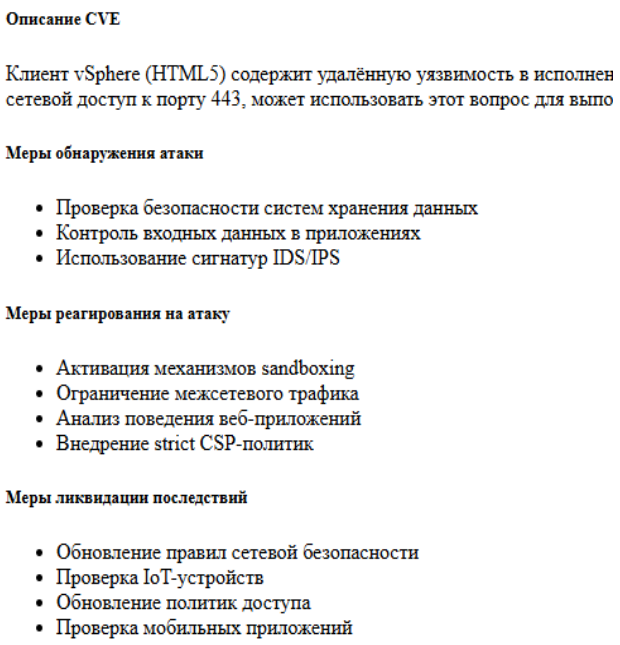


Рис. 12. Пакет мер противодействия для CVE

Заключение

В результате выполненной работы была получена система генерации мер противодействия кибератакам, способная адаптироваться к быстро изменющемуся киберландшафту, используя достижения в области машинного обучения, а также гибкую графовую базу данных, польза которой также заключается в исследовательской ценности, так как данная графовая модель охватывает все абстрактные уровни кибератаки, что позволяет не только оценивать риски в реальном времени, но и изучать эволюцию кибератак вплоть до предсказания новых тенденций в развитии атак на автоматизированный информационные системы.

Список литературы

1. Киберугрозы в первом квартале 2025: глобальные тенденции и фокус на Россию. URL: https://www.forus.ru/about/news/kiberugrozy-v-pervom-kvartale-2025/?ysclid=mb5cjgo34703253661 (дата обращения 06.05.25).

2. Модели BERT для машинного обучения. URL: https://habr.com/ru/companies/skillfactory/articles/862130/ (дата обращения 07.05.25).

3. Markusbayer/CySecBERT. URL: https://huggingface.co/markusbayer/CySecBERT (дата обращения 07.05.2025)

4. CVE. URL: https://cve.mitre.org/ (дата обращения 07.05.25).

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

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

7. Exploit Prediction Scoring System (EPSS). URL: https://www.first.org/epss/ (дата обращения 08.05.25).

8. Каталог KEV / CISA. URL: https://www.cisa.gov/resources-tools/resources/kev-catalog (дата обращения 08.05.25).

9. CWE. URL: https://cwe.mitre.org/index.html (дата обращения 10.05.25).

10. CAPEC. URL: https://capec.mitre.org/ (дата обращения 10.05.25).

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 17.05.2025

Информация об авторах

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

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

Кондратьев Максим Витальевич – студент, Воронежский государственный технический университет, e-mail: mkondratev77@gmail.com

Малежик Юлия Михайловна – студентка, Воронежский государственный технический университет, e-mail: juliamihailovna2003@mail.ru

Герасимова Дарья Николаевна – студентка, Воронежский государственный технический университет, e-mail: dashka20.0615@gmail.com

RISKS OF IMPLEMENTATION OF CYBER-ATTACKS: GRAPHIC FORMALIZATION OF RISK ANALYSIS

G.A. Ostapenko, A.A. Ostapenko, M.V. Kondratyev, Yu.M. Malezhik, D.N. Gerasimova

The main idea of the article is that it is necessary to develop a methodology and implement systems for automated generation of measures and scenarios to counter cyberattacks based on graph analysis. In addition, the software implementation of the proposed system is considered, which includes the automation of the generation of measures and scenarios to counter cyberattacks and the development of algorithms for dynamic risk analysis and an algorithm for dynamic generation of countermeasures. The results of the study are aimed at increasing the resilience of information systems to constantly evolving threats, as well as reducing the time of detection and response to emerging cybersecurity incidents.

Keywords: cyber attack, modeling, vulnerabilities, risk analysis, graph model.

Submitted 17.05.2025

Information about the authors

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

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

Maxim V. Kondratiev – student, Voronezh State Technical University, e-mail: mkondratev77@gmail.com

Yulia M. Malezhik – student, Voronezh State Technical University, e-mail: juliamihailovna2003@mail.ru

Daria N. Gerasimova – student, Voronezh State Technical University, e-mail: dashka20.0615@gmail.com