

# МЕХАНИЗМ ПОВЫШЕНИЯ ЖИВУЧЕСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ПУТЕМ ВЫБОРА МЕТРИКИ МАРШРУТИЗАЦИИ С ИСПОЛЬЗОВАНИЕМ ТЕОРИИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Снегуров А.В., Чакрян В.Х.

Харьковский национальный университет  
радиоэлектроники, Украина.

E-mail: arksn@rambler.ru

## Abstract

*This paper demonstrates the approach of dynamic routing in telecommunication networks, where the elements of the network could be exposed to the influence of potential information security threats. The main concept of the approach is to inject the coefficient that considers the information security level of the route based on factors of network elements survivability. The coefficient is determined based on risk analysis. This allows to consider the influence of routing element failure on network survivability (considering how many links fail if routing element fails) and the probability of successful vulnerability exploitation of this routing element. This analysis allows to determine the most significant routing elements and the most safety route in the network based on the dynamic risks analysis. The goal of the further researches is to evaluate the bandwidth degradation of the links under the influence of the active attack on the routing element, to propose the methods of protection of routing elements and to develop the mechanisms of dynamic routing considering the network survivability and information security.*

Живучесть телекоммуникационной сети (ТКС) является одним из важнейших комплексных показателей, определяющих качество ее функционирования, и определяет способность ТКС выполнять свои основные функции в условиях наличия деструктивных воздействий. Под деструктивными воздействиями понимаются как воздействия физического характера, приводящие к повреждениям или уничтожениям элементов ТКС, так и воздействия информационного характера, направленные на изменения алгоритмов работы ТКС, ухудшения основных параметров функционирования ТКС. Проблеме проектирования ТКС в условиях возможности наличия непреднамеренных деструктивных воздействий (случайные повреждения линий связи, оборудования) посвящено большое количество исследований по надежности систем. Исследования по живучести сложных систем, в том числе и сетевых систем, приводятся в [1,2,3] и других источниках. Однако решение проблемы обеспечения живучести ТКС в условиях наличия преднамеренных деструктивных физических и информационных воздействий остается актуальным.

Одними из основных задач, стоящих при проектировании ТКС в условиях возможности реализации деструктивных воздействий на ее элементы, являются:

- определение тех элементов ТКС (узлов, каналов связи), выход из строя (снижение качества работы) которых приведет к ухудшению эффективности функционирования сети ниже допустимых пределов;
- разработка механизмов защиты ТКС от деструктивных воздействий, включающих выбор топологии сети, разработка алгоритмов маршрутизации с учетом живучести сети, разработка мер по защите самих элементов ТКС от деструктивных воздействий.

В данном исследовании рассматривается подход к выбору метрики маршрутизации в ТКС с учетом обеспечения живучести сети.

## I. Механизм оценки степени влияния выхода из строя элементов системы маршрутизации ТКС на ее живучесть с позиций теории риска информационной безопасности

Предположим, что существует телекоммуникационная сеть, определяемая связным физическим детерминированным графом. Структура графа описывается множеством вершин узлов (маршрутиза-

торов, коммутаторов) и множеством дуг между ними (каналов связи). Считаем, что для передачи информации по направлению от узла  $i$  в узел  $j$  может быть использовано множество маршрутов  $\{Y_k\}, k = \overline{1, K}$ . В состав каждого маршрута входит множество узлов  $\{V_n\}, n = \overline{1, N^k}$ .

Рассмотрим ситуацию, при которой деструктивным воздействием выводится из строя узел ТКС. Данная ситуация может иметь место при физическом (огневом, электромагнитном) воздействии на данный узел со стороны противника. При этом ТКС может терять сразу несколько маршрутов передачи информации. Необходимо отметить, что деструктивное воздействие также может быть организовано на канал связи путем, например, повреждения кабельной линии или радиоэлектронного подавления канала радиосвязи. Вопросы маршрутизации при комплексном воздействии на узлы и каналы связи будут рассматриваться в дальнейших работах.

В классической теории риска информационной безопасности риск ИБ – это возможный уровень воздействия на систему, определяемый исходя из вероятности реализации угрозы на ее актив, величины уязвимости данного актива и размера ущерба (ценности данного актива для системы). Последний показатель учитывает потери системы в случае реализации угрозы на актив.

С учетом вышесказанного введем термин - ценность узла ТКС для обеспечения живучести сети. Данный показатель можно найти из выражения:

$$C_n = \frac{X_n}{X_\Sigma}, \quad (1)$$

где  $X_n$  - количество всех маршрутов для направления передачи  $(i, j)$ , в состав которых входит  $n$  – й узел;  
 $X_\Sigma$  - общее количество маршрутов для направления передачи  $(i, j)$ .

Данный подход не учитывает функциональные характеристики узла (например, его пропускную способность).

Рассмотрим ситуацию, при которой информация передается от узла 1 к узлу 6 по трем маршрутам (рис.1).

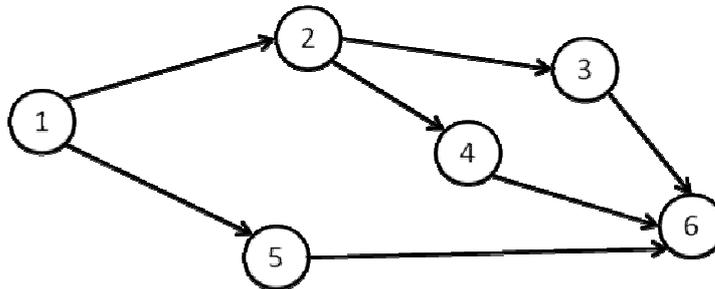


Рис. 1. Пример телекоммуникационной сети, представленный в виде графа

Тогда ценность узлов ТКС для обеспечения живучести сети будет: 2-го узла – 0,66, 3, 4, 5-го узлов – 0,33. Выход из строя (уничтожение) 2-го узла приведет к потере двух маршрутов.

Для учета возможности нападающей стороны по организации деструктивного воздействия на узлы ТКС и степени защищенности данных узлов в соответствии с теорией риска информационной безопасности введем следующие показатели -  $P_{угрн}$  - вероятность того, что нападающая сторона примет решение и организует деструктивное воздействие на  $n$  – й узел, -  $P_{уязвн}$  - вероятность того, что нападающая сторона достигнет успеха при реализации деструктивного воздействия на  $n$  – й узел. Так, например, узел 2 может находиться на значительном расстоянии от средств огневого (электромагнитного) поражения нападающей стороны, что не дает возможности осуществить эффективное деструктивное воздействие на данный узел. Кроме того, данный узел может быть хорошо защищен от деструктивного воздействия. Эти условия и будут учитываться с помощью показателей  $P_{угрн}$  и  $P_{уязвн}$ .

Тогда риск выхода из строя  $n$  – го узла для снижения живучести сети можно представить выражением:

$$R_{уязвн} = C_n \cdot P_{угрн} \cdot P_{уязвн}. \quad (2)$$

Риск нарушения живучести  $k$  – го маршрута можно определить из выражения:

$$R_{ik} = \frac{\sum_{n=2}^{N_k} R_{ij \text{ узел } n}^k}{\sum_{n=2}^{N_k} R_{ij \text{ узел } n}^k}, \quad (3)$$

где в числителе сумма рисков выхода из строя узлов, входящих в рассматриваемый -й маршрут передачи информации, а знаменателе максимальное значение риска маршрута в системе для направления передачи  $(i, j)$  (индекс  $m$  обозначает номер маршрута для направления передачи  $(i, j)$ , в котором сумма рисков выхода из строя узлов максимальна).

Например, если  $P_{у\text{тр}}^n$  и  $P_{у\text{взв}}^n$  принять для упрощения равными единице для всех узлов сети, представленных в примере, получим следующие значения риска нарушения живучести маршрутов для выбранного примера.

Для маршрута 1-2-3-6:

$$R_{1236} = \frac{0,66+0,33}{0,99} = 1.$$

Для маршрута 1-2-4-6:

$$R_{1246} = \frac{0,66+0,33}{0,99} = 1.$$

Для маршрута 1-5-6:

$$R_{156} = \frac{0,66+0,33}{0,99} = 0,33.$$

Из данного примера видно, что выход из строя узла №2 имеет максимальное влияние на живучесть системы, а маршруты, в состав которых входит данный узел имеют самый высокий уровень риска нарушения живучести сети.

## II. Подход к маршрутизации в ТКС с учетом фактора живучести

Решение задачи маршрутизации для направления передачи  $(i, j)$  можно свести к нахождению целевой функции [4]:

$$D_{ij} = \min_{k \in (i,j)} (D_k(\lambda_k)), k = \overline{1, K} \quad (4)$$

где  $D_k(\lambda_k)$  - весовые коэффициенты маршрутов.

С позиции теории массового обслуживания каждый тракт передачи ТКС рассматривается, как правило, в виде модели М/М/1. При этом поток, поступающий в сеть, считается пуассоновским, длины пакетов предусматриваются независимыми и распределенными по показательному закону. Одним из основных моментов является принятие «гипотезы о независимости», которая предусматривает, что при объединении нескольких потоков в тракте передачи сохраняется независимость между интервалами поступления и длинами пакетов [4-6]. Тогда в качестве функции, характеризующей весовой коэффициент маршрута для направления передачи  $(i, j)$  с учетом требований QoS и живучести, можно выбрать соотношение:

$$D_k(\lambda_k) = \alpha^{R_k} \sum_{n=1}^{N_k} \left( \frac{\lambda_n}{\phi_n - \lambda_n} + \tau_n^k \lambda_n \right), \quad (5)$$

где  $\lambda_n$  - информационный поток  $[1/с]$  через  $n$  - й узел;  $\phi_n$  - пропускная способность  $n$  - го узла  $[1/с]$ ;  $\tau_n^k$  - задержка формирования и распространения пакетов  $[с]$  в  $n$  - м узле с учетом задержки в прилегающем к нему канале связи  $k$  - го маршрута,  $R_k, R_k \in [0, 1]$  - риск нарушения живучести  $k$  - го маршрута. Коэффициент  $R_k$  взвешивает каждый маршрут с учетом степени риска живучести маршрута. Коэффициент  $\alpha$  может изменяться в зависимости важности информации.

### Вывод

В докладе представлен подход к маршрутизации в телекоммуникационных сетях, функционирующих в условиях возможности реализации деструктивных воздействий на ее элементы. В состав метрики маршрутизации предлагается ввести весовой коэффициент, учитывающий степень риска использования маршрута с учетом фактора живучести сетевых элементов. Данный весовой коэффициент предлагается определять с использованием подхода, представленного в теории риска информационной безопасности. Такой подход

позволяет учесть степень влияния выхода из строя узла на живучесть сети (ценность узла для сети), степень уязвимости данного узла для деструктивного воздействия и особенности целераспределения средств деструктивного воздействия нападающей стороной. При определении ценности узлов для сети учитывается возможность потери сетью нескольких маршрутов при выходе из строя одного узла. Представленный в докладе подход позволит выбирать системе маршрутизации ТКС более безопасные с точки зрения живучести маршруты на основе прогноза складывающейся ситуации. Целью дальнейших исследований является оценка влияния ухудшения пропускных способностей узлов вследствие наличия деструктивных воздействий на маршрутизацию в сети, исследование вопросов защиты узлов и каналов связи от деструктивных воздействий, разработка эффективных алгоритмов маршрутизации в ТКС с учетом обеспечения живучести и информационной безопасности сетей.

### Литература:

1. Громов Ю. Ю. и др. Синтез и анализ живучести сетевых систем. – М.: «Издательство Машиностроение-1». – 2007. – 152 с.
2. Додонов А. Г., Ландэ Д. В. Живучесть информационных систем – К.: Наук. думка. – 2011. – 256 с.
3. Кочкаров А. А., Малинецкий Г. Г. Управление безопасностью и стойкостью сложных систем в условиях внешних воздействий // Проблемы управления. – 2005. – Т. 5. – №. 0. – С. 70-76.
4. Gallager R. A minimum delay routing algorithm using distributed computation // Communications, IEEE Transactions on. – 1977. – V. 25, №. 1. – P. 73-85.
5. Lemeshko O., Drobot O. A Mathematical Model of Multipath QoS-based Routing in Multiservice Networks // Modern Problems of Radio Engineering, Telecommunications, and Computer Science, 2006. TCSET 2006. International Conference. – IEEE, 2006. – С. 72-74.
6. Лемешко А.В., Дробот О.А., Добрышкин Ю.Н. Повышение масштабируемости управления трафиком и обеспечения качества обслуживания с использованием оверлейных сетей [Электронный ресурс] // Проблемы телекоммуникаций. – 2011. – № 1 (3). – С. 11 – 27. – Режим доступа: [http://pt.journal.kh.ua/2011/1/1/111\\_lemeshko\\_scalability.pdf](http://pt.journal.kh.ua/2011/1/1/111_lemeshko_scalability.pdf).