МОДЕЛЬ, ОПТИМИЗАЦИЯ И ОЦЕНКА ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ МНОГОАДРЕСНЫХ СЕТЕВЫХ СОЕДИНЕНИЙ В УСЛОВИЯХ СЕТЕВОЙ РАЗВЕДКИ

Москвин А.А.[1], Максимов Р.В.[2], Горбачёв А.А.[3]

Цель исследования: *разработка моделей повышения доступности сетевых устройств вычислительной сети при смене их структурно-функциональных характеристик.*

Используемые методы: *в работе использованы методы исследования случайных процессов, а также методы решения задач многокритериальной оптимизации.*

Результат исследования: *разработана модель функционирования сетевых устройств, между которыми установлено многоадресное сетевое соединение, которая формализована в виде полумарковского случайного процесса с дискретными состояниями и непрерывным временем. Получены вероятностно-временные характеристики исследуемых процессов, которые впоследствии выступают в качестве критериев эффективности при формулировании задачи векторной оптимизации.*

Решена задача определения оптимальных параметров сетевого соединения, таких как количество IP-адресов и время их использования, при которых критерии эффективности принимают оптимальные значения. Проведена оценка эффективности применения многоадресных сетевых соединений по критериям «доступность» и «защищенность».

Научная новизна: *заключается в разработке модели и решении задачи оптимизации параметров многоадресных сетевых соединений в условиях сетевой разведки с применением математического аппарата полумарковских случайных процессов и скаляризацией задачи векторной оптимизации методом идеальной точки.*

Ключевые слова: *структурно-функциональные характеристики, многоадресные сетевые соединения, непрерывность информационного обмена, случайный процесс, доступность и защищенность сетевых устройств.*

DOI:10.21681/2311-3456-2023-3-13-22

Введение

На фоне внешнеполитической деятельности нашей страны аналитиками в сфере информационной безопасности отмечается беспрецедентное увеличение количества компьютерных атак. Так, согласно отчету[4] компании «Лаборатория Касперского», большая часть атак приходится на сетевые инфраструктуры, а в качестве основных угроз фигурируют программы, пытающиеся подобрать пароли методом перебора, сканеры портов, эксплойты для различных уязвимостей.

Отмечается, что данные угрозы остаются актуальными даже при условии применения средств защиты информации, что обусловлено в первую очередь применением сетей связи общего пользования, использованием импортного оборудования, кризисом доверия к открытому программному обеспечению [1], а также статичностью структурно-функциональных характеристик сетевых устройств вычислительной сети, таких как *IP*-адрес, сетевые порты, *DNS*-имена и т.п.

Одной из перспективных концепций защиты вычислительных сетей, позволяющей скрывать её истинные структурно-функциональные характеристики (далее – СФХ), является концепция *Moving Target Defense* (*MTD*), суть которой заключается в замене статических параметров сети динамическими [2-6]. При этом основным средством, обеспечивающим многоадресность (и многопоточность) соединений абонентов, является протокол транспортного уровня *SCTP* (*Stream Control Transmission Protocol, RFC*

1 Москвин Артём Александрович, адъюнкт, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: tema.kg9012@gmail.com

2 Максимов Роман Викторович, доктор технических наук, профессор, Заслуженный изобретатель Российской Федерации, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: rvmaxim@yandex.ru

3 Горбачёв Александр Александрович, адъюнкт, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: infosec23.00@ mail.ru.

4 Статистика сетевых атак АО «Лаборатория Касперского», URL: http://statistics.securelist.ru/

Функциональные возможности	UDP	TCP	SCTP
Установка соединения	Нет	Да	Да
Надежная передача	Нет	Да	Да
Сохранение границ сообщения	Да	Нет	Да
Упорядоченная доставка	Нет	Да	Да
Неупорядоченная доставка	Да	Нет	Да
Контрольная сумма данных	Да	Да	Да
MTU пути	Нет	Да	Да
Многопточность	Нет	Нет	Да
Многоадресность	Нет	Нет	Да

Рис. 1. Функциональные возможности протоколов транспортного уровня

4960) [7]. Сравнительная характеристика функциональных возможностей различных протоколов транспортного уровня представлена на рис. 1. Многоадресность протокола *SCTP* позволяет осуществлять смену *IP*-адресов без разрыва установленного сетевого соединения, потенциально обеспечив тем самым необходимый уровень доступности сетевых устройств в целом. Технологии применения *SCTP* [8-10], однако, не предусматривают поиска оптимальных параметров и количественной оценки доступности абонентов.

В данной статье предложена модель функционирования сетевых устройств, между которыми установлено многоадресное сетевое соединение, позволяющая оценить эффективность его применения при смене СФХ вычислительной сети по критериям «доступность» и «защищенность». Сформулирована и решена задача определения оптимальных параметров сетевого соединения, за счет которых эта эффективность достигается. Решение такой задачи обеспечит возможность использования *SCTP*-ассоциаций между элементами клиент-серверной сети [11] решать задачи маскирования адресации при противодействии атакам типа «отказ в обслуживании» [12], моделирования и оптимизации систем в условиях конфликта [13-15].

Модель функционирования сетевых устройств, между которыми установлено многоадресное сетевое соединение, в условиях ведения сетевой разведки

С одной стороны, процесс функционирования сетевых устройств, между которыми установлено многоадресное сетевое соединение (далее – система L_1), может быть представлен как случайный процесс с дискретными состояниями и непрерывным временем, где в качестве дискретных состояний выступают этапы функционирования системы L_1, определенные в *RFC* 4960, а переход между ними осуществляется за счёт поступления в случайный момент времени *SCTP*-пакетов.

С другой стороны, процесс функционирования сетевых устройств в условиях ведения сетевой разведки (далее система L_2) может быть представлен как случайный процесс, состоящий из двух состояний: либо СФХ известны злоумышленнику, либо нет. Причем переход из одного состояния в другое зависит от количества предварительно заданных сетевым устройствам *IP*-адресов, а также времени их использования.

В статье рассматриваются полумарковские случайные процессы, протекающие в системах L_1 и L_2, обладающие свойствами простейшего потока событий.

Основными вероятностными характеристиками полумарковского процесса[4] являются: функция распределения времени ожидания перехода из состояния i в состояние j (далее – $F_{ij}(t)$), а также соответствующие им вероятности перехода (далее – p_{ij}). Данные вероятностные характеристики, вследствие соблюдения свойств простейшего потока, имеют экспоненциальный закон распределения [17, 18]:

$$F_{ij}(t) = 1 - e^{-\lambda_{ij} t} \quad (1)$$

$$p_{ij} = \int_0^{\infty} f_{ij}(t) \prod_{k=1, k \neq j}^{n} (1 - F_{ik}(t)) dt \quad (2)$$

где: λ_{ij} - интенсивность потока событий, переводящих исследуемые системы из состояния i в состояние j, $f_{ij}(t)$ – функция плотности распределения времени ожидания перехода из состояния i в состояние j.

На (рис. 2) представлен ориентированный граф случайного процесса для системы L_1, в (табл. 1) описаны его дискретные состояния, а в (табл. 2) приведены вероятностные характеристики.

4 Тихонов, В.И., Миронов М.А. Марковские процессы. – М.: Советское радио, 1977.

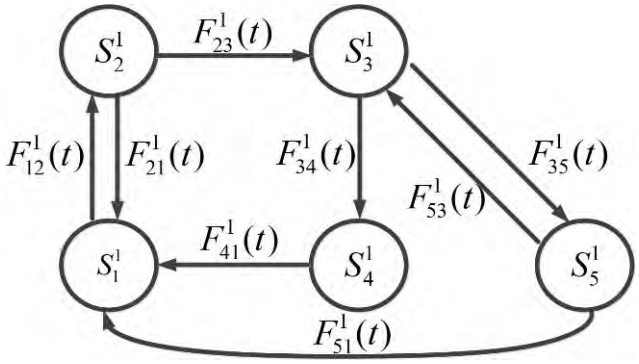

Рис. 2. Граф состояний системы L1

На (рис. 3) представлен ориентированный граф случайного процесса для системы L_2, в (табл. 3) описаны его дискретные состояния, а в (табл. 4) приведены вероятностные характеристики.

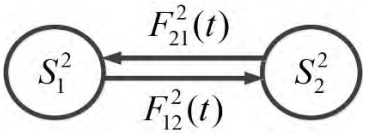

Рис. 3. Граф состояний системы L2

Таблица 1

Дискретные состояния системы L_1

Состояние	Описание состояний
S_1^1	ожидание инициализации сетевого соединения между сетевыми устройствами (ожидание получения служебного *SCTP*-пакета *INIT*)
S_2^1	ожидание приема и передачи потока данных между сетевыми устройствами (ожидание получения служебного *SCTP*-пакета *DATA*)
S_3^1	ожидание реконфигурации сетевого соединения, либо его завершения (ожидание получения служебного *SCTP*-пакета *HEARTBEAT/SHUTDOWN*)
S_4^1	ожидание перехода сетевых устройств в состояние простоя (ожидание получения служебного *SCTP*-пакета *SHUTDOWN COMPLETE*)
S_5^1	состояние ожидание возобновления информационного обмена между сетевыми устройствами (ожидание получения служебного *SCTP*-пакета *HEARTBEAT ACK*)

Таблица 2

Вероятностные характеристики процесса функционирования системы S^1

Переменная	Описание вероятностных характеристик
$F_{12}^1(t)$	функция распределения времени ожидания инициализации сетевого соединения
$F_{21}^1(t)$	функция распределения времени ожидания отказа в инициализации сетевого соединения
$F_{23}^1(t)$	функция распределения времени ожидания передачи и приема потоков данных между сетевыми устройствами
$F_{34}^1(t)$	функция распределения времени ожидания завершения сетевого соединения между сетевыми устройствами
$F_{41}^1(t)$	функция распределения времени ожидания закрытия сетевого соединения между сетевыми устройствами
$F_{35}^1(t)$	функция распределения времени ожидания реконфигурации сетевого соединения
$F_{53}^1(t)$	функция распределения времени ожидания возобновления информационного обмена между сетевыми устройствами
$F_{51}^1(t)$	функция распределения времени ожидания разрыва сетевого соединения между сетевыми устройствами

Таблица 3

Дискретные состояния системы L_2

Состояние	Описание состояния
S_1^2	ожидание вскрытия истинных СФХ сетевых устройств вычислительной сети
S_2^2	ожидание реконфигурации СФХ сетевых устройств вычислительной сети

Таблица 4

Вероятностные характеристики процесса функционирования системы L_2

Переменная	Описание вероятностных характеристик
$F_{12}^2(t)$	функция распределения времени ожидания вскрытия истинных СФХ сетевых устройств вычислительной сети
$F_{21}^2(t)$	функция распределения времени ожидания реконфигурации СФХ сетевых устройств вычислительной сети

Математическая модель исследуемых систем может быть представлена в виде отображения множества входных параметров (множество *Z*) во множество выходных вероятностно-временных характеристик (множество *V*):

$$Z^1 \to V^1,\ Z^1 = \{S^1, A^1, X^1\}; V^1 = \{P^1, G^1\}, \quad (3)$$

$$Z^2 \to V^2,\ Z^2 = \{S^2, A^2, X^2\}; V^2 = \{P^2, G^2\}. \quad (4)$$

где: S^1, S^2 – множества дискретных состояний исследуемых систем L_1, L_2; A^1, A^2 – множества неуправляемых (неконтролируемых) факторов исследуемых систем L_1, L_2; X^1, X^2 – множества управляемых факторов исследуемых систем L_1, L_2; $P^1=\{P_{ij}^{\ 1}(t)\}$, $P^2=\{P_{ij}^{\ 2}(t)\}$ – множества интервально-переходных вероятностей пребывания систем L_1, L_2 в состоянии *j* из состояния *i* в момент времени *t*; $G^1=\{G_{ij}^{\ 1}(t)\}$, $G^2=\{G_{ij}^{\ 2}(t)\}$ – множества вероятностей первого достижения состояния *j* из состояния *i* к моменту времени *t* для систем L_1, L_2.

В качестве неуправляемых и управляемых факторов для исследуемых систем выступают:

$$A^1 = \{F_{12}^1(t), F_{21}^1(t), F_{23}^1(t), F_{34}^1(t), F_{41}^1(t), F_{41}^1(t), F_{51}^1(t), T_{vost}, T_{scan}\}, \quad (5)$$

$$A^2 = \{T_{scan}\}, \quad (6)$$

$$X^1 = \{F_{35}^1(t), F_{53}^1(t), h\},\ при\ \lambda_{35} = y^{-1}u\ \ \lambda_{53} = (h \cdot T_{vost} \cdot x)^{-1}, \quad (7)$$

$$X^2 = \{F_{12}^2(t), F_{21}^2(t), h\},\ при\ \lambda_{21} = y^{-1}u\ \ \lambda_{12} = (h \cdot T_{scan} \cdot x)^{-1}. \quad (8)$$

где: *h* – количество сетевых устройств, *x* – количество *IP*-адресов для одного сетевого устройства, *y* – время использования этих адресов, T_{scan} – время, затрачиваемое злоумышленником на сканирование одного сетевого устройства, T_{vost} – время, затрачиваемое на реконфигурации одного *IP*-адреса.

Нахождение интервально-переходных вероятностей $P_{ij}(t)$ осуществляется посредством решения системы интегральных уравнений вида (9), где δ_{ij} – символ Кронекера:

$$P_{ij}(t) = \delta_{ij}\Psi_i(t) + \sum_{k=1}^{n} p_{ik} \int_0^t f_{ik}(t) P_{kj}(t-\tau) d\tau \quad (9)$$

$$\Psi_i(t) = 1 - \sum_{j=1}^{n} p_{ij} F_{ij}(t) \quad (10)$$

Последовательность решения интегральных уравнений данного типа подробно описана[5] в [16], и в матричной форме будет иметь вид:

$$\mathbf{P}(t) = \pounds^{-1}\{\left[\mathbf{I} - \mathbf{p} \times \mathbf{f}(s)\right]^{-1} \mathbf{\Psi}(s)\} \quad (11)$$

Функции распределения $G_{ij}(t)$ находятся из следующего выражения:

$$\mathbf{G}(t) = \pounds^{-1}\{s^{-1} \cdot \mathbf{p} \cdot \mathbf{f}(s) \cdot \left(\mathbf{I} - \mathbf{p} \cdot \mathbf{f}(s)\right)^{-1} \cdot \left[\mathbf{I} \times \left(\mathbf{I} - \mathbf{p} \cdot \mathbf{f}(s)\right)^{-1}\right]^{-1}\} \quad (12)$$

Параметрическая оптимизация многоадресного сетевого соединения

Поскольку состояние S_5^1 системы L_1 возможно охарактеризовать как состояние, при котором сетевые устройства недоступны для информационного обмена, то финальная вероятность нахождения системы

5 Warr R.L., Collins D.H. An Introduction to Solving for Quantities of Interest in Finite-State Semi-Markov Processes. 2012. pp. 1-18. // arXiv, 2012. URL: https://arxiv.org/abs/1212.1440/ (дата обращения 20.05.2022).

в подмножестве состояний за исключением данного состояния может рассматриваться как целевая функция, характеризующая критерий «доступности»:

$$F_1(X^1, A^1) = \overline{P_5^1} \quad (13)$$

Для системы L_2 необходимо, чтобы она находилась в состоянии S_1^2, при котором сетевые устройства находятся в защищенном состоянии. Таким образом, критерием «защищенности» системы L_2 будет являться целевая функция:

$$F_2(X^2, A^2) = P_1^2 \quad (14)$$

Стоит отметить, что целевые функции (13) и (14) содержат общие переменные, которые являются параметрами конфигурирования сетевого соединения: это количество *IP*-адресов и время их использования, причем наилучшие параметры для системы L_2 являются наихудшими для системы L_1.

Так, при увеличении числа *IP*-адресов, а также уменьшения времени их использования, сетевые устройства будут находиться в защищенном состоянии, однако частая реконфигурация этих параметров приведёт к тому, что сетевые устройства большую часть времени будут находиться в состоянии ожидания окончания этой реконфигурации, т.е. будут недоступными для осуществления информационного обмена.

Таким образом, возникает задача поиска оптимальных наборов конфигурируемых параметров многоадресного сетевого соединения, при которых сетевые устройства будут функционировать наиболее эффективно по критериям «доступности» и «защищенности». Данную задачу можно сформулировать как задачу многокритериальной (векторной) оптимизации и записать в следующем виде:

$$\begin{cases} F_1(X^1, A^1) \to \max\limits_{X^1, A^1 \in Q}, \\ F_2(X^2, A^2) \to \max\limits_{X^2, A^2 \in Q} \end{cases} \quad (15)$$

где: Q – допустимое множество:

$$Q: \begin{cases} 0 < h < 256, \\ 0.1 < T_{scan} < 38, 0.1 < T_{vost} < 3, \\ 1 < x < 4095, 0.01 < y < 86400, \\ \lambda_{12}^1 \geq 0, \lambda_{21}^1 \geq 0, \lambda_{23}^1 \geq 0, \lambda_{23}^1 \geq 0, \\ \lambda_{41}^1 \geq 0, \lambda_{35}^1 \geq 0, \lambda_{53}^1 \geq 0, \lambda_{51}^1 \geq 0, \\ \lambda_{12}^2 \geq 0, \lambda_{21}^2 \geq 0, \\ 0 < F_1(X^1, A^1) < 1, \\ 0 < F_2(X^2, A^2) < 1 \end{cases} \quad (16)$$

Количество сетевых устройств (параметр h) выбирается в зависимости от класса сети. Так, в сети класса *C* может содержаться 256 сетевых устройств, в сетях класса *B* может содержаться 65536 сетевых устройств и т.п. Среднее время ведения сетевой разведки (параметр T_{scan}) зависит от режима сканирования сети и имеет максимальное значение 38 секунд на 1 сетевое устройство (режим «*Intense scan, all tcp ports*» программы «*Nmap*»), а среднее время реконфигурации одного сетевого устройства (параметр T_{vost}) с применением *DHCP*-сервера составило 0,5-3,0 сек. Данные параметры были получены экспериментальным путем. Максимальное количество *IP*-адресов (параметр x), которое может использовать одно сетевое устройство в рамках многоадресного сетевого соединения, равно 4095, поскольку в одном физическом соединении путем мультиплексирования может быть организовано 4095 логических каналов, что определено стандартом 802.1Q. Максимальное время использования *IP*-адресов (параметр y), в соответствии с *RFC* 2131, может составлять до 100 лет, однако на данный параметр было введено ограничение в 1 сутки (86400 сек).

В двумерном критериальном пространстве[6] множество значений целевых функций представляет собой фронт Парето (рис. 4).

Оценка эффективности применения многоадресного сетевого соединения для сетевых устройств, функционирующих в условиях ведения сетевой разведки

Идеальная точка, имеющая в критериальном пространстве координаты (1, 1), представляет собой состояние, при которой критерии «доступности» и «защищенности» имеют максимальное значение, соответственно и эффективность в этой точке максимальная. Таким образом, показатель эффективности применения многоадресного сетевого соединения для сетевых устройств, функционирующих в условии сетевой разведки ($\sqrt{2}$ учитывает максимальное расстояние до наиболее неблагоприятной точки критериального пространства в начале координат), рассчитан следующим образом:

$$W = 1 - R(X^1, A^1, X^2, A^2) / \sqrt{2} \quad (18)$$

Используя функции $G_{ij}(t)$, возможно оценить время, по истечении которого с вероятностью $G(t)$ произойдет прерывание информационного обмена.

6 Ногин В.Д. Протодьяконов И.О., Евлампиев И.И. Основы теории оптимизации: Учеб. пособие для студентов втузов/под ред. И.О. Протодьяконова. – М.: Высш. шк., 1986.

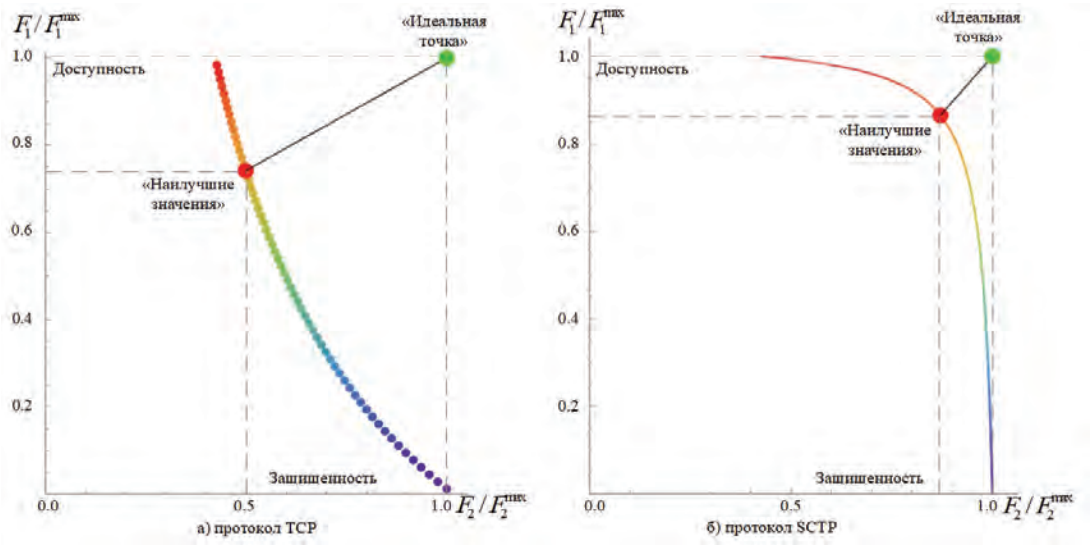

Рис. 4. Визуализация критериального пространства и фронта Парето

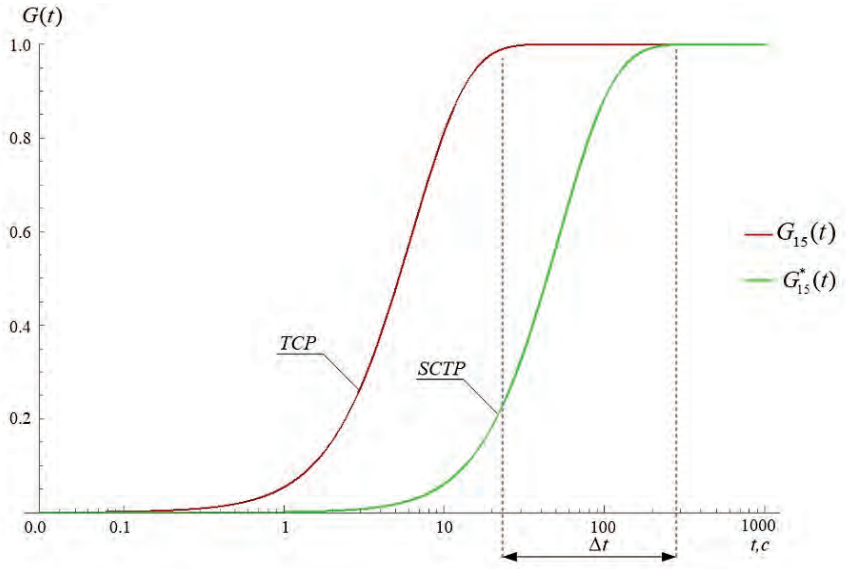

Рис. 5. Оценка времени доступности при использовании протоколов TCP/SCTP

На рис. 5 приведен результат оценки продолжительности непрерывного информационного обмена при смене *IP*-адресов вычислительной сети, состоящей из 100 сетевых устройств, между которыми установлены сетевые соединения с применением различных протоколов транспортного уровня.

Так, например, при режиме сетевого сканирования «*Ping scan*» (рис. 5) в случае применения протокола *TCP* (функция $G_{15}(t)$), сетевое устройство при смене *IP*-адресов станет недоступным через 22 сек после начала процесса, однако, при применении протокола *SCTP* с оптимальными параметрами (функция $G^*_{15}(t)$), время непрерывного информационного обмена увеличится на Δt = 282 сек.

Оценка эффективности функционирования сетевых устройств, между которыми установлено сетевое соединение с множественной адресацией, в случае применения оптимальных параметров при различных режимах сканирования, приведена в табл. 5.

Выводы

Предложенная модель позволяет исследовать процесс функционирования сетевых устройств при конфигурировании параметров сетевых соединений, имеющих множественную адресацию, в условиях ведения злоумышленником сетевой разведки. Модель формализована в виде полумарковского случайного процесса с дискретными состояниями и непрерыв-

DOI:10.21681/2311-3456-2023-3-13-22

Таблица 5

Оценка эффективности применения многоадресных сетевых соединений

№ п/п	Режим сканирования/ время сканирования одного СУ, с	Протокол	Оптимальные количество IP-адресов / время их использования, шт/с	«Доступность»		«Защищенность»		Значение показателя эффективности (W)	Прирост эффективности, %	Прирост времени непрерывного информационного обмена (Δt), с
1				Значение целевой функции (F^1/F^1_{max})	Прирост «Доступности», %	Значение целевой функции (F^2/F^2_{max})	Прирост «Защищенности», %			
2	*Quick scan* / 0,15	TCP	1 / 20	0,68	23	0,42	97	0,54	55	260
		SCTP	10 / 28	0,84		0,83		0,84		
3	*Ping scan* / 0,22	TCP	1 / 23	0,74	17	0,49	75	0,61	43	193
		SCTP	8 / 27	0,87		0,86		0,87		
4	*Intense scan* / 0,42	TCP	1 / 25	0,84	7	0,62	45	0,71	26	131
		SCTP	6 / 26	0, 90		0, 90		0,91		
5	*Intense scan, all tcp ports* / 37,8	*TCP*	1 / 39	0, 99	0,1	0, 99	0,1	0,99	0,1	1
		SCTP	1 / 31	0, 99		0, 99		0,99		

ным временем, при этом выходные характеристики (интервально-переходные вероятности, функции распределения первого достижения соответствующего состояния) определяются через основные характеристики полумарковского процесса с экспоненциальным законом распределения.

Полученные вероятностно-временные характеристики применимы в качестве целевых функций, характеризующих критерии «защищенности» и «доступности» сетевых устройств, функционирующих в условиях сетевой разведки.

Оптимальное количество *IP*-адресов, используемых в многоадресном сетевом соединении, зависит от предполагаемого режима сканирования злоумышленника и находится в пределах от 1 (для низкоинтенсивного сканирования) до 10 (для высокоинтенсивного сканирования). Оптимальное время использования *IP*-адресов составляет величину от 20 до 39 секунд.

Оценка эффективности применения многоадресных сетевых соединений для 100 сетевых устройств локальной вычислительной сети показала, что при ведении интенсивной сетевой разведки (0,15-0,22 сек на одно сетевое устройство) применение многоадресных сетевых соединений на 43-55 % эффективнее относительно одноадресных, при этом доступность сетевых устройств для осуществления информационного обмена увеличилась на 17-23 % в соответствии с приведенной метрикой.

Литература

1. Марков А.С. Важная веха в безопасности открытого программного обеспечения // Вопросы кибербезопасности. 2023. № 1 (53). С. 2-12. DOI:10.21681/2311-3456-2023-1-2-12.
2. Ворончихин И.С., Иванов И.И., Максимов Р.В., Соколовский С.П. Маскирование структуры распределенных информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6 (34). С. 92-101. DOI:10.21681/2311-3456-2019-6-92-101.
3. Maximov R.V., Sokolovsky S.P., Telenga A.P. Methodology for substantiating the characteristics of false network traffic to simulate information systems // Selected Papers of the XI Anniversary International Scientific and Technical Conference on Secure Information Technologies (BIT 2021). Bauman Moscow Technical University. Aprill 6-7, 2021, Moscow, Russia. P. 115-124.
4. Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., Kambhampati, S.A Survey of Moving Target Defenses for Network Security // IEEE Commun. Surv. Tutor. 2020, 22, 1909-1941.
5. Kanellopoulos, A., Vamvoudakis, K.G. A Moving Target Defense Control Framework for Cyber-Physical Systems // IEEE Trans. Autom. Control 2020, 65, pp. 1029-1043.
6. Maximov R.V., Sokolovsky S.P., Telenga A.P. Honeypots network traffic parameters modeling // Selected Papers of the XI Anniversary International Scientific and Technical Conference on Secure Information Technologies (BIT 2021). Bauman Moscow Technical University. Aprill 6-7, 2021, Moscow, Russia. P. 229-239.
7. Лейкин А.В., Развитие SCTP как конвергентного транспортного протокола следующего поколения // Вестник связи. 2020. № 1. С. 13-17.
8. Патент № 2716220 Российской Федерации. Способ защиты вычислительных сетей / Р.В. Максимов, С.П. Соколовский, И.С. Ворончихин // заявитель и патентообладатель Краснодарское высшее военное училище имени генерала армии С.М. Штеменко. № 2019123718, заявл. 22.07.2019, опубл. 06.03.2020.
9. Патент № 2726900 Российской Федерации. Способ защиты вычислительных сетей / Р.В. Максимов, С.П Соколовский, И.С. Ворончихин, [и др.] // заявитель и патентообладатель Краснодарское высшее военное училище имени генерала армии С.М. Штеменко. № 2019140769, заявл. 09.12.2019, опубл. 16.07.2020.
10. Патент № US20120117376A1 США. Method and apparatus for anonymous IP datagram exchange using dynamic network address translation / R.A.Fink, E.A.Bubnis, T.E.Keller // заявитель и патентообладатель Raytheon BBN Technologies corp. – № US12/814624, опубл. 10.05.2012.
11. Максимов Р.В., Соколовский С.П., Ворончихин И.С. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей // Информатика и автоматизация. 2020. Т. 19. № 5. С. 1018-1049.
12. Максимов Р.В., Кучуров В.В., Шерстобитов Р.С. Модель и методика маскирования адресации корреспондентов в киберпространстве // Вопросы кибербезопасности. 2020. № 6 (40). С. 2-13. DOI:10.21681/2311-3456-2020-06-2-13.
13. Евневич Е.Л., Фаткиева Р.Р. Моделирование информационных процессов в условиях конфликтов // Вопросы кибербезопасности. 2020. № 2 (36). С. 42-49. DOI:10.21681/2311-3456-2020-2-42-49.
14. Кубарев А.В., Лапсарь А.П., Федорова Я.В. Повышение безопасности эксплуатации значимых объектов критической инфраструктуры с использованием параметрических моделей эволюции // Вопросы кибербезопасности. 2020. № 1 (35). С. 8-17. DOI:10.21681/2311-3456-2020-01-08-17.
15. Дроботун Е.Б. Методика снижения удобства использования автоматизированной системы при введении в ее состав системы защиты от компьютерных атак // Вопросы кибербезопасности. 2020. № 2 (36). С. 50-57. DOI:10.21681/2311-3456-2020-02-50-57.
16. Горбачев А.А. Модель и параметрическая оптимизация проактивной защиты сервиса электронной почты от сетевой разведки // Вопросы кибербезопасности. 2022. № 3 (49). С. 69-81. DOI:10.21681/4311-3456-2022-3-69-81.
17. Будников С.А., Бутрик Е.Е., Соловьев С.В. Моделирование APT-атак, эксплуатирующих уязвимость Zerologon // Вопросы кибербезопасности. 2021. № 6 (46). С. 47-61. DOI:10.21681/2311-3456-2021-6-47-61.
18. Иванов И.И. Модель функционирования распределенных информационных систем при использовании маскированных каналов связи // Системы управления, связи и безопасности, 2020. № 1. С. 198-234.

MODEL, OPTIMIZATION AND EFFICIENCY EVALUATION OF APPLICATION MULTICAST NETWORK CONNECTIONS IN CONDITIONS OF NETWORK INTELLIGENCE

Moskvin A.A.[7], Maksimov R.V.[8], Gorbachev A.A.[9]

The purpose of the study: *increasing the availability of network devices in a computer network in the conditions of changing them structural and functional characteristics.*

Methods used: *methods for random processes research and multicriteria optimization were used in this work.*

The result of the study: *a model of functioning of network devices with multicast network connection has been developed, which is formalized as a semi-Markov random process with discrete states and continuous time. The probabilistic-temporal characteristics of the processes are obtained, which subsequently act as efficiency criteria in formulating of the vector optimization problem.*

The problem of determining the optimal parameters of a network connection, such as the number of IP addresses and the time of their use, at which the efficiency criteria take optimal values, is solved.

The evaluation of the effectiveness of the use of multicast network connections according to the criteria of "availability" and "security" was carried out.

Scientific novelty: *consists in developing a model and solving the problem of optimization the parameters of multicast network connections under network intelligence using the mathematical apparatus of semi-Markov random processes and scalarization of the vector optimization problem by the ideal point method.*

Keywords: *structural and functional characteristics, multicast network connections, continuity of information exchange, random process, availability and security of network devices.*

References

1. Markov A.S. Vazhnaja veha v bezopasnosti otkrytogo programmnogo obespechenija // Voprosy kiberbezopasnosti. 2023. № 1 (53). S. 2-12. DOI:10.21681/2311-3456-2023-1-2-12.
2. Voronchihin I.S., Ivanov I.I., Maksimov R.V., Sokolovskij S.P. Maskirovanie struktury raspredelennyh informacionnyh sistem v kiberprostranstve // Voprosy kiberbezopasnosti. 2019. № 6 (34). S. 92-101. DOI:10.21681/2311-3456-2019-6-92-101.
3. 3. Maximov R.V., Sokolovsky S.P., Telenga A.P. Methodology for substantiating the characteristics of false network traffic to simulate information systems // Selected Papers of the XI Anniversary International Scientific and Technical Conference on Secure Information Technologies (BIT 2021). Bauman Moscow Technical University. Aprill 6-7, 2021, Moscow, Russia. P. 115-124.
4. Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., Kambhampati, S.A Survey of Moving Target Defenses for Network Security // IEEE Commun. Surv. Tutor. 2020, 22, 1909-1941.
5. Kanellopoulos, A., Vamvoudakis, K.G. A Moving Target Defense Control Framework for Cyber-Physical Systems // IEEE Trans. Autom. Control 2020, 65, pp. 1029-1043.
6. Maximov R.V., Sokolovsky S.P., Telenga A.P. Honeypots network traffic parameters modeling // Selected Papers of the XI Anniversary International Scientific and Technical Conference on Secure Information Technologies (BIT 2021). Bauman Moscow Technical University. Aprill 6-7, 2021, Moscow, Russia. P. 229-239.
7. Lejkin A.V., Razvitie SCTP kak konvergentnogo transportnogo protokola sledujushhego pokolenija // Vestnik svjazi. 2020. № 1. S. 13-17. Patent № 2716220 Rossijskoj Federacii. Sposob zashhity vychislitel'nyh setej / R.V. Maksimov,
8. S.P. Sokolovskij, I.S. Voronchihin // zajavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishhe imeni generala armii S.M. Shtemenko. № 2019123718, zajavl. 22.07.2019, opubl. 06.03.2020.
9. Patent № 2726900 Rossijskoj Federacii. Sposob zashhity vychislitel'nyh setej / R.V. Maksimov, S.P Sokolovskij, I.S. Voronchihin, [i dr.] // zajavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishhe imeni generala armii S.M. Shtemenko. № 2019140769, zajavl. 09.12.2019, opubl. 16.07.2020.
10. Patent № US20120117376A1 SShA. Method and apparatus for anonymous IP datagram exchange using dynamic network address translation / R.A.Fink, E.A.Bubnis, T.E.Keller // zajavitel' i patentoobladatel' Raytheon BBN Technologies corp. – № US12/814624, opubl. 10.05.2012.

7 Artyom A. Moskvin, post graduate student, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: tema.kg9012@gmail.com

8 Roman V. Maksimov, Dr.Sc., Professor, Honored Inventor of the Russian Federation,, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: rvmaxim@yandex.ru

9 Alexander A. Gorbachev, post graduate student, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: infosec23.00@mail.ru

11. Maksimov R.V., Sokolovskij S.P., Voronchihin I.S. Algoritm i tehnicheskie reshenija dinamicheskogo konfigurirovanija klient-servernyh vychislitel'nyh setej // Informatika i avtomatizacija. 2020. T. 19. № 5. S. 1018-1049.
12. Maksimov R.V., Kuchurov V.V., Sherstobitov R.S. Model' i metodika maskirovanija adresacii korrespondentov v kiberprostranstve // Voprosy kiberbezopasnosti. 2020. № 6 (40). S. 2-13. DOI:10.21681/2311-3456-2020-06-2-13.
13. Evnevich E.L., Fatkieva R.R. Modelirovanie informacionnyh processov v uslovijah konfliktov // Voprosy kiberbezopasnosti. 2020. № 2 (36). S. 42-49. DOI:10.21681/2311-3456-2020-2-42-49.
14. Kubarev A.V., Lapsar' A.P., Fedorova Ja.V. Povyshenie bezopasnosti jekspluatacii znachimyh ob#ektov kriticheskoj infrastruktury s ispol'zovaniem parametricheskih modelej jevoljucii // Voprosy kiberbezopasnosti. 2020. № 1 (35). S. 8-17. DOI:10.21681/2311-3456-2020-01-08-17.
15. Drobotun E.B. Metodika snizhenija udobstva ispol'zovanija avtomatizirovannoj sistemy pri vvedenii v ee sostav sistemy zashhity ot komp'juternyh atak // Voprosy kiberbezopasnosti. 2020. № 2 (36). S. 50-57. DOI:10.21681/2311-3456-2020-02-50-57.
16. Gorbachev A.A. Model' i parametricheskaja optimizacija proaktivnoj zashhity servisa jelektronnoj pochty ot setevoj razvedki // Voprosy kiberbezopasnosti. 2022. № 3 (49). S. 69-81. DOI:10.21681/4311-3456-2022-3-69-81.
17. Budnikov S.A., Butrik E.E., Solov'ev S.V. Modelirovanie APT-atak, jekspluatirujushhih ujazvimost' Zerologon // Voprosy kiberbezopasnosti. 2021. № 6 (46). S. 47-61. DOI:10.21681/2311-3456-2021-6-47-61.
18. Ivanov I.I. Model' funkcionirovanija raspredelennyh informacionnyh sistem pri ispol'zovanii maskirovannyh kanalov svjazi // Sistemy upravlenija, svjazi i bezopasnosti, 2020. № 1. S. 198-234.