

УДК 004.49.5

**АЛГОРИТМ ФОРМИРОВАНИЯ БАЗОВОГО
МНОЖЕСТВА МАРШРУТОВ ПЕРЕДАЧИ МЕТАДААННЫХ
В ОБЛАЧНЫЕ АНТИВИРУСНЫЕ СИСТЕМЫ**

А.А. Смирнов, д.т.н., профессор

*Кировоградский национальный технический университет
dr.smirnova@gmail.com, <http://it-kntu.kr.ua>*

С.А. Смирнов, аспирант

Кировоградский национальный технический университет

А.К. Дидык, к.т.н., доцент

Кировоградский национальный технический университет

В статье рассматривается алгоритм формирования базового множества маршрутов передачи метаданных в облачные антивирусные системы

Smirnov O.A., Smirnov S.A., Didyk O.K. The article discusses the algorithm of forming a plurality of base transmission routes metadata cloud antivirus system

Ключевые слова: ПЕРЕДАЧА МЕТАДААННЫХ, ОБЛАЧНЫЕ АНТИВИРУСНЫЕ СИСТЕМЫ.

Keywords: TRANSFER METADATA CLOUD ANTIVIRUS SYSTEM.

В данной работе описан алгоритм метода безопасной маршрутизации метаданных в облачные антивирусные системы. Основными составляющими метода являются: алгоритмы формирования множества маршрутов передачи метаданных, способ контроля линий связи ТКС и модели системы нейросетевых экспертов безопасной маршрутизации.

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

Новизна способа контроля линий связи ТКС заключается в учете «скомпрометированных» бит данных специальных сигнатур, передаваемых в облачные антивирусные системы. Это позволит снизить вероятность манипуляций метаданными, передаваемыми в узлы программного сервера.

Пусть программный клиент облачной антивирусной системы установлен на некотором узле i , относительно которого существуют множества: $U = \{u_\alpha \mid \mathfrak{N}(u_\alpha) \subset \mathfrak{N}\}$ – уровней иерархии на дереве допустимых маршрутов; $\mathfrak{N}_{\bar{\alpha}\alpha} = \bigcup_{u_\alpha=1}^{|U|} \mathfrak{N}(u_\alpha)$ – искомым путей передачи метаданных; $\mathfrak{N}_{\bar{\sigma}\sigma} \subset \mathfrak{N}_{\bar{\alpha}\alpha}$ – множество маршрутов передачи метаданных, выбранных из множества $\mathfrak{N}_{\bar{\alpha}\alpha}$ 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 $\mathfrak{N}_{\bar{\sigma}\sigma}$:

$$T_{mc}(\mathfrak{N}_{\bar{\sigma}\sigma}) \rightarrow \min ; \quad (1)$$

$$|U| = \{u_\alpha \mid \mathfrak{N}(u_\alpha) \subset \mathfrak{N}\}; \quad (2)$$

$$\mathfrak{N}_{\bar{\alpha}\alpha} = \bigcup_{u_\alpha=1}^{|U|} \mathfrak{N}(u_\alpha), \quad |U| \geq 1, \quad |U| < \max_{\eta_m \in \mathfrak{N}} |\eta_m|; \quad (3)$$

$$\mathfrak{N}_{\bar{\sigma}\sigma} = \bigcup_{u_\alpha=1}^{|U|} \mathfrak{N}_{\bar{\sigma}\sigma}(u_\alpha); \quad (4)$$

$$P_{\bar{\sigma}\sigma} \geq P_{\bar{\sigma}\sigma_{\text{дон}}}. \quad (5)$$

где $P_{\bar{\sigma}\sigma_{\text{дон}}}$ – допустимая вероятность безопасной передачи данных.

В том случае, если не найдено ни одного распределения из множества $\mathfrak{N}_{\bar{\sigma}\sigma}$, удовлетворяющего ограничению (5),

необходимо расширить $\aleph_{об}$ 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 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.

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

$$T_{k,j} \leq T_{i,j \min}; \quad (6)$$

$$T_{k,j \min} \leq T_{i,k,j}, \quad k \in \mathfrak{R}, \quad (7)$$

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 в которых не учитывается возможность компрометации (в результате кибератаки) маршрутов в разработанном алгоритме этот фактор учтен.

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.