

УДК 004.49.5

### Алгоритм безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер облачной антивирусной системы

Смирнов А.А., д.т.н., проф., dr.smirnova@gmail.com,

Смирнов С.А., аспирант, Дидык А.К., к.т.н., доц.

*Кировоградский национальный технический университет, г. Кировоград*

В данной работе отображен алгоритм, который является составляющим метода безопасной маршрутизации метаданных в облачные антивирусные системы. Помимо данного алгоритма, 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.

Непосредственное использование всего найденного множества  $\aleph_{\text{баз}}$  путей передачи метаданных алгоритмом формирования базового множества маршрутов передачи метаданных, 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  $\aleph_{\text{баз}}$  путей некоторой (оптимальной) совокупности  $\aleph_{\text{об}}$  маршрутов.

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

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

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

В то же время, в условиях повышенной кибербезопасности 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:

$$\{P_{\text{без}} \rightarrow \max, \text{ при } P_{\text{иск}} \leq P_{\text{иск}_{\text{дон}}}, T \leq T_{\text{дон}}, Q_c \geq Q_{\text{дон}}\}.$$

Характерной особенностью алгоритма является возможность постоянного мониторинга и учета характеристик каналов связи ТКС на маршрутах в узел программного сервера.

Именно поэтому одной из основных задач безопасной маршрутизации является определение и учет характеристических параметров линий связи, определяющих возможность кибератаки и несанкционированного доступа в ТКС.