УДК 004.056.5 **DOI** 10.15622/sp.55.7

В.И. Котенко, И.Б. Саенко, М.А. Коцыняк, О.С. Лаута

ОЦЕНКА КИБЕРУСТОЙЧИВОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ МОДЕЛИРОВАНИЯ КИБЕРАТАК МЕТОДОМ ПРЕОБРАЗОВАНИЯ СТОХАСТИЧЕСКИХ СЕТЕЙ

Котенко В.И., Саенко И.Б., Коцыняк М.А., Лаута О.С. **Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей.**

Аннотация: В статье предложен подход к оценке киберустойчивости компьютерных сетей, основанный на аналитическом моделировании компьютерных атак с применением метода преобразования стохастических сетей. Обосновывается понятие киберустойчивости компьютерных сетей. Рассматриваются математические основы такой оценки, позволяющие с помощью аналитических выражений вычислить показатели киберустойчивости. В качестве основного показателя предлагается использовать коэффициент исправного действия по киберустойчивости. Рассматриваемый подход предполагает построение аналитических моделей реализации компьютерных атак. Для построения аналитических моделей кибератак применяется метод преобразования стохастических сетей. Результатом моделирования является функция распределения времени и среднее время реализации кибератаки. Эти оценки используются затем для нахождения показателей киберустойчивости. Приведены экспериментальные результаты аналитического моделирования, которые показали, что предложенный подход обладает достаточно высокой точностью и устойчивостью получаемых решений.

Ключевые слова: кибербезопасность, кибератаки, моделирование атак, киберустойчивость, стохастические сети, преобразование Лапласа.

1. Введение. Компьютерные сети и системы в процессе своего функционирования выполняют различные функции, которые поддерживаются соответствующими сервисами. При этом все сервисы можно условно разделить на две группы: локальные и распределенные. Локальные сервисы функционируют на узлах сети. К их числу можно отнести базу данных коллективного пользования, сетевой принтер, прокси-сервер, сервер приложений и так далее. За поддержание работы локального сетевого сервиса, как правило, отвечает один узел в компьютерной сети. Коммуникационные сервисы (обмен файлами, внутренняя электронная почта, IP-телефония и другие) отвечают за передачу информации в различной форме от одного узла сети к другому узлу.

Воздействия на компьютерную сеть по своей природе могут быть разными. Традиционно выделяются три группы таких факторов: (1) внешние физические дестабилизирующие факторы; (2) внутренние дестабилизирующие факторы, обусловленные длительным временем работы элементов сети; (3) электромагнитные помехи. Однако в последнее время возникла необходимость дополнить множество сетевых дестабилизирующих факторов еще одной группой, содержанием которой являются программно-информационные воздействия, или кибератаки.

Если про традиционные группы факторов можно сказать, что они в достаточной степени исследованы и рассматриваются во многих сложных электротехнических системах, не только в компьютерных сетях, то последняя группа факторов характерна именно для компьютерных сетей, так как именно компьютерная обработка информации является средой для распространения кибератак [1]. Возможными результатами воздействия кибератак на компьютерные сети и системы являются несанкционированный доступ, блокирование управляющей информации, внедрение ложной информации, нарушение установленных регламентов сбора, обработки и передачи информации в автоматизированных системах контроля и управления, отказы и сбои в работе компьютерной сети, а также компрометация передаваемой или получаемой информации. Это позволяет считать, что кибератаки и способность противодействовать их реализации является ключевыми факторами, определяющими устойчивость компьютерных сетей. По этой причине в статье акцентируется внимание именно на кибератаках как наименее изученной, но достаточно важной группе дестабилизирующих факторов. При этом понятие киберустойчивости трактуется как устойчивость компьютерной сети в условиях воздействия кибератак.

При рассмотрении функционала, который должна обеспечить компьютерная сеть в условиях воздействия кибератак, мы будем ограничиваться только коммуникационными сервисами, не умаляя при этом важность локальных сервисов. Учет локальных сервисов рассматривается как направление дальнейших исследований.

Киберустойчивость рассматривается как способность компьютерной сети обеспечивать и поддерживать приемлемый уровень обслуживания в условиях неисправностей и проблем в нормальном режиме работы [2, 3]. Для оценки киберустойчивости необходимо определить вероятные проблемы, риски и соответствующие показатели устойчивости [4]. При этом учитываются такие этапы, как планирование, подготовка, обнаружение, принятие мер защиты и восстановление [5]. Подход, рассматриваемый в настоящей статье, следует этим принципам, однако имеет некоторые особенности. В качестве показателя, позволяющего оценить критическую функциональность компьютерной сети при условии приоритетности коммуникационных сервисов, предлагается использовать коэффициент исправного действия, который вычисляется через аналогичные по назначению показатели, применяемые к направлениям связи и к маршрутам передачи данных, существующим между критическими узлами сети. При этом про аналитические модели атак, формируемые с помощью предлагаемого в настоящей статье метода, можно говорить, что они охватывают этапы планирования, подготовки,

обнаружения, принятия мер защиты и восстановления. Эти этапы учитывают функционирование сети на начальном этапе кибератаки (сканирования сети), на этапах ее реализации и обнаружения и на этапе принятия мер по противодействию атаки и восстановлению работоспособности сети. Этап планирования учитывается косвенным образом путем анализа полученных оценок с целью выбора наиболее приемлемого варианта построения сети.

Подход, рассматриваемый в статье, предполагает построение аналитических моделей для реализации атак. Результатом моделирования является функция распределения времени и среднее время реализации кибератаки. Эти оценки используются затем для нахождения показателей киберустойчивости. Для построения аналитической модели кибератаки применяется подход, основанный на преобразовании стохастических сетей [6]. Он отличается более высокой точностью и устойчивостью получаемых решений и хорошо зарекомендовал себя для моделирования многошаговых стохастических процессов различной природы.

Рассмотренный подход получил в статье экспериментальную проверку для двух наиболее известных и популярных видов атак. Атака «Сканирование сети и выявление ее уязвимостей» является характерным примером атаки пассивного типа, которая не наносит разрушений в сети, но выявляет важную информацию, которую впоследствии злоумышленник может использовать для проведения более серьезных атак. Атака «Отказ в обслуживании (DoS)» является характерным примером активных атак, которые существенно нарушают работоспособность компьютерной сети. Эти два типа атак будут рассмотрены в качестве объектов для аналитического моделирования.

Теоретический вклад статьи заключается в дальнейшем развитии методов аналитического моделирования кибератак [7, 8] и в их применении для оценки киберустойчивости как очень важного свойства компьютерной сети или системы. Новизна полученных результатов определяется использованием метода преобразования стохастических сетей для аналитического моделирования кибератак.

2. Математические основы оценки киберустойчивости компьютерной сети. Если в качестве вида воздействия на сеть учитывать только кибератаки, то можно ограничиться рассмотрением коммуникационных сервисов, так как этот тип сервисов, как мы полагаем, при кибератаках будет испытывать наибольшее влияние. В этом случае компьютерную сеть будем рассматривать как разновидность информационно-телекоммуникационной сети (ИТКС), в которой основным функционалом является обмен информацией в различных направлениях.

Положим, сеть имеет вид, представленный на рисунке 1. ИТКС состоит из узловых элементов (УЭ) 1-4, включающих в себя маршрутизаторы 1-4 и персональные ЭВМ (ПЭВМ) 1-8, а также сетевых элементов, включающих маршрутизаторы 5-11.

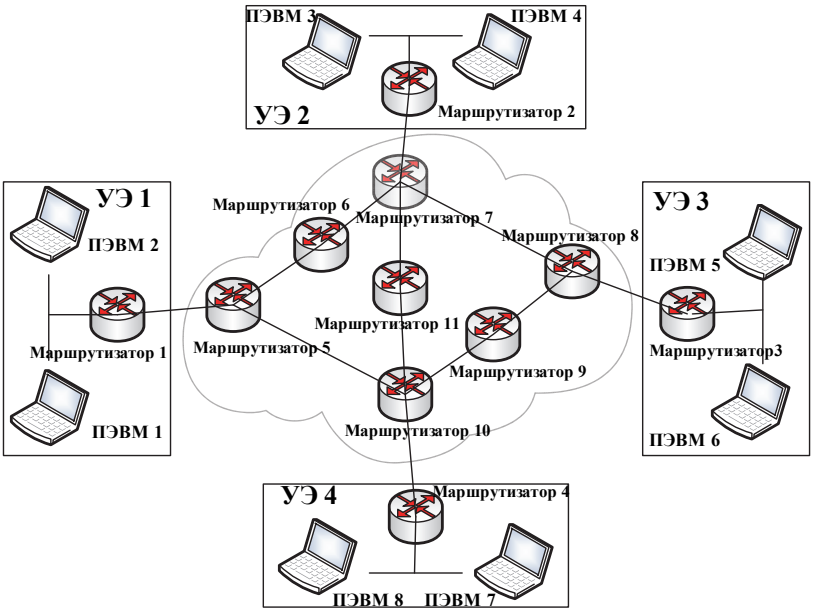

Рис. 1. Структура компьютерной сети (вариант)

Путь передачи информации от узловых элементов УЭ 1–4 через маршрутизаторы 5–11 называется *маршрутом* передачи данных. Маршруты могут быть простыми (один интервал связи) или составными (несколько интервалов связи). Совокупность маршрутов передачи информации между двумя узловыми элементами (УЭ 1 и УЭ 3; УЭ 2 и УЭ 4; УЭ 1 и УЭ 2 и др.) образуют *направление связи*, а совокупность направлений связи и ПЭВМ 1-8 — ИТКС.

В качестве показателя, характеризующего устойчивость компьютерной сети при воздействии кибератак, или *киберустойчивость*, предлагается использовать коэффициент исправного действия (K_{sa}), который вычисляется следующим образом:

$$K_{sa} = \textit{Время исправной работы сети}/\textit{Общее время работы сети}. \quad (1)$$

Этот показатель показывает, какую часть времени от всего учитываемого времени работы компьютерной сети она функционирует исправно.

С целью определения K_{sa} сначала находятся коэффициенты исправного действия для каждого маршрута в условиях воздействия атак и вероятность воздействия на эти маршруты. Для этого необходимо рассмотреть процесс функционирования компьютерной сети в условиях воздействия системы атак, представленный на рисунке 2.

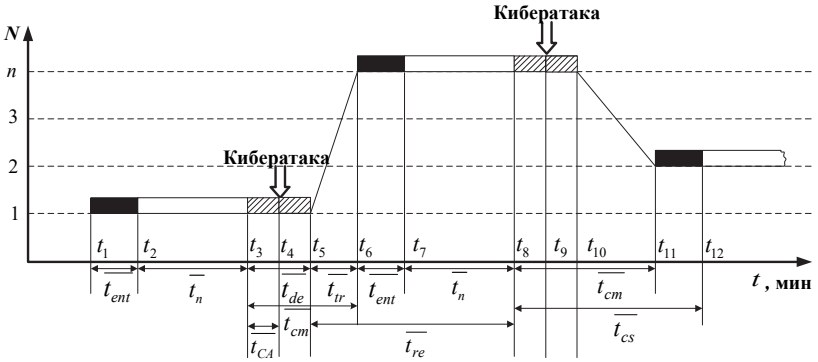

Рис. 2. Процесс функционирования компьютерной сети в условиях воздействия кибератак

В обобщенном виде процесс функционирования компьютерной сети в условиях воздействия атак можно представить следующим образом [9]. Для осуществления передачи информации длительностью t_n (в моменты времени t_2, t_7, t_{12} и т.д.) удаленные пользователи (сервисы) компьютерной сети сначала входят в связь (t_1), на что затрачивается в среднем время $\overline{t_{ent}}$. Затем (в моменты времени t_3, t_8 и т.д.) система информационного воздействия реализует кибератаку за среднее время $\overline{t_{CA}}$, которую оператор сети (компонент защиты) сможет обнаружить (в моменты времени t_5, t_{10} и т.д.) за среднее время $\overline{t_{de}}$, определяемое временем реакции системы мониторинга сети.

Обнаружив воздействие атаки, оператор сети будет принимать меры по восстановлению коммуникационных сервисов (в моменты времени t_5, t_{10} и т.д.) за среднее время $\overline{t_{tr}}$.

После этого операторы (компоненты) сети входят в связь или инициируют взаимодействие (в моменты времени t_6, t_{11} и т.д.), на что затрачивается некоторое среднее время $\overline{t_{ent}}$, и передача информации возобновляется.

Среднее время $\overline{t_{CS}}$, затрачиваемое на принятие мер защиты ($\overline{t_{cm}}$) и вхождение в связь ($\overline{t_{ent}}$), характеризует реакцию системы управления на воздействие кибератак, то есть определяется следующей суммой времен: $\overline{t_{CS}} = \overline{t_{cm}} + \overline{t_{ent}} = \overline{t_{tr}} + \overline{t_{de}} + \overline{t_{ent}}$.

Среднее время от момента принятия мер по восстановлению коммуникационных сервисов до момента воздействия кибератак назовем временем реакции $\overline{t_{re}}$. В течение этого времени злоумышленник производит сбор данных о сети (например, о топологии сети, активных элементах, открытых портах, типе операционной системы и т.д.).

Для определения коэффициента исправного действия и вероятности воздействия в условиях кибератак необходимо первоначально вычислить среднее значение времени простоя и времени исправной работы за достаточно большой промежуток времени функционирования сети. Учитывая, из чего слагаются эти времена (см. рисунок 2), коэффициент исправного действия *j*-го интервала связи маршрута можно записать в следующем виде:

$$K_{sa,j} = \frac{\overline{t_{n,j}}}{\overline{t_{n,j}} + \overline{t_{CS,j}}}. \qquad (2)$$

Так как маршрут передачи информации состоит из нескольких интервалов связи (взаимодействия), то коэффициент исправного действия *j*-го составного маршрута равен произведению коэффициентов исправного действия его интервалов:

$$K_{sa\_CM,j} = \prod_{l=1}^{O_j} K_{sa,jl}. \qquad (3)$$

где $K_{ca\_CM,j}$ — коэффициент исправного действия *j*-го составного маршрута; O_j — общее количество интервалов связи на *j*-ом маршруте; $K_{sa,jl}$ — коэффициент исправного действия *l*-го интервала на *j*-м маршруте.

Воздействие кибератаки на отдельные маршруты направлений связи повлечет нарушение их функционирования и принятие мер по восстановлению нарушенных связей. С этой целью осуществляется поиск обходных маршрутов. Для оценки возможности установления соединений и передачи сообщений в случае выхода из строя элементов или целых участков введем в рассмотрение новую характеристику —

связность K_{rel} направлений и компьютерной сети. Под связностью будем понимать свойство компьютерной сети сохранять рабочее состояние при выходе из строя ее элементов или отдельных частей.

Ограниченные возможности применения известных показателей связности при решении задач анализа и синтеза сетей вынуждают расширить поиск таковых. Рассмотрим некоторый линейный функционал, представляющий собой линейную комбинацию определенным образом выбранных параметров связности, составленную по всем маршрутам сети. Такими параметрами могут быть относительная и абсолютная связности каждого маршрута компьютерной сети.

Для оценки каждой из этих видов связности предложим коэффициенты, лежащие в диапазоне от 0 до 1. Относительную связность j-го маршрута компьютерной сети $K_{rel\_ref,j}$ определим следующим образом:

$$K_{rel\_ref,j} = \frac{H_j}{N - O_j} \ (j = 1, 2, \ldots, N), \tag{4}$$

где H_j — ранг j-го маршрута; O_j — количество обходных маршрутов для j-го маршрута; N — общее число маршрутов в направлении связи ($O_j < N$). Ранг j-го маршрута лежит в диапазоне от 1 до $(N - O_j)$, определяется экспертным путем и отражает значимость маршрута в обеспечении высокой устойчивости направления связи.

Абсолютную связность j-го маршрута можно определить отношением количества обходных маршрутов, которыми может обладать j-й маршрут, к общему числу маршрутов рассматриваемого направления связи:

$$K_{rel\_abs,j} = \frac{O_j}{N} \ (j = 1, 2, \ldots, N). \tag{5}$$

Данная величина при фиксированном числе маршрутов N в сети будет полностью определяться величиной O_j. Чем больше O_j , тем больше абсолютная связность j-го маршрута.

На основании рассмотренных параметров предложим следующее выражение для нахождения связности i-го направления связи:

$$K_{rel\_D,i} = 0.5 \cdot \sum_{j=1}^{N_i} \alpha_{ij} \cdot \left(K_{rel\_ref,j} + K_{rel\_abs,j} \right), \tag{6}$$

где α_{ij} — вес j-го маршрута в i-м направлении связи. Коэффициент 0.5 в выражении (6) установлен с целью, чтобы значение $K_{rel\_D,i}$ находилось в диапазоне от 0 до 1.

Коэффициент исправного действия i-го направления связи $K_{sa\_D,i}$ определяется по следующей формуле:

$$K_{sa\_D,i} = K_{rel\_D,i} \cdot \left(1 - \prod_{j=1}^{N} \left(1 - K_{sa\_CM,j}\right)\right). \quad (7)$$

Учитывая, что компьютерная сеть состоит из M направлений связи, коэффициент исправного действия компьютерной сети в условиях кибератак определяется на основании следующих выражений:

$$K_{sa} = K_{rel} \cdot \left(1 - \prod_{i=1}^{M} \left(1 - K_{sa\_D,i}\right)\right), \quad (8)$$

$$K_{rel} = \sum_{i=1}^{M} \alpha_i \cdot \left(\frac{G_i}{M - L} + \frac{L}{M}\right), \quad (9)$$

где K_{sa} — коэффициент исправного действия компьютерной сети; K_{rel} — коэффициент связности сети; G_j — ранг i-го направления связи; M — количество направлений связи в компьютерной сети; L — количество обходных направлений связи ($L < M$).

Таким образом, для определения коэффициента исправного действия компьютерной сети первоначально требуется определить среднее время воздействия кибератак и выработки мер противодействия, то есть определить вероятностно-временные характеристики атак. Для этого предлагается использовать эталонные модели кибератак и метод, который мы назовем методом преобразования стохастических сетей. Эталонная модель атаки — это последовательность (алгоритм) действий злоумышленника при реализации кибератаки.

3. Метод преобразования стохастической сети. Под стохастической сетью будем понимать совокупность взаимоувязанных узлов (вершин) и ветвей, соединение которых соответствует алгоритму функционирования исследуемой системы.

Суть метода преобразования стохастической сети заключается в том, что исследуется не система, а процесс, который она реализует. При этом сеть реализуется, если будет построено некоторое подмножество ветвей, время реализации которых выбирается в соответствии с вероятностным распределением [10, 11].

Стохастическая сеть не является моделью системы. Она является моделью процесса, который реализует эта система. Сложный процесс декомпозируется на элементарные процессы, каждый из которых характеризуется функцией распределения, средним временем и его дисперсией.

Логика и последовательность выполнения процессов определяется двухполюсной сетью, состоящей из входного, промежуточных и выходного узлов (вершин), при этом ребрам соответствует набор элементарных процессов, а вершинам (узлам) — условия их выполнения. Каждый узел (вершина) выполняет две функции — входную, определяющую условие (логическую операцию), при котором функция может быть выполнена, и выходную, определяющую какие из операций, следующих за узлом, будут выполняться. Входной узел сети выполняет только предшествующую выходную функцию, а выходной только входную.

Для каждого ребра определяется функция передачи. Эта функция играет роль условной характеристической функции. Она представляет собой преобразование Лапласа [12] для функции плотности вероятностей времени свершения элементарного процесса.

Далее осуществляется топологическое преобразование сети случайных процессов.

Напомним, что топология — раздел математики, изучающий свойства геометрических фигур, не изменяющиеся при любых деформациях, производимых без разрывов и склеиваний. Главной задачей топологии является изучение таких топологических свойств как связность, компактность, размерность и другие. В данном случае таким топологическим инвариантом является свойство связности графа.

Поскольку входная и выходная вершины двухполюсной сети (графа) являются связными, то с помощью стандартных процедур ее можно свести к одному ребру, связывающему эти вершины. Для этого в сети сначала выделяются последовательные, параллельные и петлеобразные пути, на которых определяются эквивалентные функции передачи, каждый из которых сводится к одному ребру. Затем с помощью правила Мейсона [13, 14] эти фрагменты объединяются в одно ребро с общей эквивалентной функцией передачи. При этом структура сети не исчезает бесследно — ее «следы» остаются в структуре эквивалентной функции. После получения эквивалентной функции производят обратное преобразование Лапласа, результатом которого является функция плотности вероятностей времени выполнения целевого процесса, либо определяют первые моменты случайного времени его выполнения [12].

В качестве примера построения эталонных моделей атак выберем следующие типы атак: «Сканирование сети и выявление ее уязвимостей» и «Отказ в обслуживании».

3. Модель атаки «Сканирование сети и выявление ее уязвимостей». Реализация этой атаки имеет следующие этапы:

– запуск программно-аппаратного комплекса (сетевого сканера) за среднее время $\overline{t_{start}}$ с функцией распределения времени $W(t)$;

– определение активных элементов атакуемой сети с вероятностью P_n за среднее время $\overline{t_{elem}}$ с функцией распределения времени $Q(t)$;

– определение типов операционных систем на активных элементах сети с вероятностью P_n за среднее время $\overline{t_{OS}}$ с функцией распределения времени $D(t)$;

– определение сервисов на элементах сети с вероятностью P_n за среднее время $\overline{t_{ser}}$ с функцией распределения времени $L(t)$;

– определение уязвимостей за среднее время $\overline{t_{vul}}$ с функцией распределения времени $O(t)$.

При этом, если активные элементы сети, типы операционных систем и сервисы на них не будут определены, то с вероятностью $(1 - P_n)$ сетевой сканер будет запущен повторно за среднее время $\overline{t_{rep}}$ с функцией распределения времени $Z(t)$.

Стохастическая сеть, отражающая выше перечисленные этапы атаки «Сканирование сети и выявление ее уязвимостей», представлена на рисунке 3.

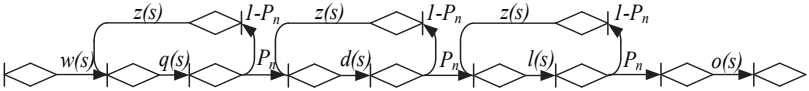

Рис. 3. Стохастическая сеть кибератаки «Сканирование сети и ее уязвимостей»

Функции $w(s)$, $l(s)$, $q(s)$, $d(s)$, $o(s)$ and $z(s)$, находящиеся на выходе узлов стохастической сети, являются эквивалентными функциями и получаются путем применения преобразования Лапласа к функциям $W(t)$, $L(t)$, $Q(t)$, $D(t)$, $O(t)$, и $Z(t)$ соответственно.

Результатом преобразования стохастической сети является эквивалентная функция, сохраняющая в своей структуре параметры распределения и логику взаимодействия элементарных случайных процессов. Эквивалентная функция позволяет определить первые моменты случайного времени выполнения целевого процесса. Эквивалентная функция вычисляется по формуле Мейсона.

Стохастическая сеть содержит множество петель. Для определения эквивалентной функции вводится понятие замкнутой стохастической сети, а также петель первого и k-го порядков.

Замкнутой стохастической сетью называется сеть, в которой каждая ветвь принадлежит по крайней мере одной петле. Пример замкнутой стохастической сети, соответствующей атаке «Сканирование сети и ее уязвимостей», представлен на рисунке 4.

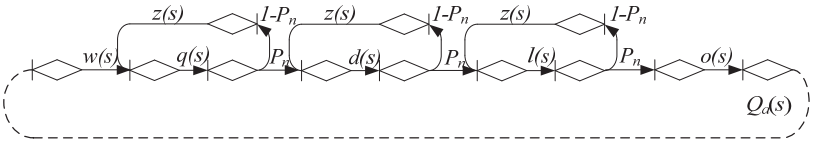

Рис. 4. Замкнутая стохастическая сеть кибератаки «Сканирование сети и ее уязвимостей»

Петли первого порядка — это петли, не содержащие других петель и позволяющие достичь каждой вершины петли из любой другой.

Петля *k*-го порядка — множество *k* не связанных между собой петель первого порядка.

Теперь определим все петли в стохастической сети, приведенной на рисунке 4. Вначале определим петли первого порядка. Общее количество этих петель равно 4.

Первая петля первого порядка состоит из последовательно соединенных ветвей $w(s)$, $q(s)$, P_n, $d(s)$, P_n, $l(s)$, P_n, and $o(s)$. Эквивалентная функция для этой петли имеет следующий вид:

$$w(s)\cdot q(s)\cdot d(s)\cdot P_n^3\cdot l(s)\cdot o(s)\,.$$

Вторая петля первого порядка состоит из следующих последовательно соединенных ветвей: $(1-P_n)$, $z(s)$, and $q(s)$. Ее эквивалентная функция имеет вид:

$$(1-P_n)\cdot z(s)\cdot q(s)\,.$$

Аналогичным образом определяются третья и четвертая петли первого порядка и соответствующие им эквивалентный функции:

$$(1-P_n)\cdot z(s)\cdot d(s)\,;$$

$$(1-P_n)\cdot z(s)\cdot l(s)\,.$$

Петли второго порядка формируются следующим образом. Общее количество таких петель равно 3. Первая петля второго порядка формируется из второй и третьей петель первого порядка. Результирующее выражение имеет вид:

$$(1-P_n)^2 \cdot z^2(s) \cdot q(s) \cdot d(s).$$

Вторая петля второго порядка формируется из третьей и четвертой петель первого порядка. Результирующее выражение для эквивалентной функции имеет следующий вид:

$$(1-P_n)^2 \cdot z^2(s) \cdot d(s) \cdot l(s).$$

Третья петля второго порядка формируется из второй и четвертой петель первого порядка аналогичным образом. В результате для эквивалентной функции получается следующее выражение:

$$(1-P_n)^2 \cdot z^2(s) \cdot q(s) \cdot l(s).$$

Наконец, можно сформировать только одну петлю третьего порядка. В нее входят все петли второго порядка, а эквивалентная функция принимает следующий вид:

$$(1-P_n)^3 \cdot z^3(s) \cdot q(s) \cdot d(s) \cdot l(s).$$

Используя уравнение Мейсона, можно сформировать эквивалентную функцию для всей сети. Она будет иметь следующий вид:

$$h(s) = \frac{w(s) \cdot q(s) \cdot d(s) \cdot P_n^3 \cdot l(s) \cdot o(s)}{R(s)}, \tag{10}$$

где

$$\begin{aligned} R(s) = 1 &- (1-P_n) \cdot z(s) \cdot q(s) - (1-P_n) \cdot z(s) \cdot d(s) - (1-P_n) \cdot z(s) \cdot l(s) + \\ &+ (1-P_n)^2 \cdot z^2(s) \cdot q(s) \cdot d(s) + (1-P_n)^2 \cdot z^2(s) \cdot d(s) \cdot l(s) + \\ &+ (1-P_n)^2 \cdot z^2(s) \cdot q(s) \cdot l(s) - (1-P_n)^3 \cdot z^3(s) \cdot q(s) \cdot d(s) \cdot l(s). \end{aligned} \tag{11}$$

Используя преобразование Лапласа и разложение Хевисайда [15], функцию распределения вероятности времени реализации кибератаки типа «Сканирование сети и выявление ее уязвимостей» можно определить следующим образом:

$$F(t) = \sum_{k=1}^{8} \frac{w \cdot q \cdot d \cdot P_n^3 \cdot l \cdot o \cdot (z+s_k)^3}{\phi(s_k)} \cdot \frac{1-\exp[s_k t]}{-s_k}, \tag{12}$$

где φ (s_k) — условное обозначение полинома в знаменателе; s_k — разложение полюсов; $w = 1/\overline{t_{start}}$; $l = 1/\overline{t_{elem}}$; $q = 1/\overline{t_{OS}}$; $d = 1/\overline{t_{ser}}$; $o = 1/\overline{t_{vul}}$; $z = 1/\overline{t_{rep}}$.

Многочлен φ имеет следующий вид:

$$\phi(s_k) = (w + s_k) \cdot [(1 - P_n) \cdot z \cdot [(1 - P_n)^2 \cdot z^2 \cdot q \cdot d \cdot l - [q \cdot (z + s)^2 \cdot$$
$$\cdot (d + s) \cdot (l + s) - d \cdot (z + s)^2 \cdot (q + s) \cdot (l + s) - l \cdot (z + s)^2 \cdot (q + s) \cdot (d + s) +$$
$$+ (1 - P_n) \cdot z \cdot q \cdot d \cdot (z + s) \cdot (l + s) + (1 - P_n) \cdot z \cdot l \cdot d \cdot (z + s) \cdot (q + s)$$
$$+ (1 - P_n) \cdot z \cdot q \cdot l \cdot (z + s) \cdot (d + s) - (1 - P_n)^2 \cdot z^2 \cdot q \cdot d \cdot l]]].$$

Среднее время $\overline{T}$, затрачиваемое на реализацию кибератаки типа «Сканирование сети и выявление ее уязвимостей», определяется следующим образом:

$$\overline{T} = \sum_{k=1}^{8} \frac{w \cdot q \cdot d \cdot P_n^3 \cdot l \cdot o \cdot (z + s_k)^3}{\phi(s_k)} \cdot \frac{1}{(-s_k)^2} \cdot \qquad (13)$$

Значения эквивалентных функций, рассчитанных для стохастической сети, представленной на рисунке 4, и функций распределения времени для каждого этапа кибератаки типа «Сканирование сети и выявление ее уязвимостей» представлены в таблице 1.

Таблица 1. Функции для оценки длительности этапов кибератаки типа «Сканирование сети и ее уязвимостей»

Содержание этапа	Эквивалентная функция	Функция распределения времени
Запуск программно-аппаратного комплекса (сетевого сканера)	$w(s) = \frac{w}{w+s}$	$W(t) = 1 - \exp[-wt]$
Определение сервисов на элементах сети	$l(s) = \frac{l}{l+s}$	$L(t) = 1 - \exp[-lt]$
Определение активных элементов атакуемой сети	$q(s) = \frac{q}{q+s}$	$Q(t) = 1 - \exp[-qt]$
Определение типов операционных систем на активных элементах сети	$d(s) = \frac{d}{d+s}$	$D(t) = 1 - \exp[-dt]$
Определение уязвимостей	$o(s) = \frac{o}{o+s}$	$O(t) = 1 - \exp[-ot]$
Повторный запуск сетевого сканера	$z(s) = \frac{z}{z+s}$	$Z(t) = 1 - \exp[-zt]$

Результаты расчетов $F(t)$ и $\overline{T}$ представлены в виде зависимостей на рисунке 5. В качестве исходных данных используются следующие значения средних времен реализации этапов атаки «Сканирование сети и выявление ее уязвимостей» и вероятности перехода пользователя по ссылке: $\overline{t_{start}} = 3$ мин, $\overline{t_{elem}} = 7$ мин, $\overline{t_{OS}} = 4$ мин, $\overline{t_{ser}} = 5$ мин, $\overline{t_{vul}} = 7$ мин, $\overline{t_{rep}} = 3$ мин, $P_n = 0.1,\ldots,0.9$.

Анализ полученных зависимостей на рисунках 5*а* и 5*б* позволяет сделать вывод о том, что для реализации атаки «Сканирование сети и выявление ее уязвимостей» с вероятностью $P_n = 0.1$ требуется 280 минут и 33 минут при $P_n = 0.9$. Полученные зависимости позволяют оценить влияние вероятности нахождения активных элементов сети, типов операционных систем и сервисов (за время, не превышающее заданное) на значения функции распределения времени реализации атаки. Видно, что увеличение вероятности P_n уменьшает среднее время реализации атаки. Однако по мере возрастания значения P_n степень влияния на интегральную функцию распределения $F(t)$ уменьшается. При преодолении значения $P_n = 0.5$ степень этого влияния пренебрежимо мала.

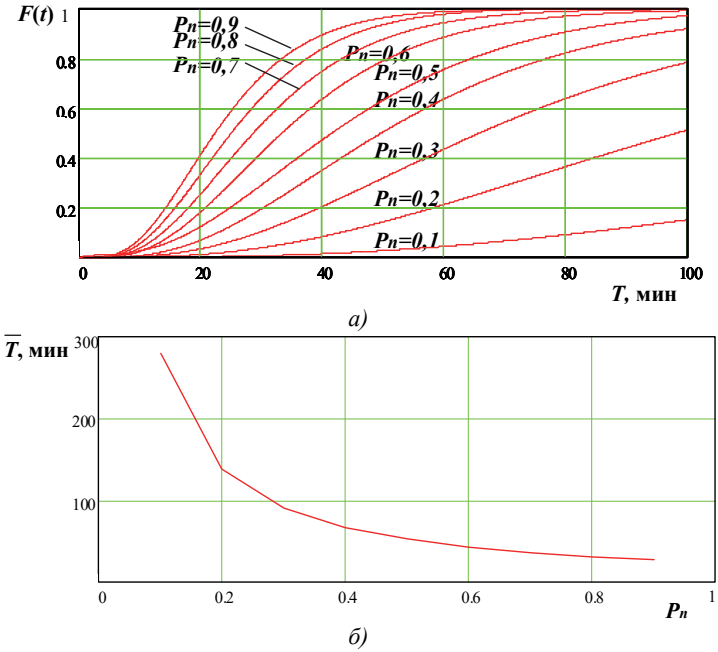

Рис. 5. Вероятностно-временные характеристики кибератаки типа «Сканирование сети и ее уязвимостей» (*а* – зависимость интегральной функции распределения вероятности от времени реализации кибератаки; *б* – зависимость среднего времени реализации кибератаки от вероятности P_n)

Среднее время реализации кибератаки также зависит от вероятности P_n. При значении P_n, превышающем 0.5, среднее время реализации этой атаки возрастает не очень сильно. Оно изменяется от 33 (при $P_n = 0.9$) до 50 минут (при $P_n = 0.5$). Если вероятность $P_n < 0.5$ и далее уменьшается, то среднее время реализации атаки начинает существенно увеличиваться, достигая значения 280 минут при $P_n = 0.1$. Это означает, что при малом значении вероятности P_n злоумышленник не может с первого раза выявить правильно уязвимость, и ему приходится неоднократно повторять операцию сканирования. Чем меньше вероятность P_n, тем больше потребуется повторов и, следовательно, тем больше будет среднее время реализации атаки.

5. Модель атаки «Отказ в обслуживании». Пусть имеется компьютерная сеть, в состав которой входит n серверов, находящихся в постоянном ожидании запросов на подключение от удаленного объекта. Реализация атаки «Отказ в обслуживании» имеет следующие этапы:

– запуск и настройка программы, осуществляющей формирование и направление запросов, за среднее время $\overline{t_{start}}$ с функцией распределения $W(t)$;

– с вероятностью P_q направление запроса на сервер за среднее время $\overline{t_{que}}$ с функцией распределения $M(t)$;

– получение ответа от сервера за среднее время $\overline{t_{srv}}$ с функцией распределения $D(t)$;

– отправка большого количества («шторма») анонимных запросов на подключение от имени других объектов за среднее время $\overline{t_{pack}}$ с функцией распределения $L(t)$;

– переполнение очереди запросов сервера и нарушение работоспособности за среднее время $\overline{t_{voil}}$ с функцией распределения $Q(t)$.

При этом получение ответа от сервера происходит с вероятностью P_n. С вероятностью $(1 – P_n)$ запрос будет направлен повторно за среднее время $\overline{t_{rep}}$ с функцией распределения $Z(t)$.

Кроме того, с вероятностью $(1 – P_q)$ на атакуемый сервер может быть направлен некорректный, специально подобранный, запрос за среднее время $\overline{t_{unq}}$ с функцией распределения $O(t)$. В этом случае при наличии ошибок в удаленной системе возможно зацикливание процедуры обработки запроса и переполнение буфера с последующим зависанием серверов.

Стохастическая сеть, отражающая выше перечисленные этапы атаки «Отказ в обслуживании», представлена на рисунке 6.

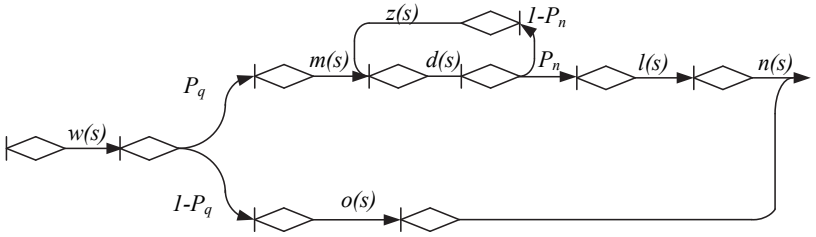

Рис. 6. Стохастическая сеть атаки «Отказ в обслуживании»

Порядок расчетов, по своей сути, аналогичен расчетам по предыдущей атаке. Поэтому сразу приведем расчетные выражения для интегральной функции распределения вероятностей и среднего времени реализации атаки. Функция распределения вероятностей $F(t)$ будет иметь следующий вид:

$$F(t)=\sum_{k=1}^{7}\frac{w\cdot P_q\cdot m\cdot P_n\cdot d\cdot l\cdot n\cdot(z+s_k)\cdot(o+s_k)+(1-P_q)\cdot o\cdot}{\phi(s_k)}$$

$$\cdot[(d+s_k)\cdot(l+s_k)\cdot(n+s_k)\cdot(m+s_k)\cdot(z+s_k)-(1-P_q)\cdot z\cdot m]\cdot\frac{1-\exp[s_k t]}{-s_k}$$

Среднее время $\overline{T}$, затрачиваемое на реализацию кибератаки, определяется следующим выражением:

$$\overline{T}=\sum_{k=1}^{7}\frac{w\cdot P_q\cdot m\cdot P_n\cdot d\cdot l\cdot n\cdot(z+s_k)\cdot(o+s_k)+(1-P_q)\cdot o\cdot}{\phi(s_k)}$$

$$\cdot[(d+s_k)\cdot(l+s_k)\cdot(n+s_k)\cdot(m+s_k)\cdot(z+s_k)-(1-P_q)\cdot z\cdot m]\cdot\frac{1}{(-s_k)^2}.$$

Результаты расчетов $F(t)$ и $\overline{T}$ представлены в виде зависимостей на рисунке 7. В качестве исходных данных используются следующие значения средних времен реализации этапов атаки «Отказ в обслуживании» и вероятности перехода пользователя по ссылке: $\overline{t_{start}}$ = 5 мин; $\overline{t_{que}}$ = 3 мин; $\overline{t_{srv}}$ = 1 мин; $\overline{t_{pack}}$ =9 мин; $\overline{t_{voil}}$ = 2 мин; $\overline{t_{rep}}$ = 3 мин; $\overline{t_{unq}}$ = 3 мин; P_n = 0.1–0.9; P_q = 0.5.

Анализ полученных зависимостей на рисунках 7*а* и 7*б* позволяет сделать вывод о том, что для реализации кибератаки «Отказ в обслуживании» с вероятностью P_n=0,1 требуется 77 минут и 20 минут при P_n=0,9. При этом снижение вероятности P_n от 1 до 0.6 не приводит к существенному увеличению времени реализации атаки. Начиная со значения 0.6, уменьшение вероятности P_n оказывает существенное влияние на увеличение времени реализации атаки, которое возрастает в конечном итоге почти в 4 раза.

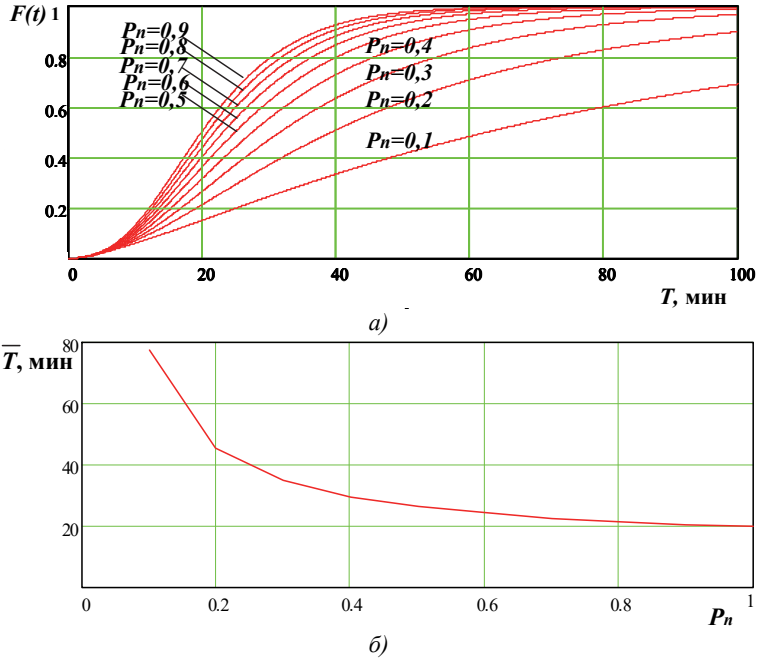

Рис. 7. Вероятностно-временные характеристики кибератаки типа «Отказ в обслуживании» (*а* – зависимость интегральной функции распределения вероятностей от времени реализации кибератаки; *б* – зависимость среднего времени реализации кибератаки от вероятности получения ответа от сервера)

Полученные зависимости позволяют оценить влияние вероятности получения ответов от сервера на подключение на значения функции распределения времени реализации атаки. Видно, что увеличение вероятности P_n уменьшает среднее время реализации кибератаки. Однако по

мере возрастания значения P_n степень влияния на интегральную функцию распределения $F(t)$ уменьшается, и при преодолении значения $P_n > 0{,}3$ степень этого влияния пренебрежимо мала.

6. Экспериментальная оценка киберустойчивости. С целью проверки полученных результатов проведен эксперимент. Для расчета коэффициента исправного действия в условиях воздействия кибератак была рассмотрена структура разветвленной компьютерной сети, включающая в себя персональные компьютеры (1000 шт.), коммутаторы (50 шт.), маршрутизаторы (15 шт.) и серверы (20 шт.).

Для расчета коэффициента исправного действия в условиях воздействия кибератак первоначально была проведена проверка особенностей вероятностно-временных характеристик на имитационном стенде. В состав имитационного стенда входили следующие модули: (1) ввода исходных данных, (2) генерации длительности этапов атаки, (3) менеджер. Модуль ввода исходных данных устанавливал значения $\overline{t_W}$, $\overline{t_L}$, $\overline{t_M}$, $\overline{t_D}$, $\overline{t_Z}$ и P_n. Модули генерации с помощью датчика случайных чисел формировали случайным образом времена реализации этапов атаки. Менеджер формировал случайное значение для времени реализации всей атаки. При этом использовались значения, полученные на выходах модулей генерации, и вероятность P_n.

Полученные экспериментальные результаты приведены в таблице 2. Для каждого значения P_n проводилось 100 экспериментов. При этом использовались значения средних времен реализации этапов атак, представленные на рисунке 5 и рисунке 7.

Таблица 2. Экспериментальные результаты

P_n	Среднее время моделирования, мин		Равномерное распределение		
	Сканирование сети	Отказ в облуживании	Среднее время, мин		Ошибка, %
			Сканирование сети	Отказ в облуживании	
0,2	140	48	146,1	50,1	4,4
0,3	90	35	89,4	34,75	0,7
0,4	70	30	72,9	31,2	4,2
0,5	60	27	62,4	28,1	4,1
0,6	50	23	50,7	23,3	1,3
0,7	45	22	45,7	22,2	1,5
0,8	40	21	41,3	21,7	3,3
0,9	35	20	35,6	20,4	1,8

Как видно из таблицы 2, погрешность оценки времени реализации атаки не превышает 5 процентов. Следовательно, предложенная аналитическая модель и метод ее формирования являются достаточно корректными и адекватными.

Используя эти вероятностно-временные характеристики, были получены зависимости коэффициента исправного действия от количества маршрутов, представленные на рисунке 8 и рисунке 9. В качестве исходных данных использовались следующие значения: $\alpha_i = 1$; $\overline{t_{ent}} = 3$ мин; $\overline{t_{tr}} = 1$ мин; $\overline{t_{de}} = 2$ мин; $\overline{t_{re}} = 10$ мин; $\overline{t_{CA}} = 13$ мин.

Полученные зависимости коэффициентов исправного действия от количества маршрутов позволяют определить рациональный диапазон количества потребных маршрутов при воздействии кибератак. Из рисунка 8 и рисунка 9 видно, что чем больше количество направлений связи в компьютерной сети, тем выше киберустойчивость сети, которая определяется значением коэффициента исправного действия. Это справедливо, так как при большом количестве направлений связи выход одного и даже нескольких из них из строя не приводит к полному пропаданию работоспособности сети.

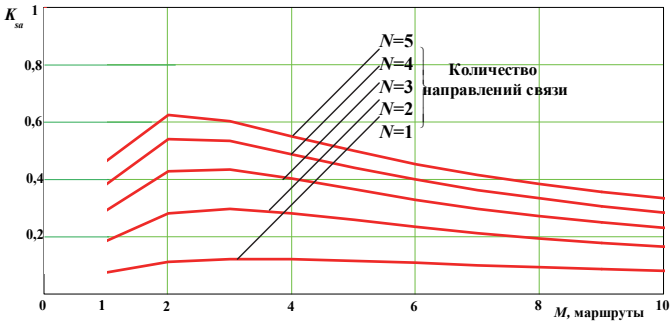

Рис. 8. Зависимость коэффициента исправного действия компьютерной сети от количества маршрутов и направлений связи

С другой стороны, киберустойчивость сети принимает максимальное значение при использовании для передачи информации от 2 до 5 маршрутов в зависимости от количества направлений связи в компьютерной сети. Это объясняется возможностью сформировать в сети обходные маршруты, по которым будет осуществляться передача данных в случае выхода из строя основных маршрутов. Однако дальнейшее увеличение количества маршрутов приводит к снижению киберустойчивости.

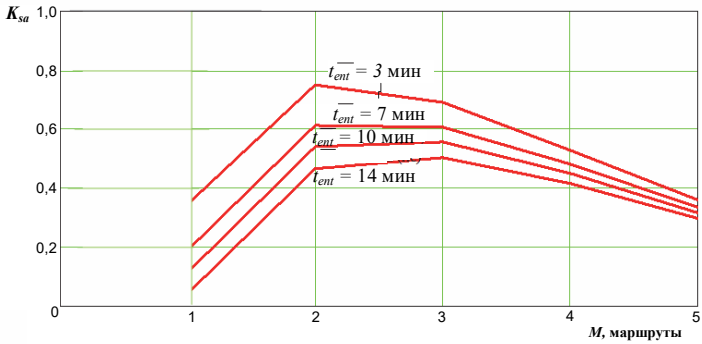

Рис. 9. Зависимость коэффициента исправного действия компьютерной сети от количества маршрутов и времени вхождения в связь

С другой стороны, киберустойчивость сети принимает максимальное значение при использовании для передачи информации от 2 до 5 маршрутов в зависимости от количества направлений связи в компьютерной сети. Это объясняется возможностью сформировать в сети обходные маршруты, по которым будет осуществляться передача данных в случае выхода из строя основных маршрутов. Однако дальнейшее увеличение количества маршрутов приводит к снижению киберустойчивости.

Этот неожиданный результат объясняется тем, что злоумышленник может использовать дополнительные маршруты для своих корыстных целей, что приведет к увеличению активности кибератак. При этом следует заметить, что снижение киберустойчивости сети при достаточно большом количестве маршрутов демонстрирует необходимость перехода от распределенной структуры компьютерной сети, пример которой представлен на рисунке 1, к структуре типа «звезда».

Кроме того, из рисунка 9 видно, что коэффициент исправного действия принимает максимальное значение в случае использования сетевых средств, обладающих наибольшей оперативностью. Иными словами, коммуникационные средства с большим временем вхождения в связь уменьшают киберустойчивость, так как при этом увеличивается время нахождения интервала на маршруте и маршрута в целом в неисправном состоянии. Этот вывод также следует из выражения (2), которое определяет порядок вычисления коэффициента исправного действия исходя из длительности отдельных этапов работы компьютерной сети в условиях воздействия кибератак.

Приведенные экспериментальные данные подтверждают достоверность и обоснованность предлагаемого метода и возможность его

использования для оценки киберустойчивости в компьютерных сетях, в которых определяющую роль играют коммуникационные сервисы.

7. Заключение. В настоящей статье предложен новый подход к аналитическому моделированию кибератак, основанный на методе преобразования стохастических сетей. Сущность данного подхода заключается в замене множества элементарных ветвей стохастической сети одной эквивалентной ветвью и последующем определении эквивалентной функции сети, а также начальных моментов и функции распределения случайного времени реализации кибератаки.

Проверка предложенного подхода произведена для моделирования кибератак типа «Сканирование сети и выявление ее уязвимостей» и «Отказ в обслуживании», которые являются одними из наиболее распространенных и опасных для компьютерных сетей.

Предложенный метод оценки устойчивости компьютерной сети в условиях кибератак, или киберустойчивости компьютерной сети, позволяет определить показатели, ее характеризующие, и обосновать ее наиболее устойчивую структуру. Применение эталонных моделей кибератак и метода преобразования стохастических сетей позволяет вычислить вероятностно-временные характеристики известных атак как исходные данные, необходимые для оценки угроз и обоснования требований по защите информации в сети.

Определяя дальнейшие направления исследований, следует отметить, что в представленном в статье подходе к оценке киберустойчивости было принято ограничение, согласно которому новая кибератака начинается через некоторое время после того, как была обнаружена предыдущая, и были устранены последствия ее реализации. Такой случай следует рассматривать как частный случай, при котором на компьютерную сеть воздействует только один злоумышленник. В реальности одновременно действующих злоумышленников может быть достаточно много, и кибератаки, активируемые ими, могут накладываться друг на друга. Такой случай проведения массированных кибератак следует считать одним из направлений дальнейших исследований.

Другое ограничение рассмотренного подхода связано с тем, что сценарии возможных атак заранее считаются известными, а сценарии реализации мер противодействия атак не рассматриваются. В то же время множество возможных сценариев противодействия кибератакам является конечным.

По этой причине можно построить аналитические модели для реализации контрмер и интегрировать их с аналитическими моделями кибератак. В результате получится интегрированная аналитическая модель поведения компьютерной сети в условиях кибервоздействий, поз-

воляющая оценивать и выбирать наиболее эффективные меры противодействия. Это направление следует также считать достаточно перспективным для дальнейших исследований.

Литература

1. *Luvanda A., Kimani S., Kimwele M.* Identifying Threats Associated With Man-In-The Middle Attacks during Communications between a Mobile Device and the Back End Server in Mobile Banking Applications // IOSR Journal of Computer Engineering (IOSR-JCI). 2014. vol. 12(2). pp. 35–42.
2. *Sterbenz J.P.G. et al.* Modelling and Analysis of Network Resilience // Proceedings of the Third IEEE International Conference on Communication Systems and Networks (COMSNETS). 2011. pp. 1–10.
3. *Sterbenz J.P.G. et al.* Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines // Computer Networks: Special Issue on Resilient and Survivable Networks (COMNET). 2010. vol. 54(8). pp.1245–1265.
4. *Smith P. et al.* Network resilience: a systematic approach // IEEE Communications Magazine. 2011. vol. 49(7). pp. 88–97.
5. *Ganin A.A. et al.* Operational resilience: Concepts, design and analysis // Scientific Reports. 2015. vol.6. Article 19540.
6. *Kelly F., Yudovina E.* Stochastic Networks // Cambridge University Press. 2014. 222 p.
7. *Котенко И.В., Саенко И.Б.* SIEM-системы для управления информацией и событиями безопасности // «Защита информации. Инсайд». 2012. № 5. С. 54–65.
8. *Котенко И.В., Саенко И.Б.* Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. Вып. 3(22). С.84–100.
9. *Саенко И.Б., Лаута О.С., Котенко И.В.* Применение метода преобразования стохастических сетей для моделирования мобильных банковских атак // Известия высших учебных заведений. Приборостроение. 2016. Т. 59. № 11. С. 928–933.
10. *Srikant R., Ying L.* Communication Networks: An Optimization, Control, and Stochastic Networks Perspective // Cambridge University Press. 2014. 363 p.
11. *Robert P.* Stochastic Networks and Queues // Springer Science & Business Media. 2013. 399 p.
12. *Williams J.* Laplace Transforms // Problem Solvers. George Allen & Unwin. 1973. 91 p.
13. *Van Valkenburg M.E.* Network Analysis: 3rd ed. // Englewood Cliffs. 1974. 571 p.
14. *Phillips D.T., Garsia-Diaz A.* Fundamentals of Network Analysis // Prentice-Hall. Englewood Cliffs. NJ. 1981. 474 p.
15. *Petrova S.S.* Heaviside and the development of the symbolic calculus // Archive for History of Exact Sciences. 1981. vol. 37(1). pp. 1–23.

Котенко Игорь Витальевич — д-р техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — 500. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7-(812)-328-71-81, Факс: +7(812)328–4450.

Саенко Игорь Борисович — д-р техн. наук, профессор, ведущий научный сотрудник лаборатории проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: автоматизированные информационные системы, информационная безопасность, обработка и передача данных по каналам связи, теория моделирования и математическая статистика, теория информации. Число научных публикаций — 350. ibsaen@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)328-7181, Факс: +7(812)328-4450.

Коцыняк Михаил Антонович — д-р техн. наук, профессор, профессор кафедры безопасности инфокоммуникационных систем специального назначения, Военная академия связи имени Маршала Советского Союза С.М. Будённого (ВАС им. Буденного). Область научных интересов: противодействие иностранным техническим разведкам. Число научных публикаций — 200. kot-c@yandex.ru; Тихорецкий проспект, 3, Санкт-Петербург, 194064; р.т.: +7(921)971-60-58.

Лаута Олег Сергеевич — к-т техн. наук, преподаватель кафедры безопасности инфокоммуникационных систем специального назначения, Военная академия связи имени Маршала Советского Союза С.М. Будённого (ВАС им. Буденного). Область научных интересов: защита от компьютерных атак. Число научных публикаций — 79. laos-82@yandex.ru; Тихорецкий проспект, 3, Санкт-Петербург, 194064; р.т.: +7(911)842-02-28.

Поддержка исследований. Работа выполнена при финансовой поддержке РНФ (проект № 15-11-30029).

DOI 10.15622/sp.55.7

I.V. KOTENKO, I.B. SAENKO, M.A. KOTSYNYAK, O.S. LAUTA

ASSESSMENT OF CYBER-RESILIENCE OF COMPUTER NETWORKS BASED ON SIMULATION OF CYBER ATTACKS BY THE STOCHASTIC NETWORKS CONVERSION METHOD

Kotenko I.V., Saenko I.B., Kotsynyak M.A., Lauta O.S. **Assessment of Cyber-Resilience of Computer Networks based on Simulation of Cyber Attacks by the Stochastic Networks Conversion Method.**

Abstract. The paper offers an approach for assessment of cyber-resilience of computer networks based on analytical simulation of computer attacks using a stochastic networks conversion method. The concept of cyber-resilience of computer networks is justified. The mathematical foundations of its assessment, allowing to calculate cyber-resilience indices by means of analytical expressions, are considered. The coefficient of serviceability on cyber-resilience is offered to be used as the key such indicator. The considered approach assumes the creation of analytical models of cyber-attacks. The method of the stochastic networks conversion is applied to create analytical models of cyber-attacks. The time distribution function and average time to implement cyber-attacks are the simulation results. These estimates are used then to search cyber-resilience indices. The experimental results of analytical simulation which showed that the offered approach has rather high accuracy and stability of the received solutions are given.

Keywords: cyber security, cyber-attacks, attack modeling, cyber-resilience, stochastic network, Laplace transform.

Kotenko Igor Vitalievich — Ph.D., Dr. Sci., professor, head of computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism. The number of publications — 500. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7-(812)-328-71-81, Fax: +7(812)328–4450.

Saenko Igor Borisovich — Ph.D., Dr. Sci., professor, leading researcher of computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: automated information systems, information security, processing and transfer of data on data links, theory of modeling and mathematical statistics, information theory. The number of publications — 350. ibsaen@comsec.spb.ru, http://www.comsec.spb.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-7181, Fax: +7(812)328-4450.

Kotsynyak Mikhail Antonovich — Ph.D., Dr. Sci., professor, professor of security of special-purpose infocommunication systems department, S.M. Budjonny Military Academy of the Signal Corps. Research interests: counteraction to foreign technical intelligence services. The number of publications — 200. kot-c@yandex.ru; Tikhoretsky avenue, 3, St. Petersburg, 194064, Russia; office phone: +7(921)971-60-58.

Lauta Oleg Sergeyevich — Ph.D., lecturer of security of special-purpose infocommunication systems department, S.M. Budjonny Military Academy of the Signal Corps. Research interests:

protection against the computer attacks. The number of publications — 79. laos-82@yandex.ru; Tikhoretsky avenue, 3, St. Petersburg, 194064, Russia; office phone: +7(911)842-02-28.
Acknowledgements. This research is supported by RSF (project № 15-11-30029).

References

1. Luvanda A., Kimani S., Kimwele M. Identifying Threats Associated With Man-In-The Middle Attacks during Communications between a Mobile Device and the Back End Server in Mobile Banking Applications. IOSR Journal of Computer Engineering (IOSR-JCI). 2014. vol. 12(2). pp. 35–42.
2. Sterbenz J.P.G. et al. Modelling and analysis of network resilience. Proceedings of the Third IEEE International Conference on Communication Systems and Networks (COMSNETS). 2011. pp. 1–10.
3. Sterbenz J.P.G. et al. Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines. Computer Networks: Special Issue on Resilient and Survivable Networks (COMNET). 2010. vol. 54(8). pp. 1245–1265.
4. Smith P. et al. Network resilience: a systematic approach. *IEEE Communications Magazine*. 2011. vol. 49(7). pp. 88–97.
5. Ganin A.A. et al. Operational Resilience: Concepts, Design and Analysis. *Scientific Reports*. 2015. vol.6. Article 19540.
6. Kelly F., Yudovina E. Stochastic Networks. Cambridge University Press. 2014. 222 p.
7. Kotenko I.V., Saenko I.B. [SIEM-systems for security information and event management]. *«Zashhita informacii. Insajd»* – «*Information protection. Inside»*. 2012. vol. 5. pp. 54–65. (In Russ.).
8. Kotenko I.V., Saenko I.B. [Developing the system of intelligent services to protect information in cyber warfare] *Trudy SPIIRAN – SPIIRAS Proceeding.* 2012. vol. 3(22). 2012. pp. 84–100. (In Russ.).
9. Saenko I.B., Lauta O.S., Kotenko I.V. [Application of a stochastic networks conversion method for modeling mobile banking attacks]. *Izv. vyssh. uchebn. zavedenij: Priborostroenie – Proceedings of the higher educational institutions: Instrumentation*. 2016. vol.11. pp. 928–933. (In Russ.).
10. Srikant R., Ying L. Communication Networks: An Optimization, Control, and Stochastic Networks Perspective. Cambridge University Press, 2014. 363 p.
11. Robert P. Stochastic Networks and Queues. Springer Science & Business Media. 2013. 399 p.
12. Williams J. Laplace Transforms. Problem Solvers. George Allen & Unwin, 1973. 91 p.
13. Van Valkenburg M.E. Network Analysis (3rd ed.). NJ: Prentice-Hall. 1974. 571 p.
14. Phillips D.T., Garsia-Diaz A. Fundamentals of Network Analysis. Prentice-Hall. Englewood Cliffs. NJ. 1981. 474 p.
15. Petrova S.S. Heaviside and the development of the symbolic calculus. *Archive for History of Exact Sciences*. 1981. vol. 37(1). pp. 1–23.