МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СЕТИ СВЯЗИ С НЕИЗВЕСТНЫМ УРОВНЕМ ДОВЕРИЯ И ОЦЕНКИ ЕЁ ВОЗМОЖНОСТЕЙ ПО ПРЕДОСТАВЛЕНИЮ УСЛУГИ VPN С ЗАДАННЫМ КАЧЕСТВОМ

Анисимов В.В.[1], Бегаев А.Н.[2], Стародубцев Ю.И.[3]

Использование виртуальных частных сетей позволяет обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети с меньшим или неизвестным уровнем доверия (например, Интернет). Использование криптографии позволяет защитить информацию от доступа, подмены и изменения. Наиболее эффективным в таком случае способом воздействия на логическую сеть со стороны злоумышленника является воздействие на узлы публичной сети для снижения качества обслуживания или прекращения информационного обмена между её абонентами (DDoS-атаки). Разработана аналитико-имитационная модель, одновременно учитывающая структурные и потоковые характеристики физической сети связи и развёрнутых на её основе логических сетей. Представленная модель позволяет имитировать функционирование сети связи в условиях DDoS-атак и получать зависимости количества узлов сети связи, производительности которых недостаточно для обеспечения услуг связи с заданным качеством, а также определять необходимое увеличение производительности критических узлов. С помощью модели можно решать задачи по выявлению слабых мест в существующих физических и логических сетях, по управлению и модернизации сети связи, при планировании развёртывания и заблаговременной подготовке к эксплуатации сети связи.

Ключевые слова: сетевая структура, сетевой поток, критический узел, сеть связи, вероятность обслуживания, сетевой мониторинг, отказ в обслуживании, инкапсуляция, виртуальная частная сети, уровень доверия, криптографическая защита сообщения.

DOI: 10.21681/2311-3456-2017-1-6-15

Введение

Для управления важными системами развёртываемая система связи должна отвечать заданным к ней требованиям, например, по своевременности и вероятности обслуживания, по пропускной способности. При территориальном разносе элементов системы рационально использовать ресурсы сетей связи общего пользования Единой сети электросвязи РФ. В таком случае, сочетание технологий VPN и IPsec позволяет обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети с меньшим или неизвестным уровнем доверия [1, 2]. Уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии.

Существующие сети связи обслуживают значительное число абонентов, малая часть которых также принадлежит логическим сетям VPN с заданным требованиям. Используя средства сетевого мониторинга, злоумышленник с определённой долей вероятности к определённому моменту времени сможет выявить из общего информационного обмена, поток сообщений между абонентами сети VPN. Благодаря использованию средств криптографии он не получит доступа к семантической части сообщения. Наиболее эффективным в таком случае является воздействие на узлы публичной сети для снижения качества обслуживания или прекращения информационного обмена между её абонентами (DDoS-атаки) [2-6].

Требуется разработать модель, в которой учитываются структурные и потоковые характеристики физической сети и развёрнутой поверх её логической сети, а также их взаимосвязь. Целью моделирования является получение зависимо-

1 Анисимов Василий Вячеславович, Военная академия связи им. С.М.Будённого, г. Санкт-Петербург, Anisimov.VV-vas@yandex.ru

2 Бегаев Алексей Николаевич, кандидат технических наук, ЗАО «Эшелон-СЗ», г. Санкт-Петербург, a.begaev@nwechelon.ru

3 Стародубцев Юрий Иванович, доктор военных наук, профессор, Военная академия связи им. С.М.Будённого, г. Санкт-Петербург, ys@e-nw.ru

стей количества узлов сети связи, производительности которых недостаточно для обеспечения услуги VPN с заданным качеством, от структуры сети связи, производительности её узлов, количества всех абонентов и создаваемой ими нагрузки на сеть связи, количества абонентов, использующих услугу VPN, их привязки к узлам сети связи и информационных направлений между ними, а также необходимое увеличение производительности выявленных узлов.

Постановка задачи на исследование.

Выходным результатом является множество пар $W_z(v,w) = \{(v_1,w_1);(v_2,w_2);\dots;(v_n,w_n)\}$, где $v_i, i = \overline{1,n}$ — узлы сети связи, $w_i, i = \overline{1,n}$ — необходимое увеличение производительности узлов для обеспечения услуги VPN с заданным качеством.

Основными исходными данными модели являются: $G(V,E)$ — граф, задающий структуру сети связи, где V — множество узлов сети связи $v, v \in V$, и E — множество линий связи между узлами сети связи u и v, $(u,v) \in E, \{u,v\} \in V$; $\Pr(v,\mu_v)$ — множество, задающее производительность μ_v каждого узла сети связи v, $v \in V$; $F_{P_b}(v)$ — модель функционирования узла сети связи v, $v \in V$; $N_{\text{польз}}$ — количество абонентов сети связи (пользователи), не использующие сеть VPN; $L_G = (m,v)$ — множество $m = \overline{1,N_{\text{польз}}}$, задающее привязку пользователей к узлам сети связи v, $v \in V$; $\Lambda_G(m,\lambda_m)$ — множество, задающее нагрузку от каждого пользователя в виде интенсивности потока сообщений λ_m от m-го пользователя; $F_\lambda(t)$ — закон распределения интенсивности потока λ_m; M_G — матрица информационных направлений между пользователями размерности $N_{\text{польз}} \times N_{\text{польз}}$; $F_{M_G}(i,j)$ — закон формирования матрицы информационных направлений между пользователями, $i \neq j$, $i = \overline{1,N_{\text{польз}}}$, $j = \overline{1,N_{\text{польз}}}$; $N_{\text{аб}}$ — количество абонентов сети связи (абонентов), использующих сеть VPN; $L_{\text{аб}}(n_{\text{аб}},v)$ — множество, задающее привязку абонентов $n_{\text{аб}}$, $n_{\text{аб}} = \overline{1,N_{\text{аб}}}$ к узлам сети v, $v \in V$; $\Lambda_{\text{аб}}(n_{\text{аб}},\lambda_{n_{\text{аб}}})$ — множество, задающее нагрузку от каждого абонента в виде интенсивности потока $\lambda_{n_{\text{аб}}}$ от $n_{\text{аб}}$-го абонента; $M_{\text{аб}}$ — матрица информационных направлений между абонентами размерности $N_{\text{аб}} \times N_{\text{аб}}$; $P^q_{\text{треб}}$ — требуемая вероятность обслуживания на q-м информационном направлении из матрицы $M_{\text{аб}}$ информационных направлений.

Основными допущениями и ограничениями являются: структура сети связи задана и неизменна; узлы сети связи характеризуются заданной производительностью; для передачи сообщений между абонентами сети связи выбирается кратчайший маршрут по известному алгоритму; абоненты характеризуются только привязкой к узлу сети связи, интенсивностью и направлением информационного обмена; повышение производительности узлов сети связи происходит одновременно на определённое значение для каждого узла.

Алгоритм моделирования функционирования сети связи, с учётом нагрузки от пользователей

Моделирование функционирования сети связи, с учётом нагрузки от пользователей реализовано в виде алгоритма (рис. 1). Ниже описаны ключевые этапы алгоритма, которые раскрывают взаимосвязь структурных и потоковых характеристик.

В блоке 1 задают исходные данные. Исходными данными является фрагмент сети связи, топологически инвариантный реальному фрагменту сети связи [7, 6]. Задают количество разнородных абонентов $N_{\text{разнород}}$:

$$N_{\text{разнород}} = N_{\text{аб}} + N_{\text{польз}} \quad (1)$$

Задают распределение разнородных абонентов по узлам сети связи.

Задают нагрузку от каждого пользователя в виде интенсивности потока λ_m и закон её распределения $F_\lambda(t)$. Интенсивностью потока называют математическое ожидание числа событий в единицу времени в данный момент. Например, для пуассоновского (простейшего) потока закон распределения задаётся выражением [9]:

$$P_i(t) = \frac{(\lambda t)^i}{i!} e^{-\lambda t}, \quad (2)$$

а для нормального распределения выражением [10]:

$$P(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(t-\lambda)}{2\sigma^2}} \quad (3)$$

Задают закон формирования матрицы информационных направлений между пользователями. Задают требуемую вероятность обслуживания для каждого информационного направления $P^q_{\text{треб}}$, производительность для каждого узла сети связи $\mu_j = \frac{1}{\bar{x}}$, где $\bar{x}$ — среднее время обслуживания в узле сети связи.

Задают K — количество статистических экспериментов.

В блоке 8 рассчитывают кратчайший маршрут между пользователями q-го информационного направления, например, по известному алгоритму Дейкстры.

В блоке 9 рассчитывают и запоминают нагрузку на каждом узле маршрута:

$$\lambda_{jq} = \lambda_{q_1}^{\text{польз}} + \lambda_{q_2}^{\text{польз}} \quad (4)$$

где λ_{jq} — нагрузка на j-й узел сети связи, входящий в маршрут -го информационного направления, $\lambda_{q_1}^{\text{польз}}$ и $\lambda_{q_2}^{\text{польз}}$ — нагрузка от пользователей q-го информационного направления.

Если значение счётчика номера информационного направления больше количества информационных направлений между пользователями, то в блоке 11 рассчитывают нагрузку для каждого узла сети связи и запоминают её:

$$\lambda_j = \sum_{q=1}^{N_{\text{инф.напр}}^{q}} \lambda_{j_q} \quad (5)$$

где λ_j^k — нагрузка -го узла сети связи в k-ом статистическом эксперименте.

В блоке 12 увеличивают значение счётчика количества статистических экспериментов на «1» и начинают новый статистический эксперимент.

Если значение счётчика больше количества статистических экспериментов, то в блоке 13 рассчитывают среднюю нагрузку для каждого узла сети связи:

$$\lambda_j = \frac{1}{K}\sum_{k=1}^{K} \lambda_j^k, \quad (6)$$

В блоке 14 рассчитывают вероятность обслуживания на каждом узле сети связи и прекращают моделирование. Рассчитывают вероятность обслуживания P_j: $P_j = 1 - P_b$, где $j = 1,2,\dots,J$, J–– количество узлов в сети связи, P_b— вероятность блокировки b-го узла. Расчёт вероятности блокировки P_b зависит от принятой модели функционирования узла. Например, для системы с полными потерями, состоящей из m-серверов, рассчитывается по формуле потерь Эрланга:

$$P_b = \frac{\frac{\rho^m}{m!}}{\sum_{k=0}^{m}\frac{\rho^k}{k!}} \quad (7)$$

где $\rho = \frac{\lambda_j}{\mu_j}$, λ_j — нагрузка на j-м узле сети связи, μ_j — производительность -го узла сети связи.

Для системы M/M/1:N рассчитывается по формуле:

$$P_b = \frac{(1-\rho)\rho^N}{1-\rho^{N+1}} \quad (8)$$

где N — размер буфера.

Алгоритм расчёта вероятности обслуживания на каждом информационном направлении между абонентами и изменения параметров модели под заданные требования

Расчёт вероятности обслуживания на каждом информационном направлении между абонентами и изменение параметров модели под заданные требования реализовано в виде алгоритма (рис. 2). Ниже описаны ключевые этапы алгоритма, которые раскрывают взаимосвязь структурных и потоковых характеристик.

В блоке 1 вводят исходные данные: распределение разнородных абонентов по узлам сети связи, матрица информационных направлений между абонентами и др.

В блоке 4 рассчитывают все возможные маршруты между абонентами текущего информационного направления и запоминают их [11].

В блоке 5 рассчитывают вероятность обслуживания на каждом маршруте и запоминают их. Т.к. вероятность обслуживания на каждом узле сети связи — событие l-независимое, то вероятность обслуживания на -м маршруте рассчитывается по формуле:

$$P_l = \prod_{z_l=1}^{L} P_{z_l} \quad (9)$$

где $l = 1,2,\dots,L$, L — количество маршрутов в i-м информационном направлении, z_l— количество узлов сети связи в -м маршруте.

В блоке 6 рассчитывают вероятность обслуживания на текущем информационном направлении, включающем себя L маршрутов, по формуле, согласно теореме сложения вероятностей:

$$P\left(\sum_{l=1}^{L} P_l\right) = \sum_{i} P(P_i) - \sum_{i,j} P(P_iP_j) + \sum_{i,j,k} P(P_iP_jP_k) - \dots + \\ + (-1)^{n-1}P(P_1P_2\dots P_n) \quad (10)$$

Если значение вероятности обслуживания на информационном направлении меньше требуемой, то в блоке 9 формируют вариационный ряд, состоящий из вероятности обслуживания на узлах P_z, входящих в маршруты текущего информационного направления.

В блоке 10 рассчитывают разницы $\Delta_{i,i-1}$ между значениями членов вариационного ряда и запоминают их.

В блоке 11 рассчитывают среднюю разницу между значениями членов вариационного ряда и запоминают её. Среднее значение изменения

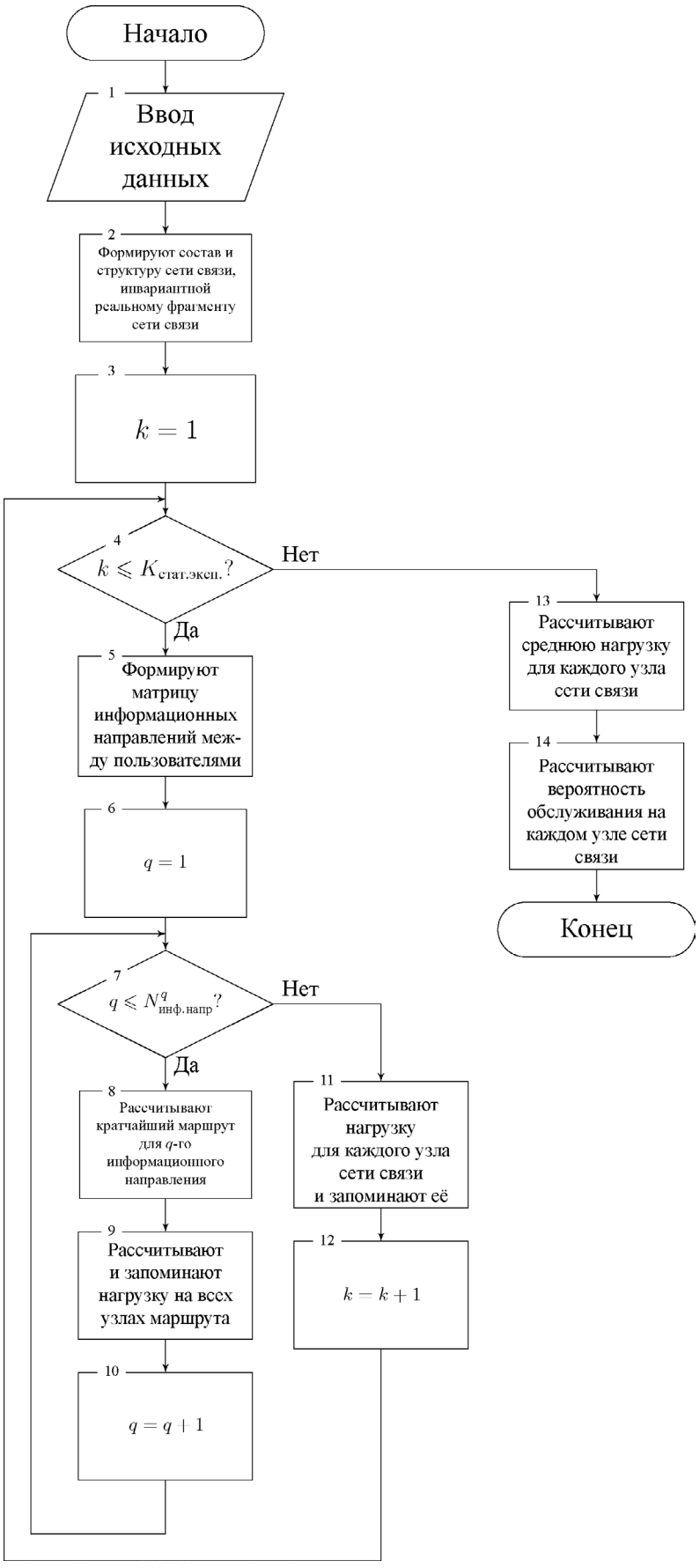

***Рис. 1** Блок-схема алгоритма моделирования функционирования сети связи с учётом нагрузки от пользователей*

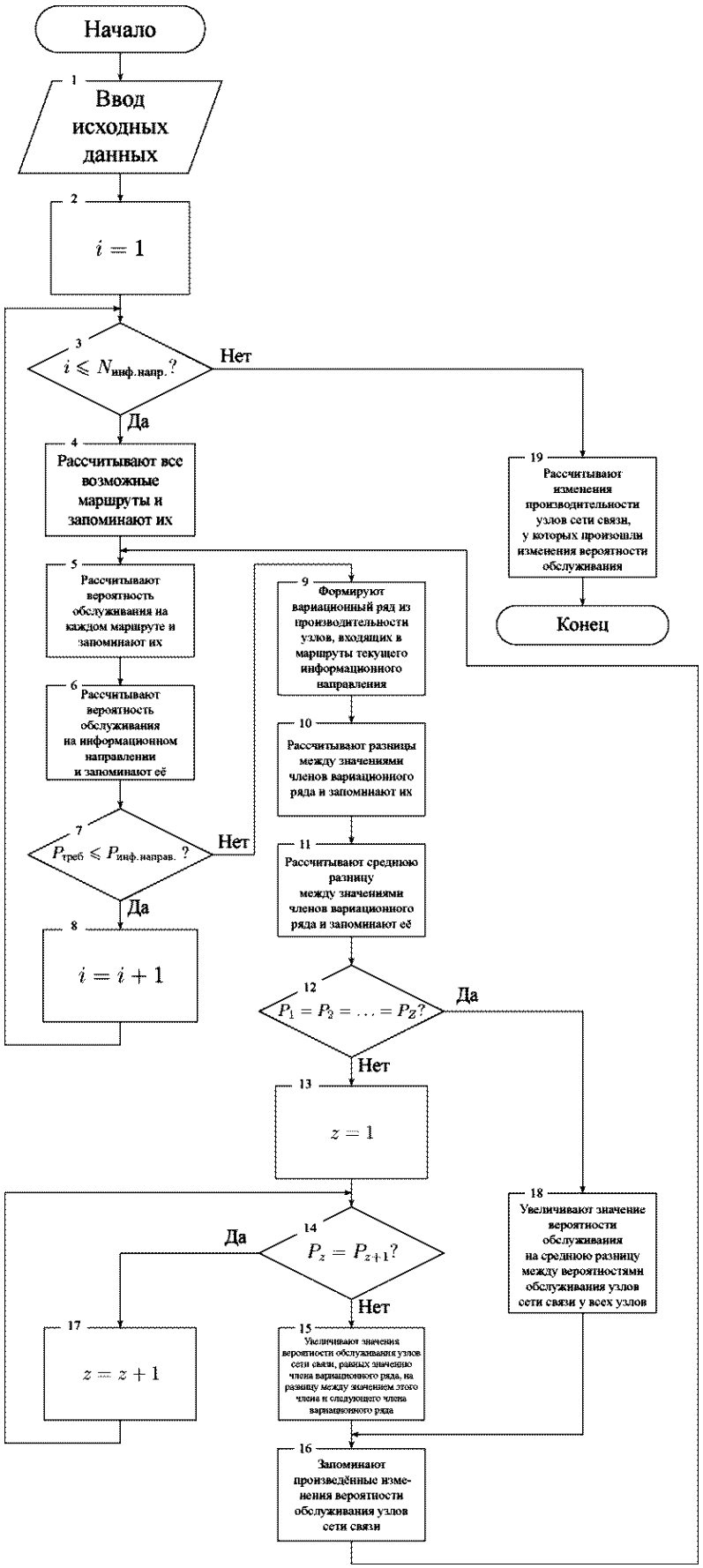

Рис. 2 *Блок-схема алгоритма расчёта вероятности обслуживания на каждом информационном направлении между абонентами и изменения параметров модели под заданные требования*

вероятности обслуживания узлов производится по формуле:

$$\bar{\Delta} = \frac{1}{N-1}\sum_{i=1}^{N-1}\Delta_{i,i+1} \qquad (11)$$

где N — количество членов вариационного ряда.

В блоке 15 значения увеличивают вероятности обслуживания узлов сети связи, равных значению текущего члена вариационного ряда, на разницу между значением этого члена и следующего члена вариационного ряда.

Если значения вероятностей обслуживания на узлах сети связи станут равны между собой, то в блоке 18 увеличивают значение вероятности обслуживания на среднюю разницу между вероятностями обслуживания узлов сети связи у всех узлов, входящих в маршруты текущего информационного направления. Изменения параметров модели производят до тех пор, пока вероятность обслуживания на текущем информационном направлении будет не меньше требуемой, для чего переходят к блоку 5.

Реализация модели

Алгоритм был реализован в программной среде имитационного моделирования «AnyLogic 7». Результаты оценки качества разработанной модели удовлетворяют общепринятым требованиям.

На имитационной модели была проведена серия экспериментов, которые можно разделить на четыре группы – исследование зависимости качества функционирования сети VPN:

1. от общей потоковой нагрузки на сеть связи;
2. от собственной потоковой нагрузки;
3. от собственной потоковой структуры;
4. от структуры сети связи.

Принятым показателем качества функционирования сети VPN в модели является отношение критических узлов сети связи к общему количеству узлов в сети связи. Под критическим узлом сети связи понимается узел сети связи, производительности которого недостаточно для функционирования сети VPN, удовлетворяющей требованию $P^{q}_{\text{треб}}$. Для экспериментов принято $P^{q}_{\text{треб}} = 0{,}95$.

К первой группе относятся серии экспериментов, в ходе которых последовательно увеличивалось количество узлов сети связи (рис. 3). Для моделирования сети с заданным количеством узлов сети, программой генерировался безмасштабный граф Барабаши-Альберта с параметром $m = 2$. Граф БА-2 достаточно точно описывает структуры сетей, например, Интернет, на сетевом уровне ЭМВОС [1, 11].

Исходными данными для каждого эксперимента были:

$$N_{\text{узлов}} = 19;$$

$$\mu_{v} \approx 3 \;\forall\, v \in V;$$

$$\lambda_{m} \cong \lambda_{n_{\text{аб}}};$$

$$N_{\text{аб}} = 23;$$

$$M_{\text{аб}} = const;$$

$$N_{\text{польз}} \approx 23 \times N_{\text{узлов}}.$$

Количество пользователей растёт с количеством узлов. С количеством пользователей пропорционально растёт нагрузка в сети. При дости-

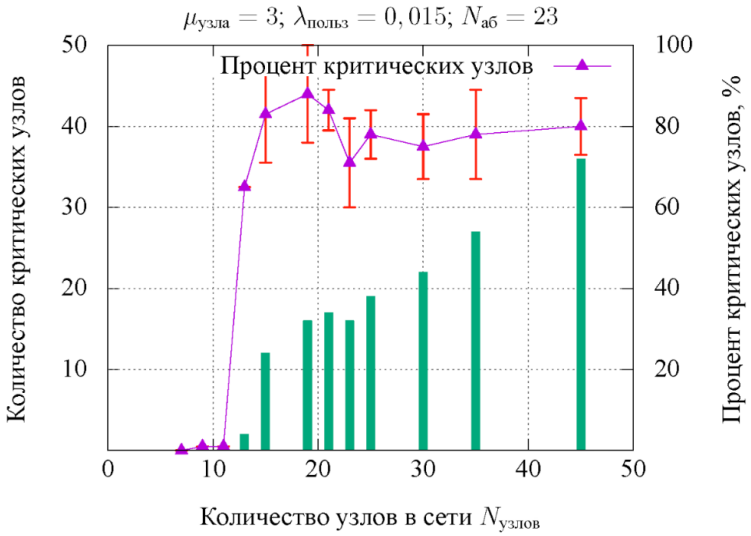

***Рис. 3** Зависимость количества критических узлов от общего количества узлов в сети при $\lambda_{\text{польз}} = 0{,}015$*

жении определённого значения нагрузка в сети становится критичной для функционирования сети VPN. Т.к. $N_{аб} > N_{узлов}$, то количество критических узлов в этот момент составляет около 90% от общего числа узлов сети связи. С ростом количества узлов сеть связи лучше распределяет нагрузку, но количество критических узлов уменьшается не сильно и составляет 70%–80% от общего количества узлов в сети.

Характер изменения качества функционирования сети VPN не зависит от нагрузки, создаваемой каждым пользователем сети связи. От неё зависит момент ухудшения качества функционирования сети VPN (при $\lambda_{польз} = 0{,}005$ $N_{узлов} = 19$; при $\lambda_{польз} = 0{,}015$ $N_{узлов} = 15$) и необходимое увеличение производительности выявленных узлов (рис. 4).

Ко второй группе экспериментов относятся эксперименты, в ходе которых последовательно увеличивалось количество абонентов сети VPN (рис. 5).

При проведении экспериментов структура сети, количество пользователей, создаваемая ими нагрузка не менялись.

К третьей группе экспериментов относятся эксперименты, в ходе которых последовательно увеличивалось количество информационных направлений между абонентами сети VPN (рис. 6).

При проведении экспериментов структура сети, количество пользователей, количество абонентов, распределение их по узлам сети связи и создаваемая ими нагрузка не изменялись.

К четвёртой группе экспериментов относятся эксперименты, которые при одинаковых исход-

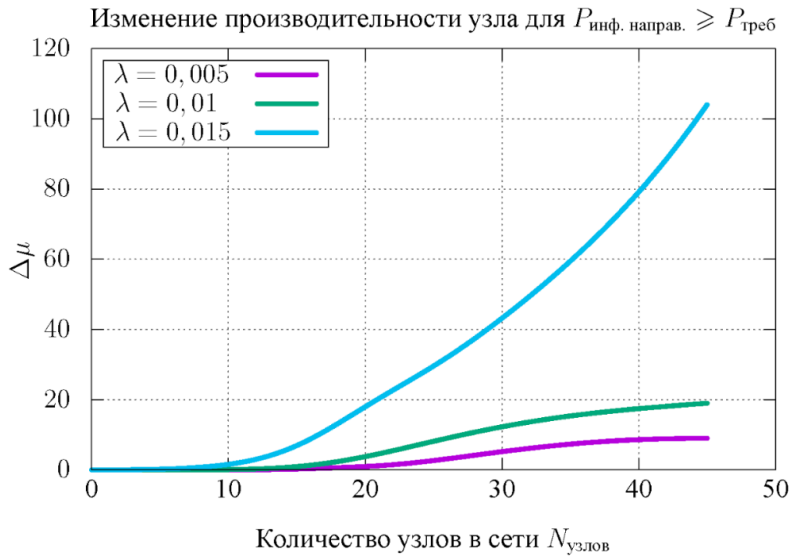

Рис. 4 *Зависимость увеличение производительности выявленных критических узлов от общего общей потоковой нагрузки $\lambda_{польз}$ в сети*

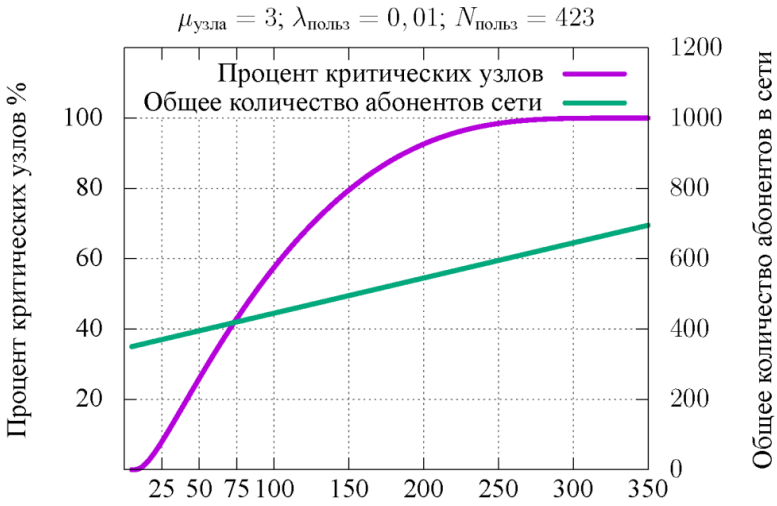

Рис. 5 *Зависимость количества критических узлов от количества абонентов сети VPN $N_{аб}$*

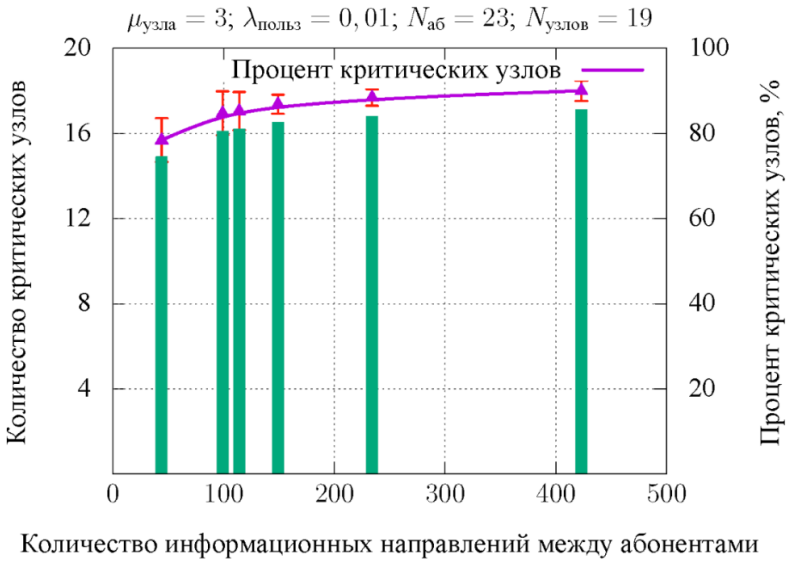

***Рис. 6** Зависимость количества критических узлов от количества информационных направлений между абонентами сети VPN*

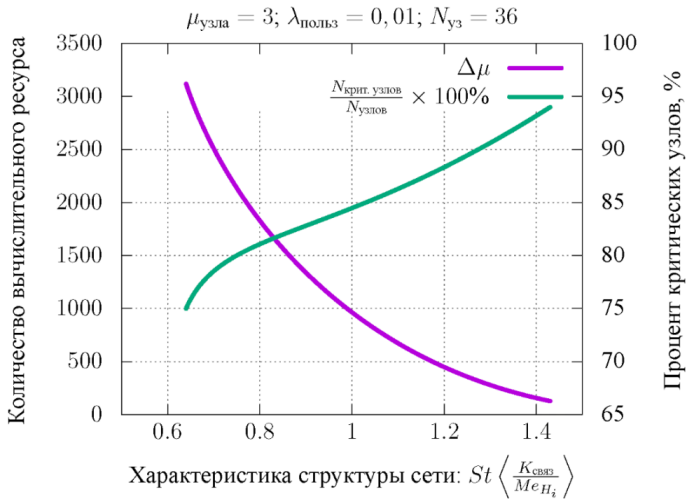

***Рис. 7** Зависимость количества вычислительного ресурса от характеристики структуры сети*

ных данных проводились на графах сети связи разной структуры (рис. 7).

Общими исходными данными для каждого эксперимента были:

$N_{узлов} = 36; N_{аб} = 23;$

$N_{польз} \approx 23 \times N_{узлов}.$

$\mu_v \approx 3\ \forall\ v \in V; \lambda_m \cong \lambda_{n_{аб}};$

$L_G = const; \quad M_G = const; \quad L_{аб} = const;$

$M_{аб} = const;$

Для исходных данных были сгенерированы четыре структуры сети связи с $N_{узлов} = 36$:

1. граф Барабаши-Альберта с $m = 2$;

2. граф — остовое дерево сгенерированного графа БА-2;

3. граф Барабаши-Альберта с $m = 3$;

4. регулярная решётка.

Количество пользователей и абонентов сети VPN, их распределение на узлах сети связи были одинаковыми для всех сетей связи с разными структурами. В качестве характеристики структуры сети взято отношение:

$$St = \frac{K_{связ}}{Me_{H_i}}, \qquad (12)$$

где $K_{связ}$ — линейный функционал связанности, Me_{H_i} — среднее ме[illegible] значение степеней (рангов, валентнос[illegible] (вершин) сети связи (графа). Отношение $St\left\langle\frac{K_{связ}}{Me_{H_i}}\right\rangle$ характеризует способность сети распределять нагрузку по своей структуре. Линейный функционал связанности рассчитывается по формуле:

Таблица 1

Характеристика структуры сети связи

№ п/п	Тип графа сети связи	$K_{связ}$	Me_{H_i}	$St\langle\frac{K_{связ}}{Me_{H_i}}\rangle$
1	БА-2	3,97	5,5	0,72
2	Остовое дерево	2,92	4,5	0,64
3	БА-3	5,77	6	0,96
4	Регулярная решётка	4,31	3	1,43

$$K = \sum_{i=1}^{N} \alpha_i \left[\frac{H_i}{N - N_i} + \frac{N_i}{N}\right] \quad (13)$$

где α_i — коэффициент веса -го узла; i — номер узла в сети связи; N — общее количество узлов сети связи; H_i — степень узла в сети связи; N_i — число узлов, с которыми i-й узел может быть иметь связь в сети связи. Для всех структур связи были рассчитаны характеристики сети при условиях, что граф сети полносвязанный ($N_. = N - 1$) и узлы сети равноценны ($\alpha_i = \frac{1}{N} = const$) (табл. 1).

Несмотря на то, что количество критических узлов растёт с $St\langle\frac{K_{связ}}{Me_{H_i}}\rangle$, необходимое увеличение производительности выявленных узлов уменьшается (в отличии от экспериментов первой группы).

Выводы

Научная новизна разработанной модели заключается в одновременном учёте структурных и потоковых характеристик физической сети связи и развёрнутых на её основе логических сетей. Модель позволяет имитировать функционирование сети связи с разнородными абонентами в условиях DDoS-атак и получать зависимости количества критических узлов сети связи, производительности которых недостаточно для обеспечения услуг связи с заданным качеством от основных структурных и потоковых характеристик физической и логической сети, а также определять необходимое увеличение производительности критических узлов.

Последовательность действий, представленная в модели, реализована в заявке на предполагаемое изобретение «Способ целенаправленной трансформации модели» №2016119980 от 23.05.2016. Разработана программа для ЭВМ. Модель повышает адекватность моделирования функционирования сети связи путём учёта нагрузки, создаваемой неоднородными абонентами, и определение параметров сети связи, при которых обеспечивается обслуживание абонентов с заданным качеством.

Представленное научно-методическое обеспечение является основой для разработки подходов и научно-технических предложений по выявлению слабых мест в существующих физических и логических сетях, по управлению и модернизации сети связи, при планировании развёртывания и заблаговременной подготовке к эксплуатации сети связи.

***Рецензент**: Куделя Виктор Николаевич, доктор технических наук, профессор, главный специалист АО «Институт сетевых технологий», kvn@int.spb.ru*

Литература

1. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под ред. А. С. Маркова. - М.: ДМК Пресс, 2017. 224 с.
2. Гречишников Е.В., Добрышин М.М., Закалкин П.В. Модель узла доступа VPN как объекта сетевой и потоковой компьютерных разведок и DDoS-атак // Вопросы кибербезопасности. 2016. № 3 (16). С. 4-12.
3. Калашников А.О., Бурса М.В., Остапенко Г.А. Мультисервисные сети: дискретная риск-модель HTTP-флуда // Вопросы кибербезопасности. 2015. № 1 (9). С. 49-54.
4. Петренко А.А., Петренко С.А. Способ повышения устойчивости LTE-сети в условиях деструктивных кибератак // Вопросы кибербезопасности. 2015. №2 (10). С. 36-42.
5. Стародубцев Ю. И., Чукариков А. Г., Анисимов В. В. Объективные условия превентивной защиты инфо-телекоммункационной системы // Актуальные проблемы защиты и безопасности: Труды восемнадцатой Всероссийской научно-практической конференции. Том 5. Проблемы безопасности инфо-телекоммуникационных систем специального назначения. — СПб.: РАРАН, 2015. С. 140-145.
6. Чукариков А. Г., Анисимов В. В. Математическая формализация обеспечения превентивной защиты инфо-телекоммуникационных систем // Актуальные проблемы защиты и безопасности: Труды девятнадцатой Всероссийской научно-практической конференции. Том 1. Вооружение, военная и специальная техника. — СПб.: РАРАН, 2016. С. 203–209.
7. Способ моделирования сетей связи / Алисевич Е.А., Синев С.Г., Стародубцев П.Ю., Сухорукова Е.В., Чукариков А.Г., Шаронов А.Н. Патент на изобретение RUS 2546318 04.02.2014.
8. Стародубцев Ю.И., Сухорукова Е.В., Чукариков А.Г. Методика выявления критически важных элементов информационно-телекоммуникационных систем // Проблемы экономики и управления в торговле и промышленности. 2014. № 1. С. 95-101.

9. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.
10. Крылов В. В., Самохвалова С. С. Теория телетрафика и ее приложения. — СПб.: БХВ-Петербург, 2005. — 288 с.
11. Кристофидес Н. Теория графов. Алгоритмический подход / под ред. Г. П. Гаврилова ; пер. с англ. Э. В. Вершкова, И. В. Коновальцева. — М.: Издательство «Мир», 1978. — 432 с.

FUNCTIONAL MODEL FOR COMMUNICATION NETWORK WITH UNKNOWN ASSURANCE LEVEL AND EVALUATION OF ITS CAPABILITIES OF RENDERING VPN SERVICE OF THE SET QUALITY

Anisimov V.V.[4], Begaev A.N.[5], Starodubtsev Y.I.[6]

Abstract. The use of virtual private networks allows for one or more network connections (logical network) above the other network with lower or unknown assurance level (for instance, Internet). Cryptography protects information from access, substitution or change. The most effective means for the 'hacker' to impact the logic network is to affect the public network nodes to lower the quality of service or terminate information exchange between its subscribers (distributed denial-of-service attacks, DDoS attacks). We have developed an analytical simulation model that simultaneously takes into account structural and streaming properties of a physical communication network and logical networks developed on its basis. The presented model allows simulating operation of the network in the conditions of DDoS-attacks and finding out dependence of the number of the communication network nodes, which performance is not sufficient to assure the set quality of communication, and determining the necessary increase in performance of the critical nodes. This model can help to identify vulnerabilities in the available physical and logical networks, manage and upgrade the communication network, plan deployment of the communication network and its timely preparation for operation.

Keywords: network structure, network flow, critical node, communication network, likelihood of service, network monitoring, denial of service, encapsulation, virtual private network, level of trust, cryptographic protection posts.

References

1. Barabanov A.V., Dorofeev A.V., Markov A.S., Tsirlov V.L. Sem' bezopasnykh informatsionnykh tekhnologiy (Seven information security technologies), by ed. A.S. Markov, Moscow, DMK, 2017, 224 p.
2. Grechishnikov E.V., Dobryshin M.M., Zakalkin P.V. Model' uzla dostupa vpn kak ob"ekta setevoy i potokovoy komp'yuternykh razvedok i DDoS-atak, Voprosy kiberbezopasnosti [Cybersecurity issues], 2016, No 3 (16), pp. 4-12.
3. Kalashnikov A.O., Bursa M.V., Ostapenko G.A. Mul'tiservisnye seti: diskretnaya risk-model' HTTP-fluda, Voprosy kiberbezopasnosti [Cybersecurity issues], 2015, No 1 (9), pp. 49-54.
4. Petrenko A.A., Petrenko S.A. Sposob povysheniya ustoychivosti LTE-seti v usloviyakh destruktivnykh kiberatak, Voprosy kiberbezopasnosti [Cybersecurity issues], 2015, No 2 (10), pp. 36-42.
5. Starodubtsev Yu. I., Chukarikov A. G., Anisimov V. V. Ob"ektivnye usloviya preventivnoy zashchity info-telekommunkatsionnoy sistemy, Aktual'nye problemy zashchity i bezopasnosti: Trudy vosemnadtsa-toy Vserossiyskoy nauchno-prakticheskoy konferentsii. Tom 5. Problemy bezopasnosti info-telekommunikatsionnykh sistem spetsial'nogo naznacheniya, St-Peterburg, RARAN, 2015, pp. 140-145.
6. Chukarikov A. G., Anisimov V. V. Matematicheskaya formalizatsiya obespecheniya preventivnoy zashchi-ty info-telekommunikatsionnykh sistem, Aktual'nye problemy zashchity i bezopasnosti: Trudy devyatna-dtsatoy Vserossiyskoy nauchno-prakticheskoy konferentsii. Tom 1. Vooruzhenie, voennaya i spetsial'naya tekh-nika, St-Peterburg, RARAN, 2016, pp.203-209/
7. Sposob modelirovaniya setey svyazi / Alisevich E.A., Sinev S.G., Starodubtsev P.Yu., Sukhorukova E.V., Chukarikov A.G., Sharonov A.N. Patent RUS 2546318 04.02.2014.
8. Starodubtsev Yu.I., Sukhorukova E.V., Chukarikov A.G. Metodika vyyavleniya kriticheski vazhnykh ele-mentov informatsionno-telekommunikatsionnykh sistem, Problemy ekonomiki i upravleniya v torgovle i promyshlennosti, 2014, No 1, pp. 95-101.
9. Markov A.S., Tsirlov V.L., Barabanov A.V. Metody otsenki nesootvetstviya sredstv zashchity informatsii, Moscow, Radio i svyaz', 2012. 192 p.
10. Krylov V. V., Samokhvalova S, pp. Teoriya teletrafika i ee prilozheniya. St-Peterburg, BKhV-Peterburg, 2005. 288 p.
11. Kristofides N. Teoriya grafov. Algoritmicheskiy podkhod, by ed. G. P. Gavrilova ; per. s angl. E. V. Vershkova, I. V. Konoval'tseva, Moscow, Izdatel'stvo Mir, 1978, 432 p.

4 Vasiliy Anisimov, Federal State Public Educational Institution of Higher Professional Education Military Telecommunication Academy named after the Soviet Union Marshal Budienny S. M., Saint-Petersburg, Anisimov.VV-vas@yandex.ru

5 Alexey Begaev, Ph.D., CJSC «North-West Echelon», Saint-Petersburg, a.begaev@nwechelon.ru

6 Yuriy Starodubtsev, Dr.Sc., Professor, Federal State Public Educational Institution of Higher Professional Education Military Telecommunication Academy named after the Soviet Union Marshal Budienny S. M., Saint-Petersburg, ys@e-nw.ru