УДК 621.391

Еременко А. С., канд. техн. наук. Тел. +380 (63) 589 47 02. E-mail: oleksandra.yeremenko@nure.ua.
(Харьковский национальный университет радиоэлектроники)

МЕТОДИКА РАСЧЕТА ВЕРОЯТНОСТИ КОМПРОМЕТАЦИИ СООБЩЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ ПЕРЕСЕКАЮЩИХСЯ МАРШРУТОВ С ПОСЛЕДОВАТЕЛЬНО-ПАРАЛЛЕЛЬНОЙ ИЛИ КОМБИНИРОВАННОЙ СТРУКТУРОЙ

Yeremenko O. S. Methods of calculation the probability of message compromise using the overlapping paths with series-parallel or combined structure. Among the existing methods of providing a given level of security there is secure transmission of messages, divided into parts and transmitted from source to destination with multipath routing of its fragments over non-overlapping paths. In this case it is necessary to provide a specified level of network security, presented by the probability of compromise the transmitted message. As shown by the analysis, the analytical calculation of the probability of message compromise is an important step in solving the secure routing problems. However, currently it was proposed methodology for calculating the probability of message compromise only for the case of non-overlapping paths. In turn, the use of non-overlapping paths leads to inefficient use of network resources and reduce the quality of service, especially in terms of performance.

In this regard, the proposed method of calculation the probability of message compromise using overlapping routes with a series-parallel and combined structure. On a number of numerical examples analyzed the influence on the probability of message compromise the security parameters of individual elements (links), and network fragments. It is shown that the proposed method is more accurate calculation from 20% to 40% in the vast majority of initial data than previously known technique applied for the case of the overlapping paths.

Keywords: network security, quality of service, probability of compromise, multipath routing, network node, link

Єременко О. С. Методика розрахунку ймовірності компрометації повідомлення при використанні маршрутів, які перетинаються, з послідовно-паралельною або комбінованою структурою. У роботі запропонована методика розрахунку ймовірності компрометації повідомлення при використанні маршрутів, які перетинаються, з послідовно-паралельною та комбінованою структурою. На ряді числових прикладів проведений аналіз впливу на ймовірність компрометації повідомлення параметрів безпеки окремих елементів (каналів зв'язку) і фрагментів мережі. Показано, що запропонована методика дає більш точні результати розрахунку від 20% до 40% в переважній більшості вихідних даних, ніж раніше відома методика, застосована для випадку шляхів, які перетинаються.

***Ключові слова*:** мережна безпека, якість обслуговування, ймовірність компрометації, багатошляхова маршрутизація, вузол мережі, канал зв'язку

Еременко А. С. Методика расчета вероятности компрометации сообщения при использовании пересекающихся маршрутов с последовательно-параллельной или комбинированной структурой. В работе предложена методика расчета вероятности компрометации сообщения при использовании пересекающихся маршрутов с последовательно-параллельной и комбинированной структурой. На ряде численных примеров произведен анализ влияния на вероятность компрометации сообщения параметров безопасности отдельных элементов (каналов связи) и фрагментов сети. Показано, что предложенная методика дает более точные результаты расчета от 20% до 40% в подавляющем большинстве исходных данных, чем ранее известная методика, примененная для случая пересекающихся путей.

Ключевые слова: сетевая безопасность, качество обслуживания, вероятность компрометации, многопутевая маршрутизация, узел сети, канал связи

1. Введение и постановка задачи. Как показал проведенный анализ, одной из важнейших задач, регламентируемой стандартами построения сетей следующего поколения NGN, является задача реализации функций информационной безопасности. В соответствии с требованиями стандартов Международного Союза Электросвязи обеспечение информационной безопасности осуществляется в рамках трех уровней: безопасности инфраструктуры, безопасности сервисов и безопасности приложений [1]. При этом эффективность работы верхних двух уровней целиком и полностью определяется эффективностью функционирования средств уровня безопасности инфраструктуры,

основными задачами которого являются: обеспечение безопасности на уровне сетевых элементов (коммутаторов, маршрутизаторов, серверов), каналов связи и состоящих из них маршрутов в целом.

Как правило, уровень безопасности сетевых элементов оценивается с помощью такого важного показателя как вероятность компрометации, где под компрометацией понимается факт несанкционированного доступа к защищенной информации, а также подозрение осуществления такого доступа. Данные могут быть скомпрометированы в результате физической потери носителя, передачи информации по незащищенным каналам в незашифрованном виде, несанкционированного доступа постороннего лица, перехвата информации вредоносными программами, прослушивания каналов связи, а также сознательной передачи носителя с данными третьему лицу.

Если рассматривать обеспечение сетевой безопасности с точки зрения уровней модели OSI (Open Systems Interconnection) и стандарта ISO 7498-1, а также архитектуры безопасности, согласно ISO 7498-2 [2], то соответствие их уровней представляется, как показано на Рис. 1. При этом сервисы безопасности должны обеспечиваться протоколами соответствующих уровней модели взаимодействия открытых систем. В свою очередь безопасность на сетевом уровне должна поддерживаться и обеспечиваться протоколами маршрутизации.

Рис. 1. Соответствие уровней OSI и модели безопасности

На сегодняшний день эффективным представляется использование потоковых протоколов маршрутизации и соответственно их моделей вследствие таких преимуществ, как учет особенностей структуры сети, параметров каналов связи и характеристик передаваемого трафика, а также поддержка мультипотоковости и контроль перегрузки элементов сети. При этом основными целями маршрутных задач являются не только обеспечение заданного качества обслуживания, но и повышение безопасности и отказоустойчивости в сети.

Среди существующих методов обеспечения заданного уровня безопасности можно выделить защищенную передачу сообщения, разделенного на фрагменты и переданного от отправителя получателю посредством многопутевой маршрутизации с балансировкой числа фрагментов по непересекающимся маршрутам. В этом случае в ходе многопутевой маршрутизации и балансировки числа частей сообщения по путям необходимо обеспечить заданный уровень сетевой безопасности, представленной, например, вероятностью компрометации передаваемого сообщения P_{msg} :

$$P_{msg} \le \gamma_P , \qquad (1)$$

где γ_P – допустимая вероятность компрометации сообщения в сети.

Т.е. в ходе решения маршрутной задачи важно иметь инструментарий для численной оценки вероятности компрометации сообщения. В настоящее время известны только методики оценки вероятности компрометации для случая использования непересекающихся путей, т.е. для путей, в которых общими являются только узлы отправитель и получатель. Однако использование лишь непересекающихся маршрутов негативно сказывается на эффективности использования сетевого (канального, буферного) ресурса, что в итоге отрицательно сказывается на параметрах и производительности сети в целом. С целью повышения производительности необходимо задействовать маршруты, в том числе и пересекающиеся по каналам и/или узлам.

Однако в случае использования пересекающихся путей процедура численной оценки вероятности компрометации передаваемого сообщения заметно усложняется, а в ряде случаев становится невозможной (в аналитическом виде). В этой связи актуальной представляется задача поиска компромиссного решения, связанного с определением такого класса пересекающихся маршрутов, для которых возможно в аналитическом виде рассчитать, а значит, контролировать вероятность компрометации передаваемого сообщения.

2. Методики аналитического расчета вероятности компрометации передаваемого сообщения для различных классов структур используемых путей. Как показал проведенный анализ [3-5], возможность аналитического расчета вероятности компрометации передаваемого в сети сообщения во многом определяется особенностями структурного построения ТКС и типами используемых маршрутов. Как известно, множество путей в сети можно условно разделить на два подмножества: подмножество непересекающихся путей и подмножество путей, которые допускают узловое или канальное пересечение. При этом под непересекающимися понимаются только маршруты с общими узлами отправитель-получатель. Например, на Рис. 2 пути, проходящие через узлы 1→2→6, 1→3→6 и 1→4→5→6, являются непересекающимися, если узлы 1 и 6 – это отправитель и получатель пакетов, соответственно.

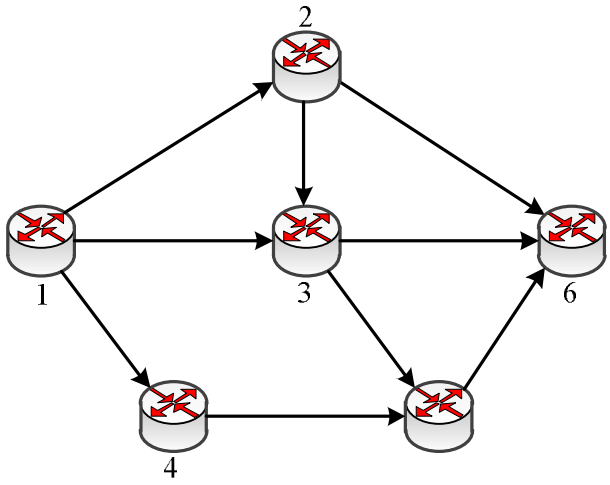

Рис. 2. Примеры типов путей при многопутевой маршрутизации

Если же пути содержат хотя бы один общий узел и/или канал, то они называются пересекающимися. Причем если пути имеют общие узлы, то они называются путями, пересекающимися по узлам, а если общие каналы – путями, пересекающимися по каналам. На рис. 2 для той же пары узлов отправитель-получатель представлены примеры пересекающихся путей, при этом пути 1→3→6 и 1→2→3→5→6 имеют узловое пересечение (узел 3), а пути 1→3→6 и 1→2→3→6 имеют канальное пересечение, т.к. у них общий канал между узлами 3 и 6.

2.1. Методика расчета вероятности компрометации для непересекающихся маршрутов. В настоящее время известны аналитические выражения для расчета вероятности компрометации сообщения, передаваемого частями по множеству непересекающихся путей. При этом предполагается, что известными являются следующие исходные данные:

S_{msg} и D_{msg} – узлы отправитель и получатель для передаваемого сообщения;

M – количество используемых непересекающихся путей при маршрутизации частей сообщения;

p_i^j – вероятность компрометации j-го элемента (узла, канала) i-го пути;

M_i – число элементов в i-м пути, подверженных компрометации.

В ходе последующих рассуждений предполагается, что отправитель и получатель безопасны, т.е. вероятности компрометации узла-отправителя и узла-получателя равны нулю. Кроме того, как и в работах [3, 4, 6], считается, что если элемент (узел, канал) пути скомпрометирован, то все фрагменты, передаваемые через этот элемент, также будут скомпрометированы. Тогда вероятность компрометации i-го пути, состоящего из M_i элементов, можно рассчитать с помощью выражения

$$p_i = 1-(1-p_i^1)(1-p_i^2)\ldots(1-p_i^{M_i}) = 1-\prod_{j=1}^{M_i}(1-p_i^j)\,. \qquad (2)$$

Одним из основных условий, которое в обязательном порядке должно выполняться в ходе безопасной маршрутизации, является то, что вероятность компрометации сообщения при его передаче по сети не должна превышать заданного допустимого значения (1). Тогда, например, вероятность компрометации сообщения, разделенного на N частей в соответствии со схемой Шамира (N,N) и передаваемого по M путям, определяется выражением [3, 4, 6]

$$P_{msg} = \prod_{i=1}^{M} p_i\,. \qquad (3)$$

Однако использование лишь непересекающихся путей при передаче сообщений отрицательно сказывается на обеспечении сбалансированной загрузки каналов связи и сети в целом, а в конечном итоге, и на уровне качества обслуживания. Поэтому с целью одновременного удовлетворений требований относительно уровня безопасности и качества обслуживания необходимо располагать инструментарием для аналитического расчета вероятности компрометации сообщения, передаваемого в том числе и по пересекающимся маршрутам.

2.2. Методика расчета вероятности компрометации сообщения при использовании пересекающихся маршрутов с последовательно-параллельной и комбинированной структурой. Как показал проведенный анализ, в случае использования в сети непересекающихся маршрутов процедура расчета вероятности компрометации сообщения значительно усложняется, а иногда становится невозможной [6-8]. При этом использование выражений (2), (3) дает адекватные результаты и для случая узлового пересечения маршрутов, но лишь при справедливости гипотезы относительно равенства нулю

вероятностей компрометации всех узлов сети, т.е. компрометации могут быть подвержены только каналы связи. Это справедливо для некоторого класса беспроводных сетей. Метод расчета путей с узловым пересечением предложен, например, в работе [8].

В данной работе предпринята попытка расширения класса пересекающихся путей, при использовании которых все еще возможно осуществить аналитический расчет вероятности компрометации передаваемого сообщения, а значит, обеспечить выполнение требований относительно уровня сетевой безопасности (1). В этой связи рассмотрим класс пересекающихся путей с последовательно-параллельной и комбинированной структурой соединения фрагментов пути, где каждый отдельный фрагмент представлен последовательным или параллельным соединением сетевых узлов и каналов связи.

При использовании пересекающихся путей с последовательно-параллельной структурой соединения его фрагментов вероятность компрометации сообщения рассчитывается как для случая его передачи по единственному пути с последовательным соединением фрагментов, причем сами фрагменты могут содержать параллельное соединение элементов сети (узлов и каналов), т.е. $P_{msg} = 1 - \prod_{j=1}^{\widetilde{N}} (1 - \widetilde{p}_j)$, где $\widetilde{N}$ – общее число последовательно соединенных фрагментов в рассматриваемой последовательно-параллельной структуре пересекающихся путей; $\widetilde{p}_j$ – вероятность компрометации j-го фрагмента, которая определяется по аналогии с формулой (3), т.е. для случая параллельного соединения сетевых элементов в рамках этого фрагмента.

Особенности расчета вероятности компрометации сообщения при использовании пересекающихся путей с последовательно-параллельной структурой соединения его фрагментов продемонстрируем на следующем примере. На Рис. 3 представлена структура сети, состоящей из двух последовательно соединенных фрагментов. Первый фрагмент включает в себя параллельно соединенные канал связи 1→3 и последовательность каналов 1→2 и 2→3. Тогда как второй фрагмент представлен каналом связи 3→4.

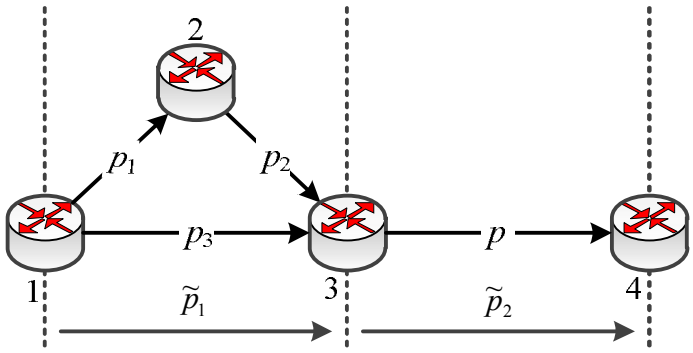

Рис. 3. Пример последовательно-параллельного соединения элементов сети

Тогда искомая вероятность компрометации рассчитывается согласно выражению $P_{msg} = 1 - (1 - \widetilde{p}_1)(1 - \widetilde{p}_2)$, где вероятности компрометации первого и второго фрагментов определяются через вероятности компрометации, составляющих их каналов связи:

$$\widetilde{p}_1 = \left[1 - (1 - p_1)(1 - p_2)\right] p_3, \quad \widetilde{p}_2 = p_4.$$

Фактически использование непересекающихся маршрутов, рассмотренных в подразделе 2.1, означает применение путей с параллельно-последовательной структурой, в которой параллельно соединенные фрагменты сети состоят лишь из последовательности сетевых элементов (узлов, каналов). Таким образом, при использовании путей с параллельно-последовательной структурой соединения его фрагментов вероятность компрометации сообщения рассчитывается как $P_{msg} = \prod_{j=1}^{\widetilde{N}} \widetilde{p}_j$, где $\widetilde{N}$ – общее число параллельно

соединенных фрагментов в рассматриваемой параллельно-последовательной структуре путей; $\tilde{p}_j$ – вероятность компрометации j-го фрагмента, которая определяется по аналогии с формулой (2), т.е. для случая последовательного соединения сетевых элементов в рамках этого фрагмента.

Наиболее общим случаем, для которого удалось предложить аналитическую процедуру расчета вероятности компрометации, является использование пересекающихся путей с комбинированной структурой, допускающей как последовательное, так и параллельное соединение разнородных фрагментов сети. Рассмотрим комбинированную структуру пересекающихся путей, представленную на рис. 4 и состоящую из семи фрагментов. Здесь фрагменты 1, 2 и 3 соединены последовательно и образуют фрагмент 4. В свою очередь последовательные фрагменты 5 и 6 являются составляющими фрагмента 7. Тогда как фрагменты 4 и 7 соединены параллельно.

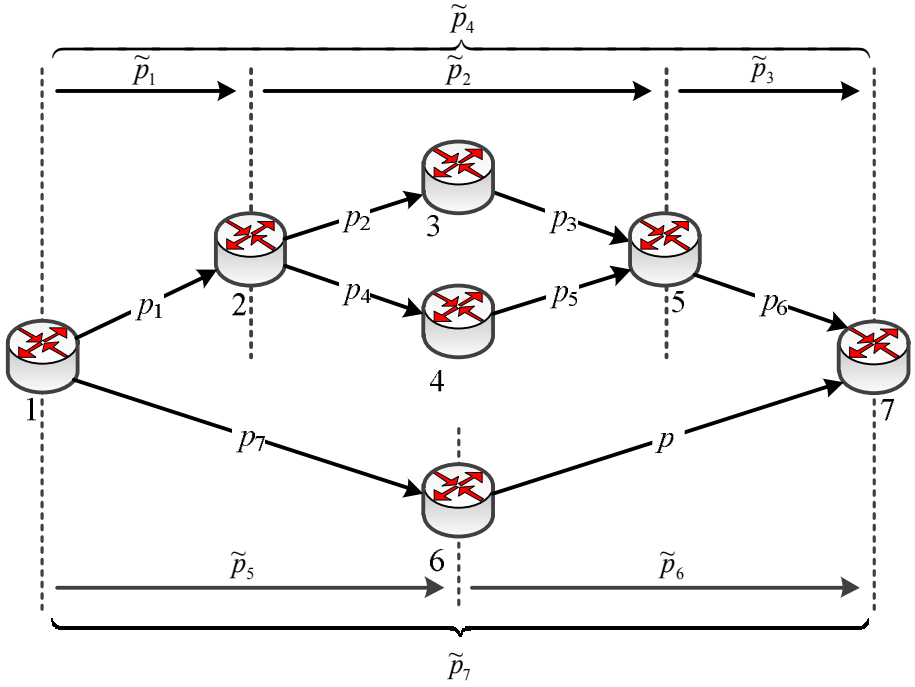

Рис. 4. Комбинированное соединение элементов сети

Тогда для рассматриваемой комбинированной структуры соединения фрагментов вероятность компрометации сообщения будет определяться как $P_{msg} = \tilde{p}_4 \cdot \tilde{p}_7$, где вероятности компрометации сетевых фрагментов 4 и 7 выражаются через соответствующие вероятности компрометации каналов связи как

$$\tilde{p}_4 = 1-(1-\tilde{p}_1)(1-\tilde{p}_2)(1-\tilde{p}_3) = 1-(1-p_1)(1-[1-(1-p_2)(1-p_3)][1-(1-p_4)(1-p_5)])(1-p_6);$$

$$\tilde{p}_7 = 1-(1-\tilde{p}_5)(1-\tilde{p}_6) = 1-(1-p_7)(1-p_8).$$

3. Анализ вероятности компрометации сообщения с использованием предложенной методики. С использованием предложенной методики произведем анализ влияния на вероятность компрометации сообщения параметров безопасности отдельных элементов (каналов связи) и фрагментов сети. Кроме того, оценим погрешность, вносимую при использовании методики, описанной в подразделе 2.1, для расчета вероятности компрометации сообщения, части которого передаются по пересекающимся путям с последовательно-параллельной структурой.

Особенности расчета вероятности компрометации сообщения будут продемонстрированы для сети, структура которой представлена на Рис. 3. В качестве исходных данных выступали значения, указанные в Табл. 1.

Исходные данные для исследования Табл. 1

№ канала связи	1	2	3	4
Вероятность компрометации канала связи p_i	0,1	0,2	0÷1	0÷1

При передаче сообщения от первого к четвертому узлу его части направлялись по двум пересекающимся маршрутам: 1→2→3→4 и 1→3→4, т.е. канал 3→4 у них являлся общим. В ходе исследования предполагалось, что вероятности компрометации первого и второго каналов были фиксированными и составляли 0,1 и 0,2 соответственно, а вероятности компрометации третьего и четвертого каналов изменялись в пределах от 0 до 1.

Расчет вероятности компрометации производился для двух случаев:

– в первом случае использовалась методика, рассмотренная в подразделе 2.1, т.е. пересечением путей в ходе расчетов пренебрегалось (P^*_{msg});

– во втором случае использовалась предложенная в подразделе 2.2 методика расчета для вероятности компрометации сообщения (P_{msg}).

Расхождение полученных результатов при использовании данных методик оценивалось по формуле $\Delta = P_{msg} - P^*_{msg}$.

Для описанных выше исходных данных оценено влияние параметров безопасности (вероятности компрометации) каналов, которые являлись (четвертый канал) и не являлись (третий канал) общими для рассматриваемых пересекающихся маршрутов (Рис. 5).

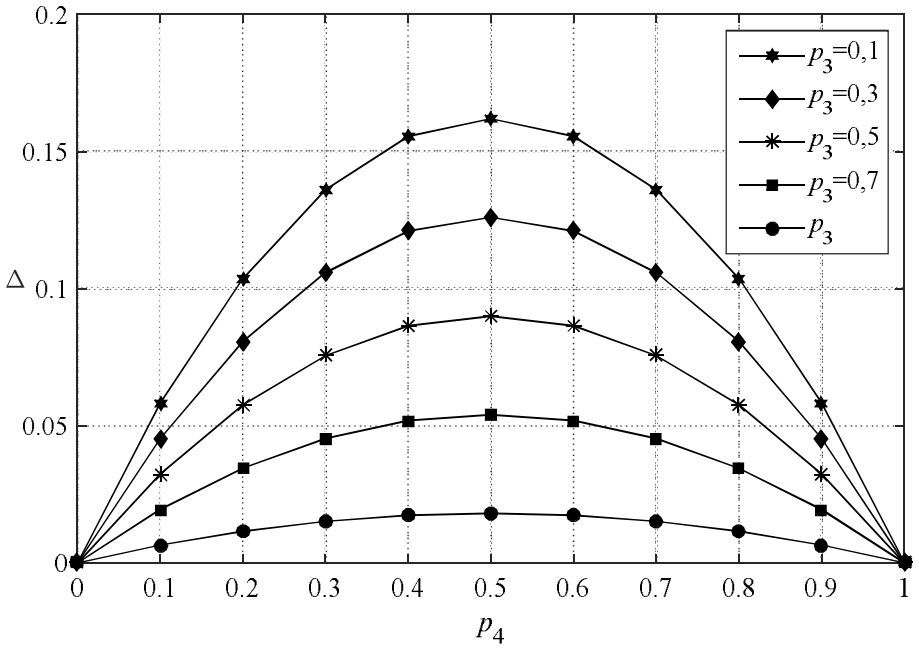

Рис. 5. Определение ошибки расчета вероятности компрометации сообщения

Как показали результаты проведенного исследования, использование методики, рассмотренной в подразделе 2.1, дает адекватные результаты при расчете вероятности компрометации сообщения лишь в двух случаях. В первом случае параметры безопасности общих элементов пересекающихся маршрутов вовсе не влияли на результаты расчета ($p_4 = 0$, $P_{msg} = P^*_{msg}$, $\Delta = 0$). Во втором случае параметры безопасности общих элементов пересекающихся маршрутов, принимая свое максимально допустимое значение, играли в ходе проводимых расчетов определяющую роль ($p_4 = 1$, $P_{msg} = P^*_{msg}$, $\Delta = 0$). Стоит отметить, что при граничных значениях p_4 (0 или 1) вероятности компрометации каналов связи, по которым пути не пересекались, на адекватность получаемых результатов не влияли.

Для других вариантов исходных данных предпочтительно использовать предложенную в подразделе 2.2 методику, т.к. пренебрежение пересечением путей приводит к ошибкам при расчете вероятности компрометации сообщения в среднем от 20% до 40% (Рис. 5).

4. Выводы

1. Как показал проведенный анализ, аналитический расчет вероятности компрометации сообщения является важным этапом в ходе решения задач безопасной маршрутизации. Однако в настоящее время предложены методики для расчета вероятности компрометации сообщения лишь для случая непересекающихся путей. В свою очередь использование непересекающихся путей приводит к неэффективному использованию сетевых ресурсов и снижению качества обслуживания, прежде всего по показателям производительности.

2. В этой связи в работе предложена методика расчета вероятности компрометации сообщения при использовании пересекающихся маршрутов с последовательно-параллельной и комбинированной структурой. На ряде численных примеров произведен анализ влияния на вероятность компрометации сообщения параметров безопасности отдельных элементов (каналов связи) и фрагментов сети. Показано, что предложенная методика дает более точные результаты расчета от 20% до 40% в большинстве вариантов исходных данных, чем ранее известная методика, примененная для случая пересекающихся путей.

3. Применение методики расчета вероятности компрометации сообщения, ранее предложенную для непересекающихся маршрутов, всегда давало более оптимистические оценки параметров безопасности при пересекающихся маршрутах. Таким образом, ее нецелесообразно использовать даже для оценки верхнего порога значения рассчитываемой вероятности компрометации сообщения.

Литература

1. ITU-T X-805. Security architecture for systems providing end-to-end communications, 2003.

2. ISO 7498-2:1989 Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, 1989.

3. Lou W. SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks / W. Lou, W. Liu, Y. Fang // INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE. – 2004. – Vol. 4. – PP. 2404 – 2413.

4. Lou W. SPREAD: Improving Network Security by Multipath Routing in Mobile Ad Hoc Networks / W. Lou, W. Liu, Y. Zhang, Y. Fang // Wireless Networks. – 2009. – Vol. 15, Issue 3. – PP. 279 – 294.

5. Alouneh S. A Multiple LSPs Approach to Secure Data in MPLS Networks / S. Alouneh, A. En-Nouaary, A. Agarwal // Journal of Networks. – 2007. – Vol. 2, Issue 4. – PP. 51 – 58.

6. Yeremenko O. S. Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET / O. S. Yeremenko, Ali Salem Ali // Radioelectronics and Informatics. – 2015. – № 1 (68). – С. 26–29.

7. Еременко А.С. Потоковая модель многопутевой маршрутизации по непересекающимся путям в телекоммуникационной сети [Електронний ресурс] / А.С. Еременко // Проблеми телекомунікацій. – 2015. – № 1 (16). – С. 85–93. – Режим доступу до журн.: http://pt.journal.kh.ua/2015/1/1/151_ yeremenko_disjoint.pdf.

8. Yeremenko O. S. Enhanced Flow-based Model of Multipath Routing with Overlapping by Nodes Paths / O. S. Yeremenko // Second International IEEE Conference Problems of Infocommunications. Science and Technology (PICS&T-2015). Proceedings. – Kharkiv: Kharkiv National University of Radio Electronics. Ukraine, Kharkiv, October 13−15, 2015. – PP. 42-45.

Дата надходження в редакцію: 09.08.2015 р. Рецензент: д.т.н., проф. О. В. Лемешко