ОБЗОР ИСПОЛЬЗОВАНИЯ ГРАФИЧЕСКИХ МОДЕЛЕЙ ДЛЯ АНАЛИЗА СИСТЕМ БЕЗОПАСНОСТИ В ЭЛЕКТРОЭНЕРГЕТИКЕ

Джазыбаева А.А. Email: Jazybayeva1168@scientifictext.ru

Джазыбаева Алтынай Аманберлеевна – магистрант,
факультет информационных технологий,
Евразийский национальный университет им. Л.Н. Гумилева,
и.о. главного эксперта,
Комитет информационной безопасности
Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан,
г. Алматы, Республика Казахстан

Аннотация: *данный обзор представляет совокупность графических моделей для анализа рисков, идентификации уязвимостей и исследования динамики эксплуатации уязвимостей в системе, указывает на необходимость нивелирования рисков для обеспечения устойчивости систем. Настоящаая работа разделена на пять частей. В первой части показывается актуальность исследования, во второй части демонстрируется модель по анализу устойчивости и восстанавливаемости электрической сети, в третьей части дается анализ графов сетевых атак, а именно байесовских графов атак, в четвертой части рассматриваются методы запутывания сетевых атак и в финальной части делается общий вывод.*
Ключевые слова: *идентификация и нивелирование рисков, устойчивость системы, байесовские графы атак, вероятностные графические модели.*

REVIEW OF GRAPHICAL MODEL USAGE FOR ANALYSIS OF SYSTEM SECURITY IN THE ELECTRIC POWER INDUSTRY

Jazybayeva A.A.

Jazybayeva Altynay Amanberleevna – Master Student,
FACULTY OF INFORMATION TECHNOLOGY,
L.N. GUMILYOV EURASIAN NATIONAL UNIVERSITY,
Acting Senior Expert,
INFORMATION SECURITY COMMITTEE
MINISTRY OF DIGITAL DEVELOPMENT, INNOVATION AND AEROSPACE INDUSTRY OF THE REPUBLIC OF KAZAKHSTAN,
ALMATY, REPUBLIC OF KAZAKHSTAN

Abstract: *this review presents a set of graphical models for risk analysis, identification of vulnerabilities and research of the dynamics of vulnerabilities exploitation, and indicates the necessity to mitigate risks in order to enhance resilience of systems. This work is divided into five parts. In the first part, the actuality of the work is shown. In the second part, the model for analyzing the resilience of the electric network is demonstrated. In the third part, analyses of network attack graphs, namely Bayesian attack graphs, are made. In the fourth part, methods of obfuscating network attacks are considered, and in the final part, general conclusion is provided.*
Keywords: *identification and mitigation of risks, resilience of systems, Bayesian attack graphs, probabilistic graphical models.*

УДК 004.942

1. Актуальность

Модели и методы симулирования представляют интерес с точки зрения анализа защищенности систем, понимания и выявления уязвимостей и угроз, исследования динамики развития атак, построения и усиления проактивных систем защиты, и могут быть полезны сетевым администраторам, пентестировщикам, программистам, специалистам по компьютерной криминалистике и сотрудникам служб безопасности и реагирования на киберинциденты.

Подходы к анализу систем критической инфраструктуры, включающие моделирование и симулирование, выражают различные точки зрения на безопасность [1, с. 1].

Моделирование и симулирование обеспечивают методами анализа динамики элементов критической инфраструктуры, используя характеристики, функции, операции и поведение различных подсистем критической инфраструктуры, при этом идентифицируя и управляя сопутствующими рисками [1, с. 2].

Взаимозависимость - это состояние, создаваемое прямой и косвенной взаимосвязанностью критически важной инфраструктуры посредством территориально-распределенной сети и каналов аппаратного обеспечения.

Так как кибератаки могут вызвать каскады и неисправности и могут иметь экономические последствия, то необходимо иметь хорошо оборудованные средства мониторинга и инструменты реагирования и восстановления. Соответствующая готовность требуется, чтобы предугадать и минимизировать уязвимости, предотвратить усиление и распространение неисправностей и их воздействия на критическую инфраструктуру. Полный контроль всех динамических угроз невозможен, как невозможно предсказать, предотвратить и подготовиться ко всем инцидентам, поэтому во избежание кризисной ситуации необходимо направить усилия на предупреждение, сопротивление, амортизацию и восстановление безопасности.

Для анализа систем защиты и предотвращения кризиса безопасности необходимо рассмотреть неотъемлемые зависимости и потенциальные каскады отказов, поскольку нереально защититься от всех угроз.

2. Устойчивость электрической сети США

Северо-Американская электрическая сеть - одна из самых сложных и взаимосвязанных технологических сетей, которая производит и передает электроэнергию на оптовый рынок. Спрос на передачу электроэнергии постоянно растет и модели генерирования (производства) электроэнергии смещаются. Электрическая сеть способна передавать электроэнергию на сотни миль, и в то же время неполадки из-за перенагрузок могут распространяться в ней, вызывая эффект каскада [2, с. 101].

В данном исследовании для моделирования использовалась актуальная топология Северо-Американской электрической сети, а именно 14099 подстанций и 19657 линий передач. Используемые подстанции были трех типов: 1633 генерирующих подстанций по производству электроэнергии, 10287 трансмиссионных подстанций, передающих электроэнергию вдоль высоковольтных линий, и 2179 дистрибьюторских подстанций, распределяющих электроэнергию небольшим местным сетям [2, с. 102].

Электрическая сеть моделировалась как взвешенный граф, где подстанции были узлами (вершинами) графа, а высоковольтные линии были ребрами графа. Элементы матрицы смежности графа означали эффективность ребра или равнялись нулю, если не было линии между двумя узлами (подстанциями) [2, с. 102].

Мощность каждого узла (подстанции) была прямо пропорциональна начальной нагрузке (посредничеству), т.е. мощность рассчитывалась как произведение начальной нагрузки (посредничества), умноженное на толерантность [2, с. 103].

Северо-Американская электрическая сеть продемонстрировала разнородную топологию, вершины которой обнаружили экспоненциальное распределение линий передач на вершину (распределение вершин) и распределение нагрузки узлов по обобщенному степенному закону. Топология электрической сети заняла промежуточное положение между случайными графами Эрдёша-Реньи с биномиальным распределением вершин и экспоненциальным распределением нагрузки и безмасштабыми сетями (масштабно-инвариантными сетями), вершины которых распределены по степенному закону и распределением нагрузки по степенному закону [2, с. 104].

Известно, что однородные сети и случайные графы не особенно подвержены к случайным неполадкам или неполадкам из-за нагрузок, в то время как безмасштабные (масштабно-инвариантные) сети уязвимы перед каскадом в связи с потерей узлов с высокой нагрузкой. Электрическая сеть при интервале изменчивого количества линий передач на подстанцию проявляет динамическую уязвимость подобно безмасштабным сетям [2, с. 104].

При моделировании предположили, что генерирующая подстанция может переносить электроэнергию всем дистрибьюторским подстанциям по линиям передачи. Для упрощения допустили, что электрический ток течет по самому эффективному (короткому) пути [2, с. 103].

В работе применили динамический подход модели Crucitti-Latora-Marchiori [3], когда отслеживалась динамическая реакция системы к перенагрузкам, изучалось, какие последствия неполадка имела в сети, и как перераспределение нагрузки в сети распространялось [2, с. 103].

Симулирование неполадки в сети означало удаление узла из сети, затем перераспределение нагрузки между другими узлами/ребрами и мониторинг прогресса у загруженных узлов. Если толерантность (резервная мощность) была маленькая, то эффективность сети падала из-за перенагруженности узлов сети вследствии эффекта каскада. Если толерантность (резервная мощность) была высокая или средняя, то эффективность сети принимала первоначальное или меньшее значение, и стабилизировалась в устойчивом состоянии, возможно после нескольких осцилляций [2, с. 103].

В симулировании использовались две схемы прогресса перенагрузки узлов: удалялся один узел или несколько узлов последовательно, причем узлы выбирались случайные или с наибольшей нагрузкой [2, с. 104].

Северо-Американская электрическая сеть показала, что устойчива к случайным неисправностям. В то же время оказалось, что устойчивость электросети зависит от топологии. Эффективность электрической сети больше всего оказывалась под воздействием, когда удалялись узлы с высокой степенью вершины и с высокой степенью посредничества, т.е. когда удалялись генерирующая или передающая станции с самыми высокими нагрузками [2, с. 104].

Мерами по повышения устойчивости и эффективности электрической сети являются построение большего числа передач и подстанций, контроль распространения каскада и обеспечение информационной безопасности.

3. Графы атак

В работе [4, с.1] дается систематическое исследование методов анализа графов атак с точки зрения обработки данных и знаний. Администраторы могут симулировать пути атак с помощью графов атак для оценки безопасности сети и прогнозирования возможных сетевых атак.

Графы атак – это проактивные формальные методы расчета стратегий защиты, нахождения решений и контрмер. Графы атак показывают пути злоумышленника, использующего последовательности уязвимостей и сетевых подключений [5, с.1].

Предложенные в 1997 году, графы атак широко используются, поскольку подробно описывают процесс и поведение сетевых атак. Пути сетевых атак и узлы могут быть описаны посредством графов.

Направленный ациклический граф может представлять абстрактную топологию сети с изображением узлов, путей и последовательности сетевых атак. Каждый узел может указывать либо на хост, либо на уязвимость, либо на устройство [4, с.1].

Структура исследования графов атак состоит из четырех этапов:

1) сбор информации о сети;

2) генерация графа атак;

3) метод анализа:

а) соответствие модели графа атак,

б) вычислениеи анализ безопасности,

4) приложения [4, с. 2].

Генерирование графа атак состоит из трех шагов: анализ достижимости, выбор шаблона атаки, построение графа атаки. Крупномасштабные графы атак требуют уменьшения сложности и времени построения графов, включая сокращение пути, сжатие свойств сетей [4, с. 2].

Чтобы выявить слабые места сетевой безопасности, необходимо провести анализ уязвимостей сети, выбрать усиление безопасности узлов, спрогнозировать пути атак и провести анализ неопределенности.

При анализе уязвимостей в первую очередь рассматривается анализ возможных путей атаки, а также защита узлов высокого риска. Вторая задача связана с анализом поведения атаки, прогнозированием следующей цели и поиском контрмер [4, с. 4].

Для усиления сети необходимо определить, какие узлы следует укрепить, рассчитать затраты и выгоды, выбрать методы защиты сети.

При прогнозировании пути атаки предполагается систематичность сетевой атаки и прослеживаемость уязвимости и пути атаки. С развитием технологий сетевой безопасности и корпоративных сервисов, необходимо определить наиболее вероятные пути атак и обновить механизм защиты против атак. Следовательно, требуется проведение анализа неопределенности в отношении проблем безопасности, вызванных конфигурацией сети [4, с. 4].

3.1 Байесовские графы атак

В работе [5] байесовские сети применяются для моделирования графов атак с использованием статического анализа для оценки безопасности в состоянии покоя, и динамического анализа для реагирования на потенциальные угрозы. Описывается эксперимент симуляции с использованием байесовского графа атак с тысячами узлами и с выполненными точными и приближенными методами вывода (*inference*).

Статический анализ оценивает априорные риски сети безопасности в состоянии покоя и помогает улучшить топологию сети. Динамический анализ исправляет эти риски, получая информацию от Системы управления информацией и событиями безопасности (SIEM) и Систем обнаружения вторжений (IDS) о скомпрометированных сетевых компонентах [5, с. 2].

Поскольку статический и динамический анализ требуют вычисления безусловных и апостериорных вероятностей, которые являются NP-трудными проблемами, соответсвенно, были применены эффективные методы вывода.

Точные и приближенные алгоритмы вывода (inference) были выполнены для проведения статических и динамических анализов байесовскихграфов атак (BAG) на кластерной структуре крупных корпоративных сетей с тысячами узлов [5, с. 2].

В этом исследовании предполагается, что граф атак описывается направленным ациклическим графом и использует принцип монотонности, подразумевая, что злоумышленник никогда не откажется от привилегий, которые он получил. Байесовская сеть вычисляет вероятность того, что злоумышленник достиг состояния безопасности в графе атак. Узлы в байесовском графе атак (BAG) показывают возможные состояния безопасности. Эти состояния определены как случайные величины Бернулли [5, с. 3].

Метрики CVSS учитываются при оценке вероятности использования уязвимостей, что необходимо для создания двух типов условных таблиц вероятностей: AND, OR [5, с. 4].

В обоих типах таблиц условных вероятностей коэффициент утечки представляет случаи, когда все предварительные условия являются ложными, при этом существует либо ненулевая вероятность уязвимости, либо вероятность ложной тревоги системы корреляции сигналов тревоги [5, с. 4].

При статическом анализе BAG для всех узлов безусловные вероятности достижения злоумышленником заданного состояния безопасности рассчитываются как оценка риска либо для усиления сети, либо для использования статических методов снижения риска.

При динамическом анализе BAG для всех узлов сети, за исключением набора узлов для которых приведены свидетельства атак по сигналам от системы корреляции сигналов тревоги, вычисляются апостериорные вероятности для переоценки рисков, что может оказаться полезнымадминистраторам для определения приоритетов мер безопасности при продолжающейся атаке.

Поскольку точные вычисления безусловной и апостериорной вероятностей для статического и динамического анализов представляют собой NP-трудные задачи, поэтому целесообразно применить алгоритм Variable Elimination (VE) и алгоритм Junction Tree (JT) [5, с.6].

Хотя BAG имеет кластерной структуру сети и ограниченное число путей атаки, тем не менее алгоритм Junction Tree (JT) работает лучше, чем алгоритм Variable Elimination (VE), и поэтому был выбран для проведения статического и динамического анализов для графов с несколькими тысячами узлов.

Приближенный вывод (inference) в байесовских сетях также является NP-трудной задачей для расчета безусловных и апостериорных вероятностей статического и динамического анализов [5, с. 6].

Алгоритм Loopy Belief Propagation (LBP) со случайными переменными Бернулли требует O(N) времени, где N - количество узлов, а s называется областью действия наибольшего фактора, равного максимальному числу родительских узлов которое может иметь узел в графе, и предполагаетсянебольшим.

Приблизительные оценки безусловных и апостериорных вероятностей LBP полезны, даже если вероятности использования уязвимостей являются грубыми из-за использования оценок CVSS [5, с. 7].

Программное обеспечение Bayes Nettoolbox для Matlab использовалось для проведения алгоритмов LBP и JT для статического и динамического анализов BAG.

Поскольку эмпирически полученных графов атак не было, поэтому были получены синтетические графы атак.

Были сгенерированы 20 независимых графов для каждого значения кластеров с размерами 20 и 50 и с 3 родителями.

По результатам эксперимента обнаружено:

1) Алгоритм JT хорошо работает для динамической оценки рисков безопасности, но экспоненциально масштабируется для статического анализа.

2) Алгоритм LBP масштабируется линейно для статического и динамического анализов.

3) Хотя алгоритм LBP работает медленнее чем алоритм JT для динамического анализа, алгоритм LBP отслеживает значения апостериорных вероятностей на каждой итерации и дает точные оценки апостериорных вероятностей до того как сходится [5, с. 9].

Графы атак ограничены топологией сети и уязвимостями программного обеспечения, что необходимо учитывать в средах IoT, и принимать во внимание кибернетические, человеческие и физические уязвимости при защите сетей [5, с. 10].

4. Анализ последовательностей запутанных кибератак

Важным свойством защиты компьютерных сетей является умение распознавать типы кибератак по наблюдаемым вредоносным действиям. Запутанность наблюдаемой последовательности атак введет к

ошибочному толкованию результата и намерений, что создаёт неэффективную защиту и развертывание восстановления [6, с. 1].

Работа [6] предложила вероятностные графические модели для обобщения методов запутывания атак и анализа Вероятной Точности Классификации *(Expected Classification Error)* по результатам использования методов запутывания на различные модели атак. Вычисление Вероятной Точности Классификации (ВТК) является NP-трудной проблемой вследствии комбинаторного числа возможностей. Данная работа представила несколько алгоритмов с полиномиальным временем решения нахождения теоретически ограниченной аппроксимации ВТК для различных запутанных моделей атак [6, с. 1].

Разработанный набор вероятностных графических моделей показал как кибератаки могут обнаруживаться без и с применением методов удаления, внедрения, и изменения. Представленные модели позволили формально проанализировать влияние методов запутывания правильно классифицировать наблюдаемую последовательность атакуемых действий как если бы не было запутывания [6, с. 1].

В данном исследовании модель атаки была представлена как Марковская модель, точнее как Скрытая Марковская Модель (*Hidden Markov Mode)*, для описания возможных действий атаки и случайных отношений действий атак использовались вероятности перехода. Последовательность атаки определялась как вектор случайных переменных, где каждое наблюдение являлось образцом (выборкой) модели атаки. Совместное распределение использовалось для описания последовательности атаки и метода запутывания [6, с. 2].

Применили два типа запутывания последовательности атак [6, с. 2]:

К первому типу запутывания отнесли модель изменения последовательности атаки, в которой чистая последовательность атаки и зашумленная последовательность имели одинаковые длины.

Ко второму типу запутывания отнесли методы внедрения и удаления последовательности атак, при которых чистые атаки и зашумленные последовательности атак имели различные длины.

В обобщенном методе запутывания применили Скрытую Марковскую Модель (СММ), где наблюдаемое событие зависело от соответствующих скрытых состояний, и добавился дополнительный параметр для оценки процента действий атак, которые атакующий может изменять; Скрытые Марковские Модели (СММ) были второго и более высокого порядков [6, с. 3].

Формальная метрика задавалась, чтобы оценить Вероятную Точность Классификации (ВТК) основываясь на концепции Байесовской ошибки. Чтобы вычислить вероятное число с экспоненциально большим числом сценариев, представленная работа разработала эффективные алгоритмы основанные на динамическом программировании (расширенный алгоритм передачи сообщения - *Extended Message Passing Algorithm*) и использовала метод выборок Монте-Карло для вычисления приближенного вывода [6, с. 3].

Комплексная симуляция различных комбинаций моделей атак и методов запутывания показала эффекты, оказываемые на ВТК с изменением, внедрением, удалением последовательности атаки, увеличением длины наблюдения, уровня запутанности и сложности модели [6, с. 1].

В процессе симулирования применили 4 модели атак (четыре стратегии) и 5 методов запутывания. Чистые последовательности атак генерировались из моделей атак. Комбинации последовательности атаки различных моделей соединялись с методами запутывания. [6, с. 7].

Сетевая схема эксперимента была представлена небольшой сетью предприятия с 5 подсетями, 11 серверами и 4 кластерами хостов, дающими в общем числе 24 хоста. Вся сеть имела 31 открытый сервис 15 типов, соединенный посредством 4 маршрутизаторов [6, с. 7].

В данной работе использовались 15 классических действий атак пяти категорий, взятых из перечня общих образцов и классификаций MITRE [7] [6, с. 9].

Для нахождения приближенной оценки ВТК с помощью алгоритма Монте-Карло в эксперименте использовалось 30000 выборок [6, с. 6].

Результаты работы выявили действия следующих факторов, изменивших эффект воздействия методов запутанности на распознавание моделей атак. Согласно эксперименту точность классификации ВТК улучшилась при увеличении длины наблюдения и при уменьшении запутанности атаки. Запутанность атаки сильнее воздействовала с увеличением сложности модели, тем не менее (inference) алгоритм больше восстанавливал [6, с. 11].

5. Вывод

В работе представлены графические модели и описаны сопутствующие эксперименты симулирования для нахождения уязвимостей сетевой инфраструктуры электроэнергетики. Работа призвана показать графические модели, лежащие в основе идентификации уязвимостей и угроз безопасности систем, и указывает на необходимость осознания и принятия контрмер по усилению защищенности и нивелированию рисков безопасности.

Отмечается, что для эффективной защиты критической инфраструктуры необходимо разрабатывать направления защиты, направленные на поддержку непрерывной и устойчивой работы развивающейся инфраструктуры.

Список литературы / References

1. *Ani U.D., Watson J. D McK., Nurse J. R.C. Cook A., Maple C.* A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape. PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT-2019.
2. *Kenney R., Crucitti P., Albert R., Latora V.* Modeling cascading failures in the North American power grid, The European Physical Journal B 46, 101-107, 2005.
3. *Crucitti P., Latora V., Marchiori M.* Model for cascading failures in complex networks Physical Review E, Vol. 69. Issue 4, 2004.
4. *Zeng J., Wu S., Chen Y., Zeng R., Wu C.* "Survey of Attack Graph Analysis Methods from the Perspective of Data and Knowledge Processing", Hindawi, Security and Communication Networks, Vol. 2019. [Электронный ресурс]. Режим доступа: https://doi.org/10.1155/2019/2031063/ (дата обращения: 01.01.2020).
5. *Mu˜noz-Gonz´alez L., Lupu E.C.* "Bayesian Attack Graphs for Security Risk Assessment", IST-153 Workshop on Cyber Resilience, 2017.
6. *Du H., Yang S.* Probabilistic modeling and inference for obfuscated cyber attack sequences IEEE Transactions on emerging topics in computing, Special issue, Sep 2018. [Электронный ресурс]. Режим доступа: http://arXiv: 1809.0156.01562v1 [cs.CR],[Online], (дата обращения:01.01.2020).
7. Common Attack Pattern Enumeraion and Classification. Access Date: Aug 2013 [Online]. [Электронный ресурс]. Режим доступа: http://capec.mitre.org./ (дата обращения: 27.04.2020).