

УДК 004.49.5

А.А. Смирнов, А.К. Дидык, А.Н. Дреев, С.А. Смирнов

Кировоградский национальный технический университет, Кировоград

АЛГОРИТМЫ ФОРМИРОВАНИЯ МНОЖЕСТВА МАРШРУТОВ ПЕРЕДАЧИ МЕТАДАННЫХ В ОБЛАЧНЫЕ АНТИВИРУСНЫЕ СИСТЕМЫ

Данная статья посвящена разработке алгоритмов формирования множества маршрутов передачи метаданных в облачные антивирусные системы. Отличительной особенностью алгоритмов формирования множества маршрутов передачи метаданных является показатели оптимизации и вводимые ограничения 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 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 так же 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 указано 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 $\mathcal{R} = \{V_n | n \in 1, N\}$ – множество маршрутизаторов в ТКС, V_n – n-й маршрутизатор, $N = |\mathcal{R}|$ – число маршрутизаторов, $\mathcal{Z} = \{\theta_\xi | \xi \in 1, \Theta\}$ – мно-

жество 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

$$\mathcal{S} = \{ \eta_s | s \in 1, M \},$$

где $\eta_s = \{ \theta_{s,c} | \theta_{s,c} \in \mathcal{Z}; c \in 1, \Theta \}$ – 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 \mathcal{S} 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 алго-

ритмов, відповідаючих заданим вимогам ($O(n^2 \wedge n)$) являється алгоритм D'Esopo-Pape.

Ефективність цього алгоритма підтверджується з однієї сторони результатами досліджень ряду авторів [1, 4, 11-17], а з другої сторони результатами експериментів, проведених з допомогою імітаційної моделі.

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 \bar{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.

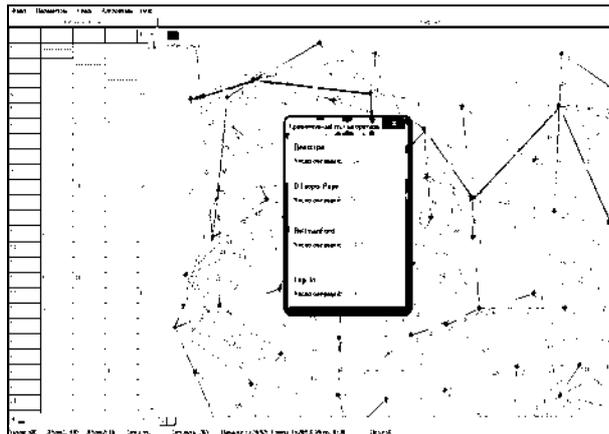


Рис. 1. Внешний вид интерфейса основной программной компоненты имитационной модели ТКС

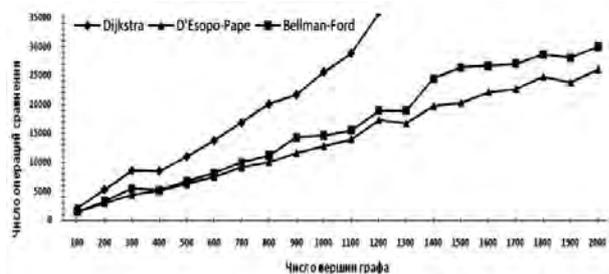


Рис. 2. Графики зависимости числа операций сравнения от числа вершин графа для различных алгоритмов поиска кратчайших путей

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 $\bar{N} = 100$.

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

$$\hat{w}(\bar{\xi})^{(i)} = \sum_{i=1}^k \hat{w}(\bar{\xi})^{(i)} / N^*; \quad \hat{\sigma}_{w(\bar{\xi})^{(i)}} = \sqrt{\bar{D}_{w(\bar{\xi})^{(i)}}};$$

$$D_{w(\bar{\xi})^{(i)}} = \sum_{i=1}^k (w(\bar{\xi})^{(i)} - \hat{w}(\bar{\xi})^{(i)})^2 / (N^* - 1).$$

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 $\hat{w}(\bar{\xi})^{(i)}$ более чем на 1:

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

где Φ – функция Лапласа вида:

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

Поведенное имитационное моделирование показало, что для всех исследуемых видов данных доверительная вероятность того, что значение статистической величины $w(\bar{\xi})$ «не отклониться» от математического ожидания $w(\bar{\xi})$ 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, включающих «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 дере-

ве допустимых маршрутов; $\aleph_{\text{баз}} = \bigcup_{u_\alpha=1}^{|U|} \aleph(u_\alpha)$ – ис-
комых путей передачи метаданных; $\aleph_{\text{вб}} \subset \aleph_{\text{баз}}$ –
множество маршрутов передачи метаданных, вы-
бранных из множества $\aleph_{\text{баз}}$ для повышения безо-
пасности, где u_α – номер уровня иерархии.

Выдвинутые предположения, а также основные процедуры рассматриваемого алгоритма формиро-
вания базового множества маршрутов передачи ме-
таданных позволяют сформулировать оптимизаци-
онную задачу повышения оперативности передачи
метаданных в пределах множества маршрутов $\aleph_{\text{вб}}$:

$$T_{\text{тс}}(\aleph_{\text{вб}}) \rightarrow \min; \tag{1}$$

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

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

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

$$P_{\text{без}} \geq P_{\text{без, доп}}. \tag{5}$$

где $P_{\text{без, доп}}$ – допустимая вероятность безопасной передачи данных.

В том случае, если не найдено ни одного рас-
пределения из множества $\aleph_{\text{вб}}$, удовлетворяющего
ограничению (5), необходимо расширить $\aleph_{\text{вб}}$ пу-
тем его объединения с множеством маршрутов сле-
дующего уровня иерархии в соответствии с (1) – (4).

Следует заметить, что при решении поставлен-
ной задачи формирования базового $\aleph_{\text{баз}}$ множества
маршрутов передачи метаданных известными алго-
ритмами поиска кратчайших путей [1, 4, 11-17] в
большинстве практических случаев приходится
сталкиваться с проблемой «зацикливания» данных в
найденных путях («петель»). Это приводит к увели-
чению времени передачи информационных пакетов,
а зачастую и их потере. Избежать «петель» можно
введя ограничения (условие постоянного отсутствия
«петель»), представленные в виде выражений:

$$T_{k,j} \leq T_{i,j \text{ min}}; \tag{6}$$

$$T_{k,j \text{ min}} \leq T_{i,k,j}, \quad k \in \aleph, \tag{7}$$

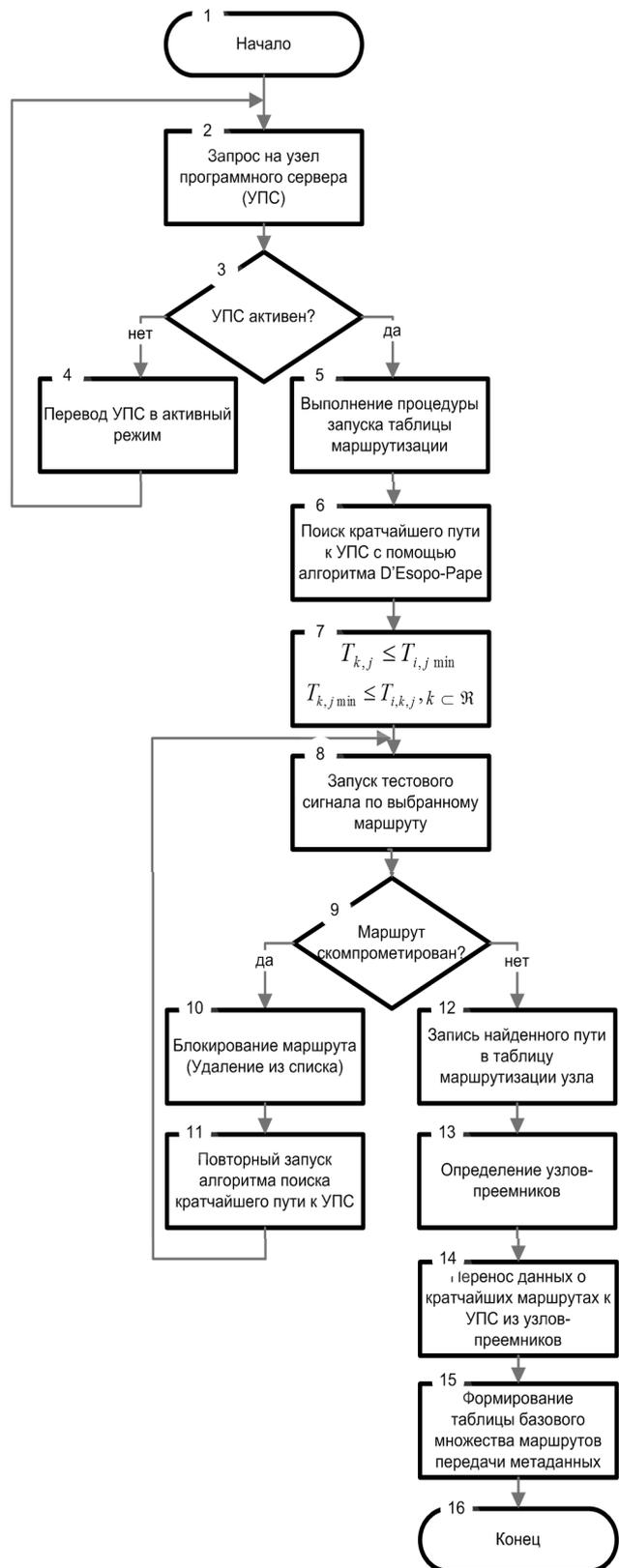


Рис. 3. Структурная схема алгоритма формирования базового множества маршрутов передачи метаданных

где $T_{k,j \text{ min}}$ – 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 адре-

сату j через вузел 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 $\mathcal{N}_{\text{баз}}$ 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 $\mathcal{N}_{\text{баз}}$ 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 $\mathcal{N}_{\text{баз}}$ путей некоторой (оптимальной) совокупности $\mathcal{N}_{\text{вб}}$ маршрутов. Современные требования к качеству предоставляемых услуг в ТКС задаются в параметрическом виде, системой ограничений:

$$\left\{ P_{\text{иск}} \leq P_{\text{иск}_{\text{доп}}}, Q_c \geq Q_{\text{доп}}, T \leq T_{\text{доп}}, P_{\text{без}} \geq P_{\text{без}_{\text{доп}}} \right\},$$

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

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

$$\left. \begin{aligned} &P_{\text{без}} \rightarrow \max, \text{ при} \\ &P_{\text{иск}} \leq P_{\text{иск}_{\text{доп}}}, T \leq T_{\text{доп}}, Q_c \geq Q_{\text{доп}} \end{aligned} \right\}. \quad (8)$$

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

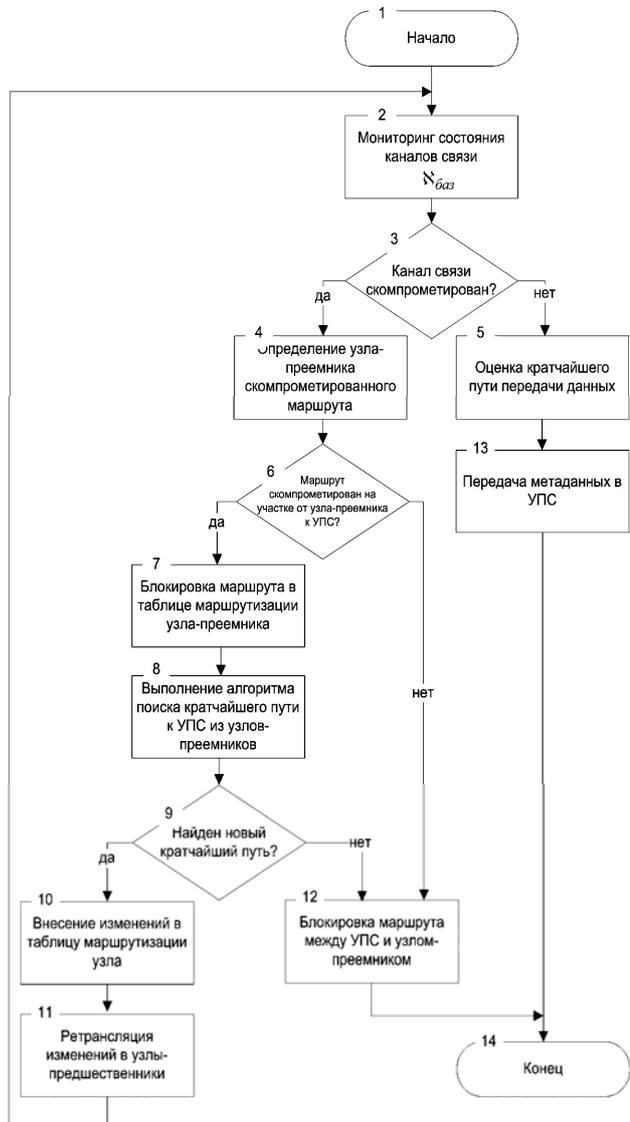


Рис. 4. Структурная схема алгоритма безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер

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, определяющих возможность кибератаки и несанкционированного доступа в ТКС.

Выводы

Таким образом, в работе разработаны алгоритмы формирования множества маршрутов передачи мета-

данных, 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 критерию максимума вероятности безопасной передачи данных.

Список литературы

1. Narvfiez P. *New Dynamic Algorithms for Shortest Path Tree Computation* [Электронный ресурс] / Paolo Narvfiez, Kai-Yeung Siu, Hong-Yi Tzeng // *IEEE/ACM transactions on networking*. – Vol. 8, no. 6. december 2000. – Режим доступа: http://akira.ruc.dk/keld/teaching/algorithmdesign_f08/Artikler/07/Narvaez00.pdf.
2. Партыка С.А. Метод ускоренной коррекции SPT с использованием динамических алгоритмов [Электронный ресурс] / С.А. Партыка. – Режим доступа: <http://openarchive.nure.ua/bitstream/123456789/936/1/ASU...pdf>.
3. Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – М.: Высшая школа, 2009. – 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. Можжаев // *Моделирование та інформаційні технології*. – К.: ПІМЕ 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 // *нПравове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. – 2001. – Вип.2. – С. 249-255
7. Все об оптоволокне (подборка из статей) [Электронный ресурс] – Режим доступа: http://pst-proekt.ru/tech/vse_ob_optovokne.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. Нейронечеткий иммунный алгоритм для оптимизации параметров радиально-базисной нейронной сети / Ю.Н. Лавренков // *Сборник материалов Всероссийской НТК. Научно-технические технологии в приборостроении и развитии инновационной деятельности в ВУЗе*. – М.: МГТУ им. Н. Э. Баумана, 2011. – Т. 2. – С. 217–221.
10. Обзор научно-технической литературы по АРТ-методам [Электронный ресурс] / Режим доступа: http://fullref.ru/job_7d20c5db5ea838ce3ad648ed743a4630.html.
11. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохаммад Абу Таам Гани, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов // *Системи обробки інформації*. – X.: ХУПС, 2014. – Вип. 9(125). – С. 105-110.
12. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохаммад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // *Збірник наукових праць Харківського університету Повітряних Сил*. – X.: ХУПС, 2014. – Вип. 4 (41). – С.48-52.
13. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохаммад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // *Наука і техніка Повітряних Сил Збройних Сил України*. – X.: ХУПС, 2014. – № 4(17). – С. 90-95.
14. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохаммад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // *Системи обробки інформації*. – X.: ХУПС, 2015. – Вип. 1 (126). – С. 150-154.
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)*. – India, Delhi, 2015. – Vol. 5, Is. 5. – P. 1-7.
16. Смирнов С.А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных / Мохаммад Абу Таам Гани, А.А. Смирнов, С.А. Смирнов // *Системи озброєння і військова техніка*. – X.: ХУПС, – 2015. – № 3(43) – С. 100-107.
17. Смирнов С.А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохаммад Абу Таам Гани, А.А. Смирнов, С.А. Смирнов // *Наука і техніка Повітряних Сил Збройних Сил України*. – X.: ХУПС, 2015. – № 3(20). – С. 134-141.

Поступила в редколлегию 14.03.2016

Рецензент: д-р техн. наук, ст. научн. сотр. С.Г. Семенов, Национальный технический университет «ХПИ», Харьков.

АЛГОРИТМИ ФОРМУВАННЯ МНОЖИНИ МАРШРУТІВ ПЕРЕДАЧІ МЕТАДАНИХ У ХМАРНІ АНТИВІРУСНІ СИСТЕМИ

О.А. Смірнов, А.К. Дідик, А.М. Дреєв, С.А. Смірнов

Дана стаття присвячена розробці алгоритмів формування множини маршрутів передачі метаданих в хмарні антивірусні системи. Відмінною особливістю алгоритмів формування множини маршрутів передачі метаданих є показники оптимізації і введені обмеження безпечної маршрутизації.

Ключові слова: інформаційно-телекомунікаційні мережі, хмарні антивіруси.

ALGORITHMS FORM A PLURALITY OF TRANSMISSION ROUTES METADATA IN CLOUD ANTIVIRUS SYSTEM

A.A. Smirnov, A.K. Didyk, A.N. Dreyev, S.A. Smirnov

This article focuses on the development of algorithms for forming a plurality of metadata transmission routes in the cloud antivirus system. A distinctive feature of the algorithms forming a plurality of metadata transmission route is a performance optimization and security restrictions imposed by routing.

Keywords: information and communication networks, cloud antivirus.