

МОДЕЛЬ ПРОЦЕССА РЕАЛИЗАЦИИ КИБЕРАТАКИ «СКАНИРОВАНИЕ СЕТИ И ЕЁ УЯЗВИМОСТЕЙ» НА СЕТЕВЫЕ ЭЛЕМЕНТЫ БАНКОВСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Бекбаев Гамзатдин Алеуатдинович

PhD, доцент кафедры «Финансы и цифровая экономика», Ташкентский государственный
экономический университет
ORCID: 0009-0002-3523-3819

Аннотация – В настоящей статье осуществлено моделирование процесса реализации компьютерной атаки «Сканирование сети и ее уязвимостей», рассматриваемого как один из ключевых этапов компьютерной разведки, предшествующего дальнейшим действиям нарушителя в отношении информационно-телекоммуникационной инфраструктуры банковской информационной системы. Основной задачей моделирования являлось получение вероятностно-временных характеристик исследуемого процесса и определение влияния отдельных операций на общую продолжительность разведывательного цикла. На первом этапе было выполнено структурное описание процесса компьютерной атаки, в рамках которого выделены основные последовательные и параллельные операции, связанные с обнаружением сетевых элементов, анализом сетевой структуры, сканированием доступных сервисов и оценкой потенциальных уязвимостей. Для каждой операции определялись ее продолжительность, вероятность успешного выполнения, а также возможность повторного выполнения в случае получения отрицательного результата. Такой подход позволяет учитывать стохастический характер исследуемого процесса и различия в условиях функционирования сетевой инфраструктуры. При математическом описании модели использовались уравнение Мейсона и преобразование Лапласа-Стилтьеса. Полученная эквивалентная функция позволяет представить сложный процесс в математической форме и использовать ее для дальнейшего определения вероятностно-временных характеристик. Особое внимание уделено определению функции распределения времени реализации компьютерной атаки. Для получения функции распределения применяется метод обращения преобразования Лапласа-Стилтьеса. В результате определяется зависимость вероятности завершения исследуемого процесса от времени его выполнения. Это позволяет не ограничиваться расчетом только среднего времени, а получить более полную характеристику процесса, включая вероятность его завершения в заданный момент времени, среднюю продолжительность и особенности распределения времени выполнения. Разработанная модель может использоваться не только для оценки характеристик процесса компьютерной разведки, но и для комплексного анализа защищенности банковских информационных систем: выявления потенциально уязвимых этапов, определения критических участков сетевой инфраструктуры и обоснования мероприятий, направленных на повышение устойчивости системы к компьютерным атакам.

Ключевые слова: компьютерная разведка; компьютерная атака; информационно-телекоммуникационная сеть; стохастическая модель; эквивалентная функция; преобразование Лапласа–Стилтьеса; уравнение Мейсона; гамма-аппроксимация; функция распределения времени; среднее время реализации.

ВВЕДЕНИЕ

Сканирование сети и выявление её уязвимостей являются одними из начальных этапов компьютерной разведки, предшествующей возможной

реализации кибератаки на банковскую информационную систему. Данный процесс направлен на сбор и анализ сведений о структуре сетевой инфраструктуры, составе подключённых устройств, доступных сетевых сервисах, особенностях взаимодействия между отдельными компонентами и наличии потенциальных уязвимостей. Полученная информация позволяет сформировать представление об архитектуре исследуемой системы, определить характерные особенности её функционирования и оценить потенциальные риски информационной безопасности.

Особую значимость данный процесс приобретает в банковском секторе, поскольку информационно-телекоммуникационная инфраструктура банков представляет собой сложную совокупность взаимосвязанных технических и программных компонентов. К ним относятся серверы приложений и баз данных, маршрутизаторы, коммутаторы, межсетевые экраны, системы обнаружения и предотвращения вторжений, рабочие станции сотрудников, системы дистанционного банковского обслуживания, платёжные шлюзы и другие критически важные элементы. Нарушение функционирования хотя бы одного из таких компонентов может привести к ограничению доступности банковских сервисов, нарушению целостности обрабатываемых данных или возникновению угроз конфиденциальности финансовой информации.

С точки зрения моделирования компьютерной разведки данный процесс целесообразно представлять как совокупность последовательных и параллельных операций, каждая из которых характеризуется определённой продолжительностью и вероятностью успешного завершения. На результаты сканирования могут влиять сегментация сети, наличие межсетевых экранов, настройки контроля доступа, активность систем обнаружения вторжений, качество исходной информации и особенности сетевой архитектуры. Кроме того, неуспешное выполнение отдельных операций может потребовать их повторения, что увеличивает общую продолжительность разведывательного цикла.

Для банковских организаций особое значение имеет не только установление самого факта потенциальной доступности сетевого ресурса, но и оценка времени, необходимого для последовательного получения сведений о нём. Защитные средства могут изменять вероятность успешного определения активных узлов, характеристик операционных систем и запущенных сервисов, а также увеличивать количество повторных обращений к объекту исследования. Поэтому исключительно детерминированное описание процедуры сканирования, основанное на суммировании фиксированных длительностей операций, не отражает возможную вариативность её завершения. Для учёта этой вариативности требуется математическая модель, связывающая последовательность действий, вероятности их выполнения и распределение затраченного времени.

Важный методологический вопрос заключается в том, каким образом представить многоэтапный разведывательный процесс так, чтобы учесть возврат к ранее выполненным операциям при отрицательном результате. Сканирование сетевых элементов, определение операционных систем, обнаружение сервисов и

выявление уязвимостей могут иметь неодинаковую длительность, а исход каждого этапа может зависеть от параметров сетевой среды. При этом практическая значимость модели определяется не только вычислением математического ожидания времени, но и возможностью оценивать вероятность завершения процесса в пределах заранее установленного временного интервала. Такой подход позволяет сопоставлять сценарии с различными исходными вероятностями и использовать полученные характеристики для оценки устойчивости инфраструктуры к компьютерной разведке.

Цель исследования — разработать стохастическое описание процесса сканирования сети и её уязвимостей на сетевых элементах банковской информационной системы и определить основные вероятностно-временные характеристики его реализации. Объектом исследования выступает сетевая инфраструктура банковской информационной системы, включающая взаимосвязанные программные и технические компоненты. Предмет исследования составляют вероятностные закономерности выполнения разведывательных операций, повторных попыток и формирования общей длительности процесса. Для достижения цели поставлены задачи: формализовать последовательность операций; построить стохастическую сеть с обратными связями; определить эквивалентную функцию с использованием топологического уравнения Мейсона; вычислить моменты распределения времени и получить его интегральную функцию. Научно-методический вклад работы состоит в объединении сетевой модели операций и вероятностно-временного анализа применительно к рассматриваемому сценарию. Исследование основано на аналитическом моделировании, а не на проведении атаки на действующую банковскую инфраструктуру.

Таким образом, моделирование процесса сканирования сети и выявления её уязвимостей позволяет определить вероятностно-временные характеристики данного этапа компьютерной разведки, оценить влияние отдельных операций на общую продолжительность процесса и исследовать роль защитных механизмов в ограничении возможностей обнаружения сетевых компонентов. Применительно к банковским информационным системам результаты такого моделирования могут использоваться для выявления критически значимых участков инфраструктуры, обоснования мер по повышению сетевой защищённости и совершенствования механизмов противодействия компьютерным атакам.

ОБЗОР ЛИТЕРАТУРЫ

Сканирование компьютерных сетей и выявление уязвимостей являются важными направлениями обеспечения информационной безопасности, поскольку позволяют определить доступные сетевые узлы, обнаружить открытые порты, идентифицировать работающие службы и выявить потенциальные недостатки конфигурации информационных систем. В современной литературе данная проблематика рассматривается в контексте технического тестирования защищённости, управления уязвимостями, анализа

сетевых протоколов и оценки рисков кибератак.

В работе K.Scarfone, M.Souppaya, A.Cody и A.Orebaugh [1] представлены методические основы технического тестирования информационной безопасности. Авторы рассматривают планирование проверок, выбор методов тестирования, анализ полученных результатов и разработку мер по устранению выявленных недостатков. Особое значение имеет системный подход, при котором результаты сканирования интерпретируются не изолированно, а в рамках комплексной оценки защищённости информационной инфраструктуры.

В руководстве National Institute of Standards and Technology (NIST) по оценке информационной безопасности [2] подчёркивается необходимость организации проверок с учётом целей исследования, особенностей тестируемой системы и допустимого воздействия на её работу. Данный подход позволяет рассматривать сканирование не только как техническую операцию, но и как элемент управляемого процесса оценки рисков. Вместе с тем технические средства выявления уязвимостей не гарантируют обнаружения всех возможных недостатков, поэтому результаты автоматизированных проверок требуют дополнительной интерпретации.

В руководстве OWASP Web Security Testing Guide [3] систематизированы методы тестирования безопасности веб-приложений и веб-сервисов. Документ охватывает этапы сбора информации, определения конфигурации, исследования механизмов аутентификации и управления доступом, а также проверки распространённых классов уязвимостей. В отличие от сканирования сетевой инфраструктуры, направленного прежде всего на обнаружение узлов и сетевых служб, тестирование по методологии OWASP ориентировано на анализ защищённости приложений и логики их функционирования.

Практическая сторона сетевого сканирования раскрывается в документации Nmap - одного из распространённых инструментов сетевого обнаружения и аудита. Nmap позволяет определять активные узлы, исследовать состояние портов, идентифицировать сетевые службы и в предусмотренных режимах получать сведения об операционной системе. Применение подобных инструментов повышает оперативность инвентаризации сети, однако точность результатов зависит от настроек сканирования, сетевой фильтрации, доступности узлов и используемых методов обнаружения. Поэтому результаты сканирования следует рассматривать как исходные данные для последующего анализа, а не как окончательное доказательство наличия или отсутствия уязвимости.

Отдельное направление исследований связано с автоматизированным обнаружением и классификацией уязвимостей. В рамках данного направления используются сканеры, сопоставляющие характеристики операционной системы, версий служб и программных компонентов с известными сведениями об уязвимостях. К этой группе относятся Nessus и Greenbone Vulnerability Management (OpenVAS). Их практическая ценность заключается в возможности систематически проверять большое количество узлов и формировать отчёты о потенциальных проблемах безопасности. Однако обнаружение соответствия определённой версии программного обеспечения записи об уязвимости ещё не

означает, что уязвимость реально эксплуатируема в конкретной среде. Для подтверждения необходимы анализ конфигурации, проверка применённых обновлений и оценка условий эксплуатации.

Важное значение для унификации описания обнаруженных недостатков имеет система Common Vulnerabilities and Exposures (CVE) [4]. Она обеспечивает единый идентификатор для публично известных уязвимостей, облегчая обмен информацией между исследователями, разработчиками средств защиты и специалистами по информационной безопасности. В свою очередь, Common Vulnerability Scoring System (CVSS) [5] позволяет стандартизированно описывать характеристики уязвимостей и оценивать их техническую серьёзность. При этом показатель CVSS не следует отождествлять с полным бизнес-риском: приоритизация устранения недостатков должна учитывать критичность конкретного актива, его доступность из сети, ценность обрабатываемых данных и существующие компенсирующие меры защиты.

В работе по формированию методологии управления уязвимостями также необходимо учитывать подходы, отражённые в стандартах и рекомендациях NIST. В частности, руководство по управлению патчами [6] рассматривает обновление программного обеспечения как организационно-технический процесс, направленный на снижение риска эксплуатации известных уязвимостей. С этой точки зрения сканирование сети приобретает практическую ценность тогда, когда его результаты используются для планирования обновлений, назначения ответственных лиц, контроля устранения недостатков и повторной проверки защищённости.

Существенное место в исследованиях занимает анализ сетевого трафика. Документация Wireshark [7] описывает возможности захвата и декодирования сетевых пакетов, позволяющие изучать взаимодействие узлов и протоколов, выявлять ошибки соединений и исследовать отдельные признаки подозрительной активности. В отличие от классического сканирования, которое преимущественно устанавливает доступность узлов и служб, анализ трафика позволяет наблюдать фактический обмен данными в пределах доступной точки захвата. Вместе с тем он не заменяет сканер уязвимостей: зашифрованные соединения, неполный захват пакетов и ограничения сетевого интерфейса могут существенно влиять на полноту анализа.

Дополнительные возможности предоставляет система Zeek [8], предназначенная для анализа сетевой активности и формирования структурированных журналов о соединениях, DNS-запросах, протоколах и событиях безопасности. Такой подход позволяет исследовать не только отдельные пакеты, но и контекст сетевых взаимодействий. Использование журналов Zeek совместно с результатами сканирования может помочь сопоставить потенциально уязвимые службы с наблюдаемой сетевой активностью. При этом обнаружение аномалии не всегда свидетельствует об атаке: необходимы проверка контекста и сопоставление с другими источниками данных.

Вопросы выявления сетевых угроз также рассматриваются в контексте

систем обнаружения вторжений. В работе D. E. Denning [9] предложена модель обнаружения компьютерных вторжений на основе анализа событий и отклонений от ожидаемого поведения системы. Данная работа имеет фундаментальное значение для понимания того, как наблюдаемые характеристики активности могут использоваться для выявления подозрительных действий. В отличие от сканирования, которое помогает определить доступные ресурсы и потенциальные слабые места, системы обнаружения вторжений ориентированы на выявление признаков нежелательной или аномальной активности.

В исследованиях R.Sommer и V.Paxson [10] проанализированы сложности применения машинного обучения для обнаружения вторжений в реальных сетях. Авторы обращают внимание на разрыв между результатами лабораторных экспериментов и требованиями практических систем мониторинга. Данное наблюдение важно и для автоматизированного выявления уязвимостей: использование алгоритмов классификации и корреляции результатов может повысить эффективность анализа, но требует качественных данных, проверки ложноположительных результатов и учёта изменений сетевой среды.

Вопросы построения систематического процесса управления уязвимостями раскрываются также в рекомендациях CIS Controls [11], предусматривающих инвентаризацию активов, управление программным обеспечением, непрерывное выявление уязвимостей и их устранение. Данный подход позволяет связать результаты технического сканирования с постоянным управлением защищённостью организации. В отличие от разовой проверки, регулярное сканирование даёт возможность отслеживать изменения сетевой инфраструктуры, появление новых узлов и устранение ранее обнаруженных недостатков.

Сопоставление рассмотренных подходов показывает различие между техническим обнаружением активов и оценкой временной динамики разведывательного процесса. Руководства NIST, OWASP и CIS Controls [1–3, 11] описывают процедуры проверки и управления защищённостью, тогда как исследования систем обнаружения вторжений [9, 10] сосредоточены на анализе наблюдаемой активности и ограничениях её интерпретации. Для поставленной задачи сохраняется потребность в отдельном вероятностном представлении последовательности сканирования, учитывающем повторные попытки и позволяющем рассчитывать распределение времени завершения. Именно этот аспект рассматривается в настоящей работе.

МЕТОДОЛОГИЯ

Постановка задачи – задана банковская информационная система (БИС) состоящая из n элементов (маршрутизаторы, коммутаторы, серверы и multifunctionальные абонентские терминалы). Злоумышленник совершает компьютерную атаку «Сканирование сети и ее уязвимостей» в следующей последовательности: запуск программно-аппаратного комплекса (сетевого сканера) за среднее время $\bar{t}_{зан}$ с функцией распределения времени $W(t)$. Определение активных элементов атакуемой БИС за среднее время $\bar{t}_{оп. элем}$ с

функцией распределения времени $M(t)$, получается с вероятностью P_n .
 Определение типов операционных систем на активных элементах атакуемой БИС за среднее время $\bar{t}_{on.oc}$ с функцией распределения времени $D(t)$.
 Определение сервисов на элементах атакуемой БИС за среднее время $\bar{t}_{on.serv}$ с функцией распределения времени $L(t)$, получается с вероятностью P_n .
 Определение уязвимостей элементов атакуемой БИС за среднее время $\bar{t}_{on.узв}$ с функцией распределения времени $K(t)$. При этом, если активные элементы БИС, типы операционных систем и сервисы на них не будут определены, то с вероятностью $(1 - P_n)$ сетевой сканер запускается повторно за среднее время $\bar{t}_{повт}$ с функцией распределения времени $Z(t)$.

Решение: Описанный в постановке задачи процесс реализации «Сканирование сети и ее уязвимостей» на сетевые элементы БИС представим в виде стохастической сети, приведенной на рисунке 1.

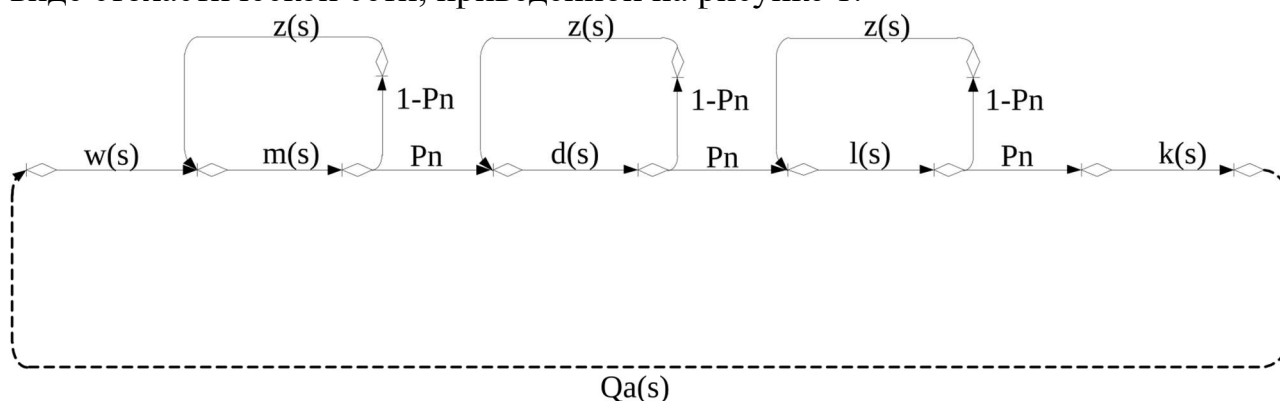


Рисунок 1 – Стохастическая сеть процесса реализации кибератаки «Сканирование сети и её уязвимостей» на сетевые элементы БИС

Предполагая, что функции распределения времени реализации частных процессов относятся к классу экспоненциальных законов, получим (ф.1):

$$\left\{ \begin{array}{l} W(t) = 1 - e^{-wt}; \\ M(t) = 1 - e^{-mt}; \\ Z(t) = 1 - e^{-zt}; \\ D(t) = 1 - e^{-dt}; \\ L(t) = 1 - e^{-lt}; \\ K(t) = 1 - e^{-kt}; \end{array} \right. \quad (1)$$

Применяя преобразование Лапласа, получим (ф.2).

$$\begin{aligned}
 w(s) &= \int_0^{\infty} e^{-st} d[W(t)] = \frac{w}{w+s}; \\
 m(s) &= \int_0^{\infty} e^{-st} d[M(t)] = \frac{m}{m+s}; \\
 z(s) &= \int_0^{\infty} e^{-st} d[Z(t)] = \frac{z}{z+s}; \\
 d(s) &= \int_0^{\infty} e^{-st} d[D(t)] = \frac{d}{d+s}; \\
 l(s) &= \int_0^{\infty} e^{-st} d[L(t)] = \frac{l}{l+s}; \\
 k(s) &= \int_0^{\infty} e^{-st} d[K(t)] = \frac{k}{k+s};
 \end{aligned} \tag{2}$$

Подставляя эти значения в ф.2 соответствующее значение $w(s); m(s); z(s); d(s) \cdot l(s) \cdot k(s)$, получаем окончательный вид эквивалентной функции:

$$w = \frac{1}{t_{\text{зан}}}; m = \frac{1}{t_{\text{оп. элем}}}; z = \frac{1}{t_{\text{повт}}}; d = \frac{1}{t_{\text{оп. ос}}}; l = \frac{1}{t_{\text{оп. серж}}}; k = \frac{1}{t_{\text{оп. уязв}}}.$$

Определим все петли k-го порядка:

Петли первого порядка: $m(s) \cdot (1 - P_n) \cdot z(s); d(s) \cdot (1 - P_n) \cdot z(s); l(s) \cdot (1 - P_n) \cdot z(s);$

$$w(s) \cdot m(s) \cdot d(s) \cdot l(s) \cdot k(s) \cdot P_n^3 \cdot Q_a(s).$$

Петли второго порядка: $m(s) \cdot d(s) \cdot z(s)^2 \cdot (1 - P_n)^2; m(s) \cdot l(s) \cdot z(s)^2 \cdot (1 - P_n)^2; d(s) \cdot l(s) \cdot z(s)^2 \cdot (1 - P_n)^2.$

Петли третьего порядка: $m(s) \cdot d(s) \cdot l(s) \cdot z(s)^3 \cdot (1 - P_n)^3.$

С использованием топологического уравнения Мейсона, получаем общий вид эквивалентной функции стохастической сети (ф.3):

$$H = 1 + \sum_{k=1}^k (-1)^k \cdot Q_k(s) = 0 \tag{3}$$

где k – максимальный порядок петель, входящих в стохастическую сеть.

$Q_a(s) = \frac{1}{Q(s)}$ подставляя это значение в ф.3, получаем общий вид эквивалентной функции стохастической сети ф.5.4:

$$Q(s) = \frac{w(s) \cdot m(s) \cdot d(s) \cdot l(s) \cdot k(s) \cdot P_n^3}{1 - z(s) \cdot (1 - P_n) \cdot [m(s) + d(s) + l(s)] + z(s)^2 \cdot (1 - P_n)^2 [m(s) \cdot d(s) + m(s) \cdot l(s) + d(s) \cdot l(s)] - z(s)^3 \cdot (1 - P_n)^3 \cdot m(s) \cdot d(s) \cdot l(s)} \tag{4}$$

Определяем функцию распределения времени проведения КА типа «Сканирование сети и ее уязвимостей», для этого определим сначала начальные первые и вторые моменты (ф.5).

$$\begin{aligned} M_1(s, P_n) &= (-1)^1 \cdot \frac{d}{ds} \left[\frac{Q(s, P_n)}{Q(s=0, P_n)} \right] \\ M_2(s, P_n) &= (-1)^2 \cdot \frac{d^2}{ds^2} \left[\frac{Q(s, P_n)}{Q(s=0, P_n)} \right] \end{aligned} \quad (5)$$

Среднее время реализации кибератаки равно (ф.6):

$$\bar{t}_p(P_n) = - \frac{d}{ds} \left[\frac{Q(s, P_n)}{Q(s=0, P_n)} \right]_{s=0} \quad (6)$$

Дисперсия времени реализации кибератаки «Сканирование сети и ее уязвимостей» $D(\bar{t}_p)$, определяемая как второй центральный момент, представлена выражением (ф.7):

$$D(\bar{t}_p) = \frac{d^2}{ds^2} \left[\frac{Q(s, P_n)}{Q(s=0, P_n)} \right]_{s=0} - \left\{ \frac{d}{ds} \left[\frac{Q(s, P_n)}{Q(s=0, P_n)} \right]_{s=0} \right\}^2 \quad (7)$$

Вычисление математического ожидания и дисперсии позволяет с достаточной для инженерных расчетов точностью определить интегральную функцию распределения времени успешной реализации кибератаки «Сканирование сети и ее уязвимостей», как неполную Гамма-функцию (ф.8):

$$F(t) = \begin{cases} 0, & \text{если } t < 0; \\ \int_0^t \frac{\mu^\alpha}{\Gamma(\alpha)} \cdot t^{\alpha-1} \cdot e^{-\mu t} dt, & \text{если } t > 0 \end{cases} \quad (8)$$

где $\alpha = \frac{[\bar{t}_p(P_n)]^2}{D(\bar{t}_p)}$ - параметр формы; $\mu = \frac{\bar{t}_p(P_n)}{D(\bar{t}_p)}$ - параметр масштаба.

АНАЛИЗ И РЕЗУЛЬТАТЫ

Расчеты производились с использованием программного комплекса Mathcad-2014. По формуле (8) произведены расчеты, результаты которых представлены на рисунке 2. В качестве исходных данных использовались следующие значения среднего времени реализации частных процессов:

$\bar{t}_{\text{згл}} = 6 \text{ мин}$; – среднее время запуска программно-аппаратного комплекса;

$\bar{t}_{\text{оп. элем}} = 7 \text{ мин}$; – среднее время определение активных элементов БИС;

$\bar{t}_{\text{оп. ос}} = 9 \text{ мин}$; – среднее время определение типов операционных систем (ОС)

БИС;

$\bar{t}_{\text{оп. серв}} = 2 \text{ мин}$; – среднее время определение сервисов БИС;

$\bar{t}_{\text{оп. уязв}} = 15 \text{ мин}$; – среднее время определение уязвимостей элементов БИС;

$\bar{t}_{\text{повт}} = 13 \text{ мин}$; – среднее время повторного запуска сетевого сканера элементов БИС;

$P_n = 0,1 \div 0,9$ – вероятность определения ОС активных элементов за среднее время соответственно $\bar{t}_{оп. элем}$, $\bar{t}_{оп. ос}$, $\bar{t}_{оп. серв}$.

Расчётный пример построен для шести частных операций процесса, включая первоначальный и повторный запуск сканера. Средние длительности указанных операций были заданы в минутах, а вероятность успешного прохождения учитываемых этапов варьировалась в предусмотренном моделью диапазоне. На основе этих исходных величин определялись моменты распределения времени и параметры гамма-аппроксимации. Полученная интегральная функция распределения характеризует вероятность завершения моделируемого процесса к заданному моменту времени и изменяется от значений, близких к нулю, к значениям, близким к единице по мере увеличения продолжительности.

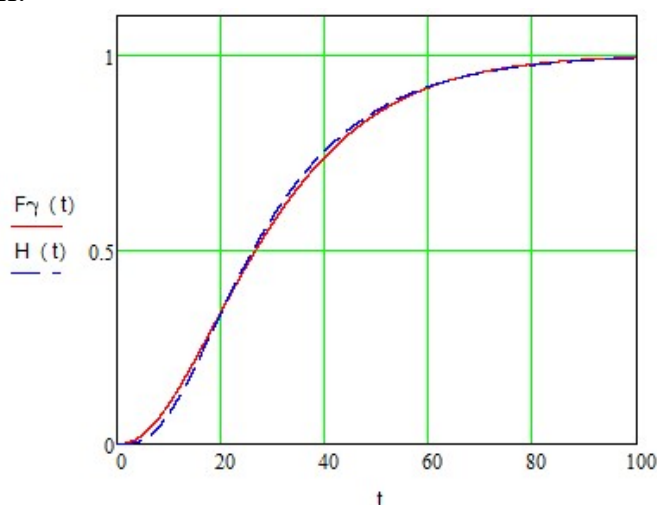


Рисунок 2 – Зависимость интегральной функции распределения вероятностей от времени реализации кибератаки «Сканирование сети и её уязвимостей» при успешной реализации с вероятностью P_n

На рисунке 2 представлены две кривые интегральной функции распределения, построенные для рассматриваемого расчётного сценария. В изображённом диапазоне времени кривые располагаются близко друг к другу и имеют сходную возрастающую форму. Наблюдаемое графическое совпадение согласуется с приведённым автором сопоставлением результатов расчёта и приближённого представления распределения. При этом исходная работа не содержит таблицы ошибок аппроксимации или числовых значений квантилей; поэтому количественная оценка расхождений между методами на основании одного графика не выполняется.

Полученные зависимости позволяют анализировать влияние вероятности успешного выполнения отдельных этапов на временные характеристики сканирования. При уменьшении такой вероятности возрастает роль повторного запуска и соответствующих возвратных переходов стохастической сети. Это сказывается на ожидаемой продолжительности процесса и форме распределения времени. Следовательно, практический результат моделирования состоит в получении расчётного инструмента для сравнительного анализа сценариев, а не

в определении универсального времени сканирования любой банковской сети.

ОБСУЖДЕНИЕ

В ходе данной работы был смоделирован процесс компьютерной атаки типа «Сканирование сети и ее уязвимостей». Для этого было произведено описание процесса атаки. На основе заданных исходных данных была построена стохастическая сеть обеспечивающая представление анализируемого процесса. Для полученной стохастической сети была определена эквивалентная функция. При определении функции распределения методом обращения, мы получаем наиболее точную оценку процесса реализации компьютерной атаки. По полученным графикам, представленным на рисунке 2, видно, что функции, полученные двумя различными методами, совпадают.

Предложенный подход дополняет технические процедуры обнаружения сетевых узлов и уязвимостей вероятностно-временным описанием их последовательного выполнения. Если средства сетевого аудита и рекомендации по тестированию защищённости [1–3] ориентированы преимущественно на организацию проверок и интерпретацию результатов, то стохастическая модель позволяет рассматривать сам процесс получения информации как совокупность взаимосвязанных операций со случайной длительностью. Тем самым единицей анализа становится не отдельное обнаруженное уязвимое место, а завершение последовательности разведывательных действий, включая возможные возвраты к предыдущим этапам. Это важно для интерпретации продолжительности разведывательного цикла и сравнения альтернативных условий сетевой защищённости.

Наличие возвратных переходов является существенной особенностью модели. Отрицательный результат определения сетевого элемента или его характеристик не обязательно означает окончательное прекращение процесса: в принятой постановке предполагается повторное выполнение части действий. Поэтому изменение вероятности успешного прохождения отдельных этапов влияет не только на вероятность получения результата при одной попытке, но и на ожидаемое число повторений. В условиях банковской инфраструктуры подобные изменения могут быть связаны с сетевой сегментацией, фильтрацией запросов, ограничением доступности сервисов и иными защитными механизмами. Вместе с тем модель не устанавливает причинно-следственного эффекта какого-либо конкретного средства защиты: для такой оценки необходимы отдельные измерения в контролируемой среде.

Использование интегральной функции распределения расширяет аналитические возможности по сравнению с рассмотрением одного среднего значения. Математическое ожидание описывает центральную характеристику длительности, однако не показывает, насколько часто процесс может завершаться раньше или позже этого значения. Функция распределения, напротив, позволяет соотносить выбранный временной горизонт с расчётной вероятностью завершения операции. Для задач управления защитой такая характеристика может служить дополнительным индикатором при оценке сценариев

обнаружения сетевых ресурсов, наряду с техническими данными сканеров и журналами мониторинга. Она не должна интерпретироваться как непосредственная вероятность компрометации банка, поскольку обнаружение уязвимости и её эксплуатация представляют собой разные события.

Сравнение с исследованиями методов обнаружения вторжений [9, 10] показывает, что временная модель и анализ сетевых событий решают взаимодополняющие задачи. Системы мониторинга могут фиксировать соединения, отклонения поведения и признаки попыток сканирования, но сами по себе не описывают распределение времени завершения многоэтапной последовательности. Напротив, стохастическая сеть обеспечивает расчётную интерпретацию этапов процесса, однако не заменяет обнаружение событий в реальном трафике. При практическом использовании моделей этих двух классов данные средств сетевого мониторинга могли бы применяться для оценивания исходных вероятностей и длительностей операций. Такое объединение следует рассматривать как направление дальнейшей проверки, а не как результат, уже подтверждённый в рассматриваемой статье.

Основное ограничение исследования связано с принятыми математическими предпосылками: частные длительности описываются экспоненциальными законами, а параметры расчёта задаются заранее. Реальные сетевые условия могут характеризоваться зависимыми событиями, неоднородностью устройств, изменением нагрузки, ограничениями по частоте запросов и адаптивной реакцией средств защиты. Кроме того, расчётный пример выполнен в Mathcad с заданными исходными параметрами и не подкреплён серией полевых измерений в действующей банковской сети. Графическое сходство функций не является самостоятельным доказательством точности аппроксимации для всех возможных сценариев. Для дальнейшей валидации потребуются экспериментальные данные, анализ чувствительности и оценка расхождений между теоретическими и наблюдаемыми распределениями.

С практической точки зрения разработанная модель может применяться в рамках разрешённого тестирования защищённости и аналитической оценки угроз. Значения средних длительностей и вероятностей целесообразно определять по результатам контролируемых испытаний либо по данным мониторинга с документированными условиями измерений. После этого можно сопоставлять сценарии изменения параметров, выделять операции с наибольшим вкладом в общую длительность и оценивать, в какой мере защитные меры затрудняют разведывательные действия. Для банковской организации такие оценки имеют вспомогательный характер и должны использоваться совместно с управлением уязвимостями, инвентаризацией активов и процедурами реагирования на инциденты [6, 11].

ЗАКЛЮЧЕНИЕ

Полученная модель позволяет оценить влияние изменения исходных вероятностных параметров на характеристики процесса. В частности, уменьшение вероятности успешного выполнения отдельных операций приводит

к увеличению числа повторных попыток, что, в свою очередь, увеличивает среднее время реализации процесса и изменяет форму функции распределения. Таким образом, разработанная стохастическая модель позволяет выявлять наиболее значимые операции и определять их вклад в общую продолжительность компьютерной разведки.

В исследовании процесс сканирования сетевых элементов банковской информационной системы представлен в виде стохастической сети, отражающей последовательность операций и возможность их повторения. Применение топологического уравнения Мейсона и преобразований Лапласа–Стилтьеса позволило сформировать аналитическое описание процесса, на основе которого рассматриваются математическое ожидание, дисперсия и интегральная функция распределения времени. Расчётный пример и соответствующий график иллюстрируют применение предложенного подхода для заданного набора исходных параметров.

Практическая значимость модели заключается в возможности сопоставлять варианты организации сетевой защиты по их влиянию на вероятностно-временные характеристики компьютерной разведки. Результаты могут использоваться при обосновании контролируемых испытаний, разработке сценариев мониторинга и определении приоритетных направлений повышения сетевой защищённости. В дальнейшем требуется проверить модель на экспериментальных данных, оценить устойчивость результатов к изменению предположений о распределении длительностей и разработать количественные критерии качества аппроксимации. Полученные выводы относятся к смоделированному сценарию и не являются оценкой защищённости конкретного банка.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Scarfone K., Souppaya M., Cody A., Orebaugh A. Technical Guide to Information Security Testing and Assessment. NIST Special Publication 800-115. Gaithersburg: National Institute of Standards and Technology, 2008.
2. Radack S. Guide to Information Security Testing and Assessment. NIST Information Technology Laboratory Bulletin. National Institute of Standards and Technology, 2008
3. OWASP Foundation. Web Security Testing Guide (WSTG)
4. MITRE Corporation. Common Vulnerabilities and Exposures (CVE).
5. FIRST. Common Vulnerability Scoring System (CVSS)
6. Souppaya M., Scarfone K. Guide to Enterprise Patch Management Technologies. NIST Special Publication 800-40 Revision 3. National Institute of Standards and Technology, 2013
7. Wireshark Foundation. Wireshark User's Guide.
8. Zeek Project. Zeek Documentation.
9. Denning D. E. An Intrusion-Detection Model // IEEE Transactions on Software Engineering. 1987. Vol. SE-13, No. 2. P. 222–232.
10. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // 2010 IEEE Symposium on Security and Privacy. 2010.

P. 305–316

11. Center for Internet Security. CIS Critical Security Controls