Кібернетична безпека

УДК 004.49.5

В.Л. Бурячок[1], С.А. Смирнов[2]

[1] *Государственный университет телекоммуникаций, Киев*
[2] *Кировоградский национальный технический университет, Кропивницкий*

МЕТОД БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ НА БАЗОВОМ МНОЖЕСТВЕ ПУТЕЙ ПЕРЕДАЧИ МЕТАДАННЫХ В ОБЛАЧНЫЕ АНТИВИРУСНЫЕ СИСТЕМЫ

Данная статья посвящена разработке метода безопасной маршрутизации на базовом множестве путей передачи метаданных в облачные антивирусные системы. Отличительной особенностью метода является реализация алгоритма формирования множества маршрутов передачи метаданных при введении показателей оптимизации и ограничений безопасной маршрутизации.

Ключевые слова: *информационно-телекоммуникационные сети, облачные антивирусы .*

Постановка проблемы исследования

Авторами предложен метод безопасной маршрутизации метаданных в облачные антивирусные системы. Основными составляющими метода являются: алгоритмы формирования множества маршрутов передачи метаданных; способ контроля линий связи ТКС; модели системы нейросетевых экспертов безопасной маршрутизации.

Данная статья посвящена разработке метода безопасной маршрутизации на базовом множестве путей передачи метаданных в облачные антивирусные системы на основе алгоритмов формирования множества маршрутов передачи метаданных.

Отличительной особенностью алгоритмов формирования множества маршрутов передачи метаданных является показатели оптимизации и вводимые ограничения безопасной маршрутизации.

Анализ процесса функционирования телекоммуникационной системы, а также исследования процессов формирования, передачи и обработки метаданных в облачных антивирусных системах [1-17], позволили определить плотность распределения вероятностей времени передачи хеш-файла метаданных в облачные антивирусные системы, а также обработки и доставки команд передачи управления, сформировать и математически формализовать знания об изменениях и характере поведения основных вероятностно-временных показателей качества обслуживания в телекоммуникационной системе.

Как было указанно в [11-17], обмен метаданными между программным клиентом и сервером, в общем случае, осуществляется через транзитные маршрутизаторы, последовательность которых на пути от отправителя к получателю в рамках работы определим как маршрут [11-17].

Пусть $\Re = \{V_n | n \in 1, N\}$ – множество маршрутизаторов в ТКС, V_n – n-й маршрутизатор, $N = |\Re|$ – число маршрутизаторов, $\Im = \{\theta_\xi | \xi \in 1, \Theta\}$ – множество каналов связи в ТКС, где θ_ξ – ξ -й канал связи, Θ – количество каналов связи в ТКС, $|Z|$ – мощность множества Z.

Информационные пакеты метаданных для анализа программному серверу могут быть переданы по одному из маршрутов, составляющих множество $\aleph = \{\eta_s | s \in 1, M\}$, где $\eta_s = \{\theta_{s,c} | \theta_{s,c} \in \Im; \ c \in 1, \Theta\}$ – s-й маршрут, $s \in 1, M$, $|\eta_s| = \Psi_s$, M – количество маршрутов, $\theta_{s,c}$ – канал связи с номером c, который принадлежит s-му маршруту, Ψ_s – количество каналов связи на s-м маршруте.

Формирование множества $\aleph$ маршрутов представляет собой сложный итерационный процесс, состоящий в выполнении нескольких алгоритмов:

– алгоритм поиска кратчайших путей между узлами в ТКС;

– алгоритм формирования базового множества маршрутов передачи метаданных;

– алгоритм безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер.

Выбор алгоритма поиска кратчайших путей между узлами в ТКС

Проведенные исследования показали, что решение задачи поиска кратчайших путей лежит в плоскости решения общей задачи маршрутизации метаданных в облачные антивирусные системы. Поэтому одним из необходимых условий является использование выбора базового алгоритма поиска

кратчайших путей является минимизация вычислительной сложности, которая во многом задается числом операций сравнения.

Проведенные исследования и анализ известных алгоритмов поиска кратчайших путей [1, 4, 11-17] показали, что одним из наиболее оперативных алгоритмов, отвечающих заданным требованиям ($O(n^{2^n})$) является алгоритм D'Esopo-Pape. Эффективность этого алгоритма подтверждается с одной стороны результатами исследований ряда авторов [1, 4, 11-17], а с другой стороны результатами экспериментов, проведенных с помощью имитационной модели.

Внешний вид интерфейса основной программной компоненты (основного поля) имитационной модели представлен на рис. 1.

В ходе моделирования выполнялись имитационные процедуры функционирования ТКС с различной топологией и количеством узлов $\overline{N}$ от 100 до 2000. Вес отдельных линий связи соответствовал возможной остаточной пропускной способности реальных каналов связи.

На рис. 2 представлены результаты исследования известных алгоритмов поиска кратчайших путей в виде графиков зависимости числа операций сравнения от числа вершин графа.

Из графиков рис. 2 видно, что алгоритм D'Esopo-Pape имеет преимущества по сравнению с известными алгоритмами Дейкстры и Беллмана-Форда.

Для подтверждения достоверности полученных результатов были проведены расчеты, соответствующие условиям моделирования:

– степень связности сети выбиралась случайным образом в рамках диапазона: от 5 до 10;

– число экспериментов на каждом из этапов, который характеризуется количеством узлов ТКС $\overline{\overline{N}} = 100$.

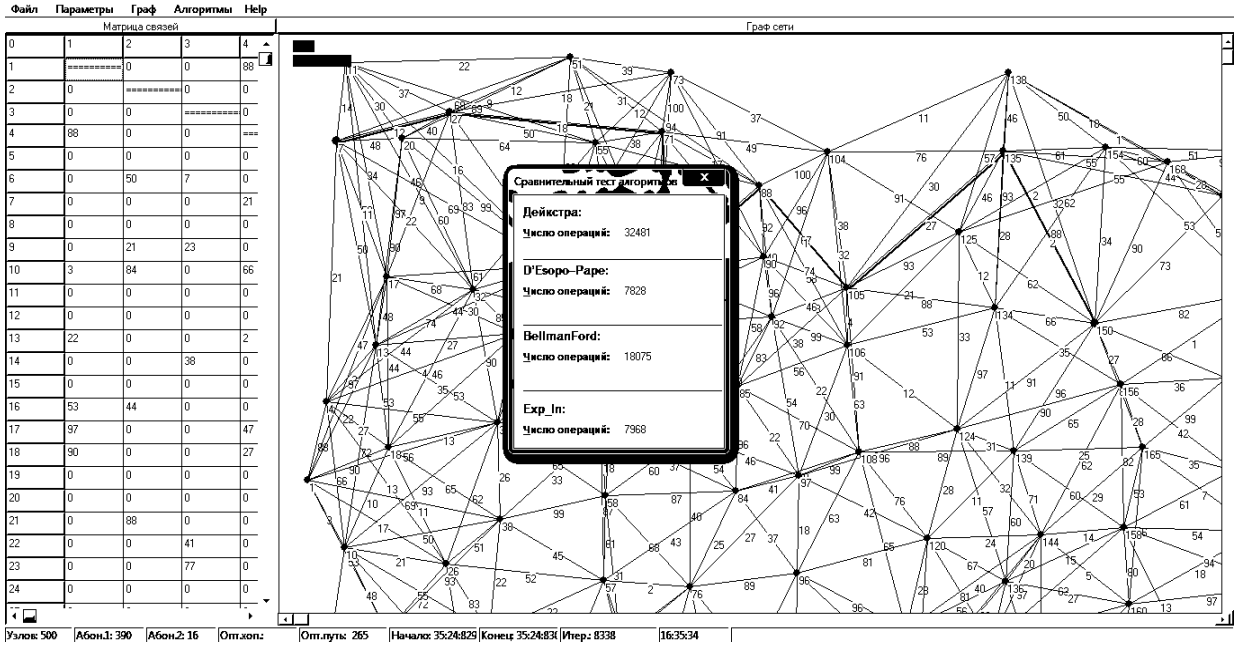

Рис. 1. Внешний вид интерфейса основной программной компоненты имитационной модели ТКС

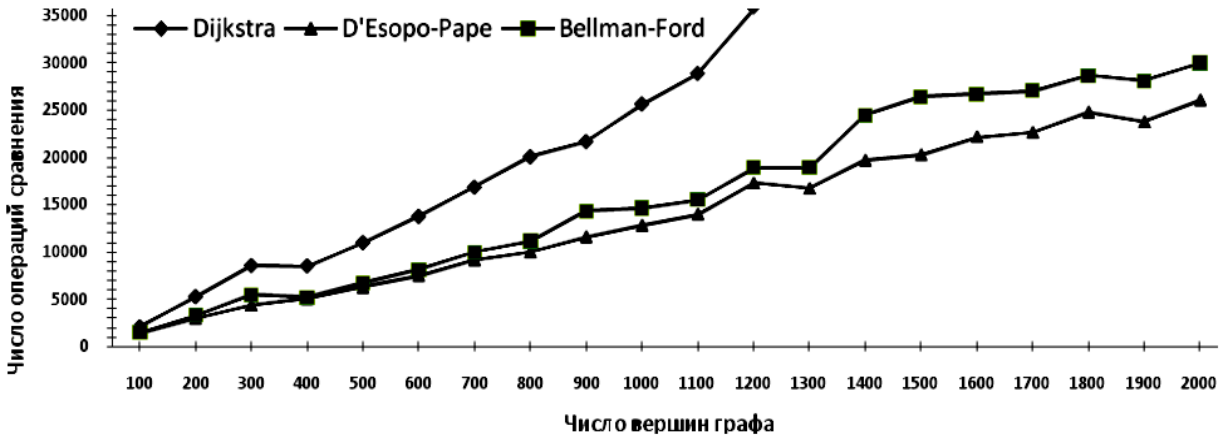

Рис. 2. Графики зависимости числа операций сравнения от числа вершин графа для различных алгоритмов поиска кратчайших путей

Выдвинутая в работе гипотеза о нормальном распределении случайной величины числа операций сравнения в алгоритмах была проверена по критерию согласия χ^2 Пирсона [3]:

$$\chi^2 = N^* \sum_{i=1}^{k} (P_i^* - P_i)^2 / P_i ,$$

где k – число разрядов (интервалов) статистического ряда, P_i^* и P_i – «статистическая» и теоретическая вероятности «попадания» величины среднего числа операций сравнения в i-й разряд.

Проведенная проверка доказала правдоподобность гипотезы о том, что величина числа операций сравнения распределена по нормальному закону.

Получены оценки $w(\vec{\xi})^{(i)}$ математического ожидания и $\hat{D}_{w(\vec{\xi})^{(i)}}$ дисперсии ($\hat{\sigma}_{w(\vec{\xi})^{(i)}}$ среднеквадратического отклонения) случайной величины числа операций сравнения $w(\vec{\xi})^{(i)}$ [3]:

$$\hat{w}(\vec{\xi})^{(i)} = \sum_{i=1}^{k} \hat{w}(\vec{\xi})^{(i)} \Big/ N^* ;$$

$$D_{w(\vec{\xi})^{(i)}} = \sum_{i=1}^{k} \left(w(\vec{\xi})^{(i)} - \hat{w}(\vec{\xi})^{(i)} \right)^2 \Big/ \left(N^* - 1 \right);$$

$$\hat{\sigma}_{w(\vec{\xi})^{(i)}} = \sqrt{\hat{D}_{w(\vec{\xi})^{(i)}}} .$$

Воспользовавшись известным выражением для расчета доверительной вероятности отклонения относительной частоты от постоянной вероятности в независимых испытаниях, полученное в результате эксперимента значение прогнозируемого числа операций сравнения «не отклониться» от математического ожидания $\hat{w}(\vec{\xi})^{(i)}$ более чем на 1:

$$P\left(\left| \hat{w}(\vec{\xi})^{(i)} - w(\vec{\xi})^{(i)} \right| < 1 \right) = 2\Phi\left(1 \Big/ \hat{w}(\vec{\xi})^{(i)} \right),$$

где Ф – функция Лапласа вида:

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-t^2/2} dt \quad [3].$$

Поведенное имитационное моделирование показало, что для всех исследуемых видов данных доверительная вероятность того, что значение статистической величины $w(\vec{\xi})$ «не отклониться» от математического ожидания $w(\vec{\xi})$ более чем на 1 равно: $P \approx 0{,}98$. Высокая степень совпадения результатов имитационного моделирования подтверждают достоверность результатов анализа алгоритмов поиска кратчайших путей.

Таким образом, можно отметить целесообразность использования алгоритма D'Esopo-Pape в качестве базового при поиске кратчайших путей между узлами в ТКС.

Алгоритм формирования базового множества маршрутов передачи метаданных

Для нахождения множества маршрутов, исключающих «петли» в рассматриваемом алгоритме используются процедуры, представленные на рис. 3.

Пусть программный клиент облачной антивирусной системы инсталлирован на некотором узле i, относительно которого существуют множества:

$U = \{ u_\alpha \mid \aleph(u_\alpha) \subset \aleph \}$ – уровней иерархии на дереве допустимых маршрутов;

$\aleph_{баз} = \bigcup_{u_\alpha = 1}^{|U|} \aleph(u_\alpha)$ – искомых путей передачи метаданных;

$\aleph_{вб} \subset \aleph_{баз}$ – множество маршрутов передачи метаданных, выбранных из множества $\aleph_{баз}$ для повышения безопасности, где u_α – номер уровня иерархии.

Выдвинутые предположения, а также основные процедуры рассматриваемого алгоритма формирования базового множества маршрутов передачи метаданных позволяют сформулировать оптимизационную задачу повышения оперативности передачи метаданных в пределах множества маршрутов $\aleph_{вб}$:

$$T_{тс}(\aleph_{вб}) \to \min ; \qquad (1)$$

$$|U| = \{ u_\alpha \mid \aleph(u_\alpha) \subset \aleph \} ; \qquad (2)$$

$$\aleph_{баз} = \bigcup_{u_\alpha = 1}^{|U|} \aleph(u_\alpha) , \; |U| \geq 1 , \; |U| < \max_{\eta_m \in \aleph} |\eta_m| ; \qquad (3)$$

$$\aleph_{вб} = \bigcup_{u_\alpha = 1}^{|U|} \aleph_{баз}(u_\alpha) ; \qquad (4)$$

$$P_{без} \geq P_{без_{доп}} . \qquad (5)$$

где $P_{без_{доп}}$ – допустимая вероятность безопасной передачи данных.

В том случае, если не найдено ни одного распределения из множества $\aleph_{вб}$, удовлетворяющего ограничению (5), необходимо расширить $\aleph_{вб}$ путем его объединения с множеством маршрутов следующего уровня иерархии в соответствии с (1) – (4).

Следует заметить, что при решении поставленной задачи формирования базового $\aleph_{баз}$ множества маршрутов передачи метаданных известными алгоритмами поиска кратчайших путей [1, 4, 11-17] в большинстве практических случаев приходится сталкиваться с проблемой «зацикливания» данных в найденных путях («петель»). Это приводит к увеличению времени передачи информационных пакетов, а зачастую и их потере.

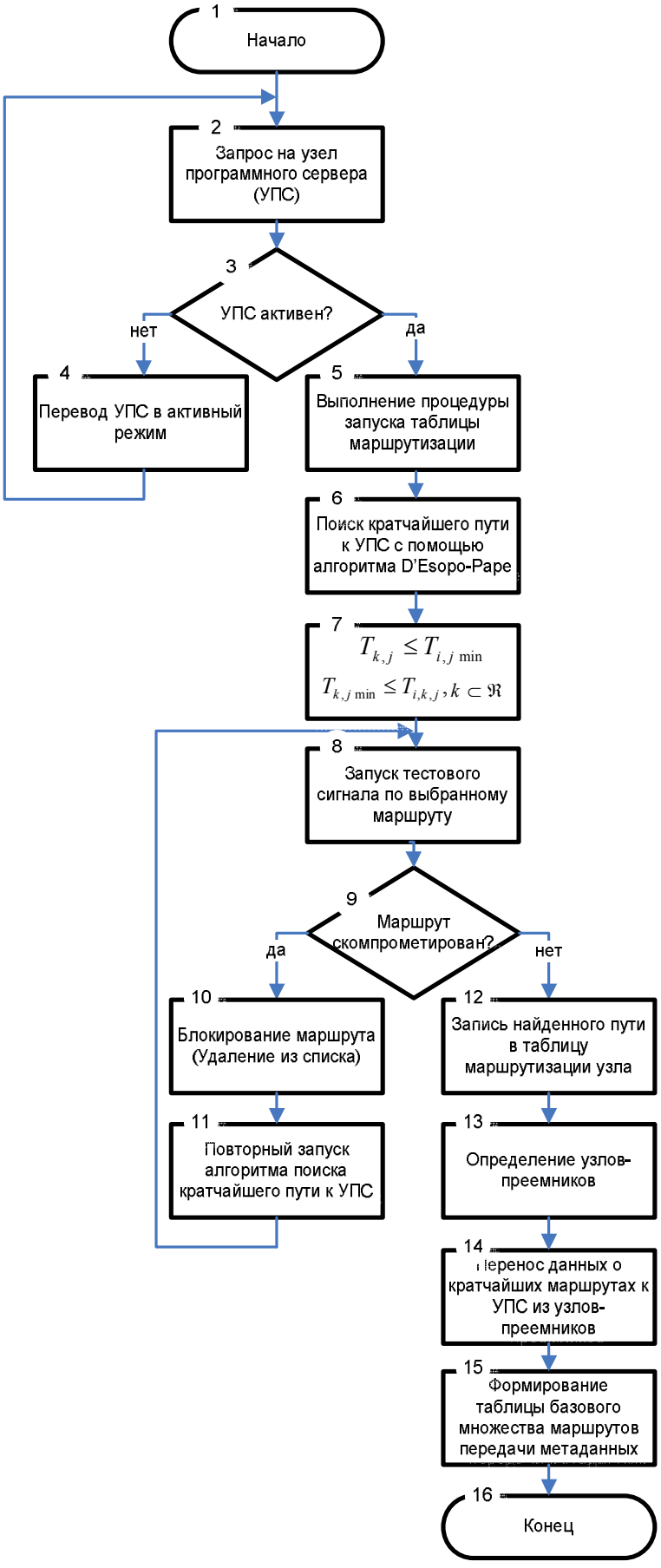

Рис. 3. Структурная схема алгоритма формирования базового множества маршрутов передачи метаданных

Избежать «петель» можно введя ограничения (условие постоянного отсутствия «петель»), представленные в виде выражений:

$$T_{k,j} \le T_{i,j\ \min}; \qquad (6)$$

$$T_{k,j\ \min} \le T_{i,k,j}; k \subset \Re, \qquad (7)$$

где $T_{k,j\ \min}$ – кратчайшее «расстояние» (минимальное время передачи информационных пакетов) от узла k к адресату j; $T_{i,k,j}$ – «расстояние» (время передачи информационных пакетов) от узла i к адресату j через узел k.

Это условие проверяется на шаге 7 рассмотренного алгоритма.

В отличие от известных алгоритмов [1, 4, 11-17] в которых не учитывается возможность компрометации (в результате кибератаки) маршрутов в разработанном алгоритме этот фактор учтен (шаги 7-11).

После того как сформировано базовое $\aleph_{баз}$ множество маршрутов передачи метаданных необходимо проводить постоянный мониторинг каналов связи и адаптивно изменять таблицы базового множества маршрутов в случае аномальных изменений в показателях тестовых сигналов. Для решения этой задачи предназначен алгоритм безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер.

Алгоритм безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер

Непосредственное использование всего найденного множества $\aleph_{баз}$ путей передачи метаданных алгоритмом, предложенным в предыдущем подразделе, не всегда возможно и оправдано. Это становится особенно очевидно в случае высокой пропускной способности хотя бы нескольких из имеющихся каналов связи, способных обеспечить выполнение требований при передаче метаданных в узлы программного сервера.

Расширение такого множества приводит к увеличению таблиц маршрутизации узлов связи, усложнению процесса распределения данных и, как следствие, к снижению достоверности передачи и информационной безопасности. Поэтому возникает необходимость в нахождении такого множества маршрутов, использование которого в условиях накладываемых ограничений позволит обеспечить максимально возможную информационную безопасность, т.е. в мониторинге каналов связи и выборе из всего найденного множества $\aleph_{баз}$ путей некоторой (оптимальной) совокупности $\aleph_{вб}$ маршрутов.

Современные требования к качеству предоставляемых услуг в ТКС задаются в параметрическом виде, системой ограничений:

$$\left\{\begin{array}{c} P_{иск} \le P_{иск_{доп}},\ Q_c \ge Q_{доп}, \\ T \le T_{доп}, P_{без} \ge P_{без_{доп}} \end{array}\right\},$$

где $P_{иск_{доп}}$ – допустимая вероятность искажения информационных пакетов в процессе передачи; $Q_{доп}$ – допустимая вероятность приема информационного пакета за время T, не превышающее допустимое.

В то же время, в условиях повышенной кибероопасности при передаче и обработке метаданных в облачных антивирусных системах, вероятность $P_{без}$ безопасной передачи данных является одним из определяющих показателей. При этом, задача безопасной маршрутизации данных трансформируется в частную оптимизационную задачу вида:

$$\left\{\begin{array}{l} P_{без} \to \max, \text{при} \\ P_{иск} \le P_{иск_{доп}}, T \le T_{доп}, Q_c \ge Q_{доп} \end{array}\right\}. \quad (8)$$

В таких условиях алгоритм безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер можно представить в виде рис. 4.

Характерной особенностью алгоритма является возможность постоянного мониторинга и учета характеристик каналов связи ТКС на маршрутах в узел программного сервера (шаги 2-7).

Именно поэтому одной из основных задач безопасной маршрутизации является определение и учет характеристических параметров линий связи,

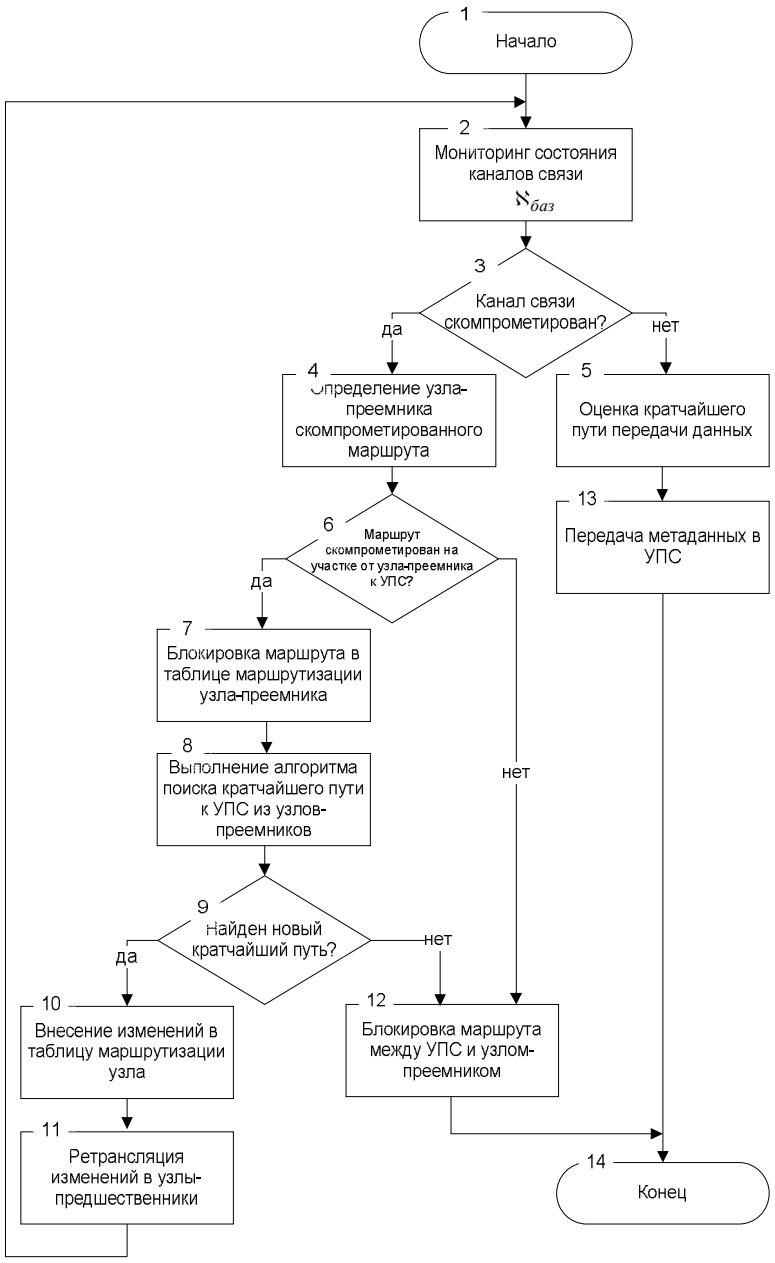

Рис. 4. Структурная схема алгоритма безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер

определяющих возможность кибератаки и несанкционированного доступа в ТКС.

Выводы

Таким образом, в работе разработаны алгоритмы формирования множества маршрутов передачи метаданных, которые являются частью метод безопасной маршрутизации метаданных в облачные антивирусные системы. Решение оптимизационной задачи выбора и формирования базового множества путей передачи данных проведено по критерию минимума времени передачи метаданных на узел программного сервера. В то же время решение частной оптимизационной задачи формирования множества выбранных маршрутов осуществлялось по крите-

рию максимума вероятности безопасной передачи данных.

Список литературы

1. Narvfiez P. New Dynamic Algorithms for Shortest Path Tree Computation / Paolo Narvfiez, Kai-Yeung Siu, Hong-Yi Tzeng // IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 8, NO. 6, DECEMBER 2000 / Электронный вариант Режим доступа: http://akira.ruc.dk/~keld/teaching/algoritmedesign_f08/Artikler/07/Narvaez00.pdf.

2. Партыка С.А. Метод ускоренной коррекции spt с использованием динамических алгоритмов / С.А. Партыка // Электронный вариант Режим доступа: http://openarchive.nure.ua/bitstream/123456789/936/1/ASU_158_2012%20%2842-47%29.pdf.

3. Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – М.: Высшая школа, 2004. – 479 с.

4. Семенов С.Г. Защита данных в компьютеризированных управляющих системах / С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко. – LAP Lambert Academic Publishing GmbH & Co. KG (Саарбрюккен, Германия), 2014. – 236 с.

5. Семенов С.Г. Разработка распределенного метода многопутевой маршрутизации, основанного на потоковой модели с предвычислением путей (маршрутов) / С.Г. Семенов, А.Г. Беленков, А.А. Можаев // Моделювання та інформаційні технології. – К.: ІПМЕ ім. Г.Є.Пухова, – 2005. – Вип. 32. – С.189-192.

6. Манько А. Защита информации в волоконно-оптических линиях связи от несанкционированного доступа / А.Манько, В. Котюк, М. Задорожний // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні" Вип.2, 2001 р. С.249-255

7. Все об оптоволокне (подборка из статей) / Электронный вариант Режим доступа: http://pst-proekt.ru/tech/vse_ob_optovolokne.pdf

8. Лавренков Ю.Н. Разработка алгоритма адаптивной маршрутизации на основе нейронечеткого иммунного подхода / Л.Г. Комарцова, Ю.Н Лавренков // Сборник трудов десятого международного симпозиума «Интеллектуальные системы», с.272 -276 , Москва 2012 г.

9. Лавренков, Ю.Н. Нейронечеткнй иммунный алгоритм для оптимизации параметров радиально-базисной нейронной сети / Ю.Н. Лавренков // Сборник материалов Всероссийской научно-технической конференции - Наукоемкие технологии в приборо- и машиностроении и развитии инновационной деятельности в ВУЗЕ, Т. 2, с.217 - 221, 2011 год, М.: МГТУ им. Н. Э. Баумана.

10. Обзор научно-технической литературы по АРТ-методам / Электронный вариант Режим доступа: http://fullref.ru/job_7d20c5db5ea838ce3ad648ed743a4630.html.

11. Смирнов С.А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 9(125). – Х.: ХУПС – 2014. – 105-110.

12. Смирнов С.А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. Вип. 4 (41). – Х.: ХУПС, 2014. – С.48-52.

13. Смирнов С.А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – № 4(17). – Харків: ХУПС. – 2014. – С.90-95.

14. Смирнов С.А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Системи обробки інформації. – Випуск 1(126). – Х.: ХУПС – 2015. – С. 150-15

15. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.

16. Смирнов С.А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных / Мохамад Абу Таам Гани, А.А. Смирнов, С.А. Смирнов // Системи озброєння і військова техніка. – Випуск 3(43) – Х.: ХУПС – 2015. – С. 100-107.

17. Смирнов С.А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А.А. Смирнов, С.А. Смирнов // Наука і техніка ПС ЗС України. – № 3(20). – Х.: ХУПС. – 2015. – С. 134-141.

Надійшла до редколегії 19.10.2016

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Національний технічний університет «Харківський політехнічний інститут», Харків.

МЕТОД БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ НА БАЗОВІЙ МНОЖИНІ ШЛЯХІВ ПЕРЕДАЧІ МЕТАДАНИХ У ХМАРНІ АНТИВІРУСНІ СИСТЕМИ

В.Л. Бурячок, С.А. Смірнов

Дана стаття присвячена розробці методу безпечної маршрутизації на базовій множині шляхів передачі метаданих в хмарні антивірусні системи. Відмінною особливістю методу є реалізація алгоритму формування множини маршрутів передачі метаданих при введенні показників оптимізації і обмежень безпечної маршрутизації.

Ключові слова: *інформаційно-телекомунікаційні мережі, хмарні антивіруси.*

METHOD SAFE ROUTE TO BASE MANY WAYS METADATA TRANSMISSION IN THE CLOUD ANTIVIRUS SYSTEM

V.L. Buryachok, S.A. Smirnov

This article is dedicated to the development of secure routing method in the base set of metadata transmission paths in the cloud antivirus system. A distinctive feature of this method is to implement the algorithm of forming a plurality of metadata transmission routes with the introduction of indicators to optimize and secure routing restrictions.

Keywords: *information and communication networks, cloud antivirus.*