УДК 621.391
DOI: 10.15827/0236-235X.122.316-320
Дата подачи статьи: 06.10.17
2018. Т. 31. № 2. С. 316–320

# *К ВОПРОСУ ОЦЕНКИ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ЭЛЕМЕНТОВ СЕТИ СВЯЗИ*

*Г.В. Попков* [1], *к.т.н., доцент, glebpopkov@rambler.ru*

[1] *Сибирский государственный университет телекоммуникаций и информатики, ул. Кирова, 86, г. Новосибирск, 630102, Россия*

В статье рассматриваются вопросы оценки устойчивости функционирования сети электросвязи к разрушающим деструктивным воздействиям. Предложена методика по представлению атакуемой сети электросвязи в виде динамических гиперсетей, позволяющих давать объективную оценку состоянию атакуемой сети с точки зрения устойчивости. Введены понятие разрушающего деструктивного воздействия и связанное с ним понятие канала разрушающего деструктивного воздействия на элементы NE сети связи, находящиеся на различных уровнях гиперсетевых моделей.

Простота и удобство представления атакуемой сети в виде динамических гиперсетей позволяют расширить класс задач, связанных с определением устойчивости сетей связи к внешним деструктивным воздействиям, в частности, находить корреляционные связи между частными моделями нарушителя, моделями атак и моделями уязвимости сети электросвязи на исследуемом уровне. Такой подход позволяет проектировать устойчивые сети связи с учетом динамически меняющихся внешних факторов, связанных с угрозами, направленными на структуру сети связи, а также эффективно выявлять и блокировать угрозы, связанные с внешними информационными воздействиями, обеспечивая доступность, целостность, конфиденциальность пользовательской информации.

На основании предложенных подходов представляется целесообразным создавать онтологии знаний, основанные на реакции сети на разрушающее деструктивное воздействие в точках мониторинга сети электросвязи, что, в свою очередь, позволит эффективно проектировать и инсталлировать средства защиты информации на реальных сетевых структурах.

Предложена частная математическая модель внешнего деструктивного воздействия, основанная на применении теории вероятности, позволяющая прослеживать динамические изменения в структуре сети электросвязи и определять количественные оценки QoS приложений.

***Ключевые слова:*** *устойчивость функционирования сети электросвязи, QoS, теория вероятности, модель нарушителя, модель угроз, проектирование сетей связи.*

В настоящее время большое внимание уделяется вопросам анализа степени защищенности сетей связи [1–3] и разработке методов защиты пользовательской информации на сетевом уровне модели OSI [4, 5]. Тем не менее, все актуальнее становятся задачи обеспечения устойчивости функционирования сети в результате *разрушающих деструктивных воздействий* (РДВ).

Основные понятия и определения предметной области «Устойчивость сети электросвязи» (устойчивость функционирования сети, дестабилизирующий фактор, живучесть сети связи) сформулированы в [6, 7] и ГОСТ 53111-2008.

Целесообразно представить элемент сети связи в виде закрытой системы, реагирующей на внешние воздействия РДВ. Представление узла связи возможно в виде A-, D-схем Бусленко, дискретных цепей Маркова (P-схемы, q-схемы), динамических гиперсетевых моделей, Fuzzy-технологий. Очевидно, что при наличии большого множества сетевых элементов NE требуется декомпозиция при решении задач повышения устойчивости того или иного сегмента (множества элементов NE) сети связи.

В частности, имеет смысл группировка элементов NE по их функциональным возможностям, ролям, выполняемым на определенных уровнях сети связи. Получая устойчивые зависимости поведения групп NE от внешних воздействий, можно формализовать приближенные модели нарушителя и модели угроз для различных ситуаций, возникающих на уровне взаимодействия <нарушитель–угроза–сеть связи>.

В дальнейшем этот вид записи удобно применять для описания конкретного воздействия на единичный или группу подобных элементов NE. Избирательное воздействие на один NE будем называть каналом РДВ, очевидно, что на множество NE воздействует множество каналов РДВ.

Рассмотрим действие канала РДВ в плоскости проектируемой сети связи. В момент времени $t_i$ формируется случайный граф состояния атакуемого сегмента сети связи. Назовем его суграфом ошибок, являющимся частью полного графа $G_{na}$ сегмента сети связи на момент воздействия РДВ. Ошибка в данном случае – это невыполнение хотя бы одного пункта из списка критически важных процессов, протекающих в сети связи (например, непрохождение служебной управляющей информации по каналу ОКС-7 сегмента сети SDH).

По скорости изменений состояний суграфа ошибок можно судить о типе и мощности РДВ на часть графа $G_{na}$. Очевидно, что состояние сетевых элементов NE графа $G_{na}$ имеет (может принимать) в общем случае бесконечное число состояний из списка процессов, протекающих в сети связи [8]. В этом случае для дальнейшей формализации задачи необходимо ввести понятие матрицы (множе-

ства) состояний элементов NE суграфа сети связи в момент воздействия РДВ в определенный момент времени $t_n$, а также массив отношений между элементами NE в суграфе ошибок на момент возникновения РДВ.

Осуществляя мониторинг потока РДВ в реальном времени на атакуемый сегмент, можно решить обратную задачу по выработке критериев или набора угроз, характеризующих модель угроз и модель нарушителя для конкретного вида сетевой атаки.

В этом случае при проектировании устойчивой сети связи с заданными параметрами большой интерес представляет построение частной модели угроз и модели нарушителя, способных подавлять работоспособность узлов сети связи сколь угодно времени вплоть до выведения узла из штатного режима работы на длительный срок, превышающий нормы на время восстановления для сетей связи конкретного вида [9–11].

Можно предположить, что на каждом из указанных уровней сети возможен стохастический поток РДВ, позволяющих говорить о параллельном воздействии на сеть связи в широком смысле. Представляется важным отделять в случае анализа угроз на сеть связи пользовательский трафик от служебного (например управляющего), циркулирующего в системах управления сетями связи (например TMN, OSS/BSS).

Очевидно, что в случае избирательного воздействия РДВ на управляющую сеть связи критически важным становится служебный трафик, в случае подавления которого сегменты сети связи выходят из штатного режима работы вплоть до полной неработоспособности. Приведем пример частной математической модели поведения сетевого элемента NE на РДВ при условии, что служебный трафик, циркулирующий в кластере сети связи, имеет пуассоновское распределение.

## Частная математическая модель РДВ на элементы сети электросвязи

Для решения данной задачи воспользуемся формулами определения вероятностей Эрланга.

Определим показатель устойчивости атакуемой сети *Stab* (stability – устойчивость) и показатель *Int* (intense – интенсивность), тогда *Stab* = 1 – *Int* – интенсивность отказов в обслуживании проходящего через узел трафика. Таким образом, чем выше показатель устойчивости, тем меньше вероятность блокировки трафика, а следовательно, тем большее число запросов в единицу времени обрабатывается сетью связи в нормальном режиме и атакуемая сеть связи более устойчива к разрушающему воздействию. Для практических расчетов и анализа удобнее использовать параметр *Int*, так как качество сети связи определяется, в первую очередь, величиной потерь, а не скоростью поступления обслуживания вызовов.

Введем следующие обозначения: $N$ – общее количество сетевых узлов (NE) в зоне РДВ (кластер); $n$ – случайное число NE, сохранивших работоспособность; $m$ – число каналов, приходящееся на один NE; $\lambda$ – интенсивность сетевой нагрузки на атакуемый кластер; $\mu$ – интенсивность обслуживания запросов по видам услуг. Для дальнейших выводов полагаем, что один нормализованный канал обслуживает один вызов.

Предположим, что трафик, поступающий в систему, соответствует пуассоновскому распределению. Приведем два варианта развития ситуации РДВ для NE.

***Вариант 1.*** Пусть вероятность выживания всех NE одинаковая и равна $p$. Например, данное предположение справедливо, если все узлы кластера находятся в зоне действия РДВ. Тогда, очевидно, вероятность выживания $k$ узлов NE определяется биноминальным распределением вида

$$P(n=k) = C_N^k p^k (1-p)^{N-k}.$$

Пользователи, подключенные к атакуемым NE, перенаправляются к соседним выжившим NE, используя механизм перемаршрутизации. В этом случае можно предположить, что параметр интенсивности суммарной нагрузки $\lambda$ не меняется.

Вероятность блокировки во время пуассоновского процесса поступления трафика и при наличии $mk$ каналов вычисляется по B-формуле Эрланга:

$$P_{\text{блк}}(k) = \frac{\dfrac{\rho^{mk}}{(mk)!}}{\dfrac{\sum_{i=0}^{mk}\rho^i}{i!}}, \qquad (1)$$

где коэффициент обслуживания

$$\rho = \frac{\lambda}{\mu}. \qquad (2)$$

Очевидно, что формула для потерь остается в силе, даже если распределение вероятностей длительности обслуживания произвольное. Отсюда можно вычислить оценку блокировки трафика:

$$Int = \sum_{k=0}^{N} P(n=k) P_{блк}(k) =$$

$$= \sum_{k=1}^{n} C_N^k p^k (1-p)^{N-k} \frac{\dfrac{\rho^{mk}}{(mk)!}}{\dfrac{\sum_{i=0}^{mk}\rho^i}{i!}} + (1-p)^N. \qquad (3)$$

Соответственно, устойчивость вычисляется следующим образом:

$$Stab = 1 - \sum_{k=0}^{N} C_N^k p^k (1-p)^{N-k} \frac{\dfrac{\rho^{mk}}{mk!}}{\dfrac{\sum_{i=0}^{mk}\rho^i}{i!}}. \qquad (4)$$

Таким образом, получена формула оценки устойчивости кластера сети связи через такие параметры системы, как количество обслуживающих трафик узлов NE, емкость и число каналов, нагрузка, проходящая через NE.

Для дальнейшего анализа формулу (3) удобно записать в виде двух слагаемых, первое из которых характеризует вероятность блокировки вызова при наличии выживших NE, второе – вероятность уничтожения всех NE. В последнем случае трафик, проходящий через узел, блокируется с вероятностью 1.

Как правило, интенсивность трафика, или средняя длительность сеанса связи между корреспондирующими парами, может зависеть от числа вышедших из строя NE, например, увеличивается трафик от пользователей, уничтоженных NE, на соседние выжившие NE в атакуемом кластере [12].

В данном случае формула (3) остается верной, лишь ρ изменяется на ρ($k$), соответственно в (2), где ρ($k$) = λ($k$)/μ($k$).

***Вариант 2.*** Вероятность выживания NE возрастает с увеличением расстояния от источника атаки РДВ (см. рисунок).

Далее упорядочим вероятности выживания NE в зависимости от расстояния $R$ от канала воздействия РДВ до NE по возрастанию и пронумеруем:

$p1 \ge p2 \ge p3 \ge \ldots \ge pN$, $p_i = p(R_i)$.

В этом случае полагаем, что вероятность равенства $R_i = R_j$, $i \ne j$, равна нулю. Введем обозначение множества индексов: $I = \{1, \ldots, N\}$.

Тогда

$$P(n=0) = \prod_{i=1}^{N}(1-p_i),$$

$$P(n=1) = \sum_{j=1}^{N} p_j \prod_{i \in I \setminus j}(1-p_i),$$

$$P(n=k) = \sum_{j_1 \ldots j_k} p_{j_1} \ldots p_{j_k} \prod_{i \in I \setminus \{j_1 \ldots j_k\}}(1-p_i),$$

$$P(n=N) = \prod_{i=1}^{N} p_i$$

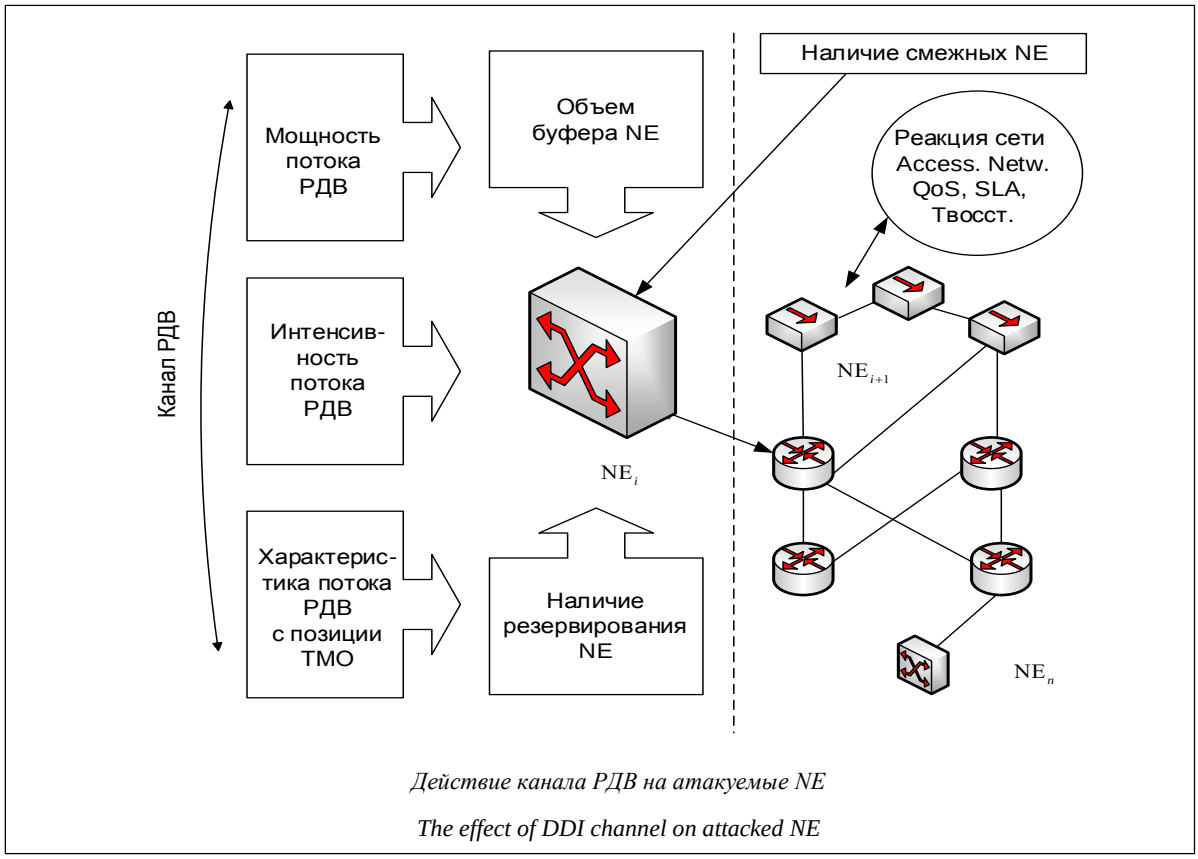
и равенство (3) в случае варианта 2 принимает вид

$$Int = \sum_{k=0}^{N} \sum_{j_1 \ldots j_k} p_{j_1} \ldots p_{j_k} \prod_{i \in I \setminus \{j_1 \ldots j_k\}}(1-p_i) \frac{\frac{\rho^{mk}}{mk!}}{\sum_{i=0}^{mk} \frac{\rho^i}{i!}} + \prod_{i=1}^{N}(1-p_i). \quad (5)$$

Соответственно, устойчивость кластера NE в случае варианта 2 будет отражена формулой

$$Stab = 1 - \sum_{k=0}^{N} \sum_{j_1 \ldots j_k} p_{j_1} \ldots p_{j_k} \prod_{i \in I \setminus \{j_1 \ldots j_k\}}(1-p_i) \frac{\frac{\rho^{mk}}{mk!}}{\sum_{i=0}^{mk} \frac{\rho^i}{i!}}. \quad (6)$$

Используя полученные результаты для анализа устойчивости сети связи, дадим оценку влияния параметров сети связи на показатель устойчивости.




*Действие канала РДВ на атакуемые NE*

*The effect of DDI channel on attacked NE*

Заметим, что в случае $\lim_{m\to\infty} Int(m) = (1-p)^N$, то есть при большом количестве независимых каналов связи, показатель устойчивости *Stab* определяется последним слагаемым формулы и равен вероятности уничтожения всех NE. В данном случае принципиальное значение имеет резервирование критически важных сетевых ресурсов на сети связи. В рассматриваемом примере получаем зависимость вероятности обеспечения доступности от блокировки трафика в сетевых элементах NE с различной степенью потерь обслуживаемого трафика.

Применяя такого рода модели, можно проследить происходящие в сети динамические изменения в случае воздействия на сеть РДВ различной природы. Более того, задавая метрики элементов сети, мы можем давать достаточно точные оценки возможного ущерба, наносимого разрушающими воздействиями.

В дальнейших исследованиях в качестве базисной предлагается рассматривать 8-уровневую гиперсетевую модель для построения устойчивой сети связи, полностью задающую структуру и состав сети связи, состоящую из пассивных и активных сетевых элементов, включая ПО. Данный подход был предложен автором в [11].

Предложенная методика позволит, например, в дальнейшем эффективно строить частные модели нарушителя, угроз, уязвимостей, возникающих на различных уровнях гиперсетевой комплексной модели сети связи.

В результате можно более эффективно выстраивать политики безопасности сетей связи общего пользования на всех уровнях, начиная со структуры первичной сети и заканчивая уровнями, представляющими непосредственный обмен, хранение и модификацию критически важной информации.

***Литература***


1. Бычков Е.Д. Математические модели управления состояниями цифровой телекоммуникационной сети с использованием теории нечетких множеств: монография. Омск: Изд-во ОмГТУ, 2010. 236 с.
2. Величко В.В., Попков Г.В., Попков В.К. Модели и методы повышения живучести современных систем связи. М.: Горячая линия–Телеком, 2014. 270 с.
3. Киселев Л.К., Маркелов А.П., Воробьев Б.В. Концептуальные основы обеспечения устойчивости сетей связи // Электросвязь. 1994. № 2.
4. Мошак Н.Н. Модели, методы и алгоритмы анализа процессов функционирования инфотелекоммуникационных транспортных систем: автореф. дис. … д-ра технич. наук. СПб, 2009. 32 с.
5. Новиков С.Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи; [под ред. В.П. Шувалова]. М.: Горячая линия–Телеком, 2015. 128 с.
6. ITU-T Recommendation G.1000 (11/2001). Communications Quality of Service: A framework and definitions.
7. ITU-T P.862. Perceptual evaluation of speech quality (PESQ): An objective method for endtoend speech quality assessment of narrowband telephone networks and speech codecs.
8. Попков В.К. Математические модели связности. Н.: Изд-во ИВМ и МГ СО РАН, 2006. 490 с.
9. Конин М.В., Лепнер Э.Ю., Попков Г.В. Применение гиперсетей для автоматизированного проектирования инженерной инфраструктуры предприятия // Проблемы информатики. 2013. № 2. С. 65–72.
10. Попков Г.В., Попков В.К. Вопросы проектирования, строительства и эксплуатации первичных сетей связи // Проблемы информатики. 2013. № 4. С. 60–65.
11. Попков Г.В. Перспективное проектирование сети абонентского доступа с использованием восьмиуровневой модели // Программные продукты и системы. 2016. № 2. С. 139–145.
12. Ромашкова О.Н., Дедова Е.В. Живучесть беспроводных сетей связи в условиях чрезвычайной ситуации // T-Comm. 2014. № 6. С. 40–43.


Software & Systems
DOI: 10.15827/0236-235X.122.316-320

Received 06.10.17
2018, vol. 31, no. 2, pp. 316–320

**ON THE ISSUE OF ASSESSING STABILITY OF FUNCTIONING OF COMMUNICATION NETWORK ELEMENTS**

***G.V. Popkov*** [1], *Ph.D. (Engineering), Associate Professor, glebpopkov@rambler.ru*

[1] *Siberian State University of Telecommunications and Information Sciences, Kirov St. 86, Novosibirsk, 630102, Russian Federation*

**Abstract.** The article considers the issues of assessing stability of power grid functioning to destructive destabilizing influences (DDI). The proposed method represents an attacked telecommunication network as dynamic hyper network that allow objective assessing an attacked network state in the context of stability. The author introduces a concept of DDI and the related concept of a DDI channel that affects NE elements of a communication network at different levels of hyper network models.

Simplicity and convenience of representing an attacked network in the form of dynamic hyper networks makes it possible to extend the class of problems related to determining stability of communication networks to external destructive influences, in particular, to find correlation links between private intruder models, attack models and vulnerability models of a power grid

at the investigated level. Such approach allows designing stable communication networks taking into account dynamically changing external factors connected with threats directed to a communication network structure. It also allows effective detecting and blocking threats related to external information influences while ensuring accessibility, integrity, confidentiality of user information.

Due to the proposed approaches, it seems appropriate to create knowledge ontologies based on a network response to DDI at network monitoring points, which in turn will effectively design and install information protection tools in real network structures.

The author proposes a private mathematical model of external destabilizing influence, which is based on the probability theory. It makes it possible to trace dynamic changes in a network structure and determine quantitative estimates of QoS applications.

**Keywords:** destructive destabilizing influences, hypernetwork theory, QoS, theory of probability, Fuzzy method, graph theory.

***References***

1. Bychkov E.D. *Matematicheskie modeli upravleniya sostoyaniyami tsifrovoy telekommunikatsionnoy seti s ispolzovaniem teorii nechotkikh mnozhestv* [Mathematical Models of State Management of a Digital Telecommunication Network Using the Theory of Fuzzy Sets]. Monograph. Omsk, OmGTU Publ., 2010, 236 p.

2. Velichko V.V., Popkov G.V., Popkov V.K. *Modeli i metody povysheniya zhivuchesti sovremennykh sistem svyazi* [Models and Methods of Increasing Survivability of Modern Communication Systems]. Moscow, Goryachaya liniya–Telekom Publ., 2014, 270 p.

3. Kiselev L.K., Markelov A.P., Vorobev B.V. Conceptual framework for ensuring stability of communication networks. *Elektrosvyaz*. 1994, no. 2.

4. Moshak N.N. *Modeli, metody i algoritmy analiza protsessov funktsionirovaniya infotelekommunikatsionnykh transportnykh sistem* [Models, Methods and Algorithms for Analyzing Functioning Processes of Infotelecommunication Systems]. PhD Thesis. St. Petersburg, 2009, 32 p.

5. Novikov S.N. *Metodologiya zashchity polzovatelskoy informatsii na osnove tekhnology setevogo urovnya multiservisnykh setey svyazi* [Methodology for Protecting User Information Based on Network Layer Technologies of Multiservice Communication Networks]. V.P. Shuvalov (Ed.). Moscow, Goryachaya liniya–Telekom Publ., 2015, 128 p.

6. ITU-T Recommendation G.1000 (11/2001). *Communications Quality of Service: A framework and definitions*.

7. ITU-T P.862. *Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrowband telephone networks and speech codecs*.

8. Popkov V.K. *Matematicheskie modeli svyaznosti* [Mathematical Models of Connectivity]. Novosibirsk, IVM i MG SO RAN Publ., 2006, 490 p.

9. Konin M.V., Lepner E.Yu., Popkov G.V. Application of hyper-networks for automated design of an engineering infrastructure of an enterprise. *Problemy informatiki* [Problems of Computer Science]. 2013, no. 2, pp. 65–72 (in Russ.).

10. Popkov G.V., Popkov V.K. Issues of design, construction and operation of primary communication networks. Novosibirsk. *Problemy informatiki* [Problems of Computer Science]. 2013, no. 4, pp. 60–65 (in Russ.).

11. Popkov G.V. Advansed design of a customer access network using an 8-tier model. *Programmnye produkty i sistemy* [Software & Systems]. 2016, no. 2, pp. 139–145 (in Russ.).

12. Romashkova O.N., Dedova E.V. Survivability of wireless communication networks in an emergency. Moscow, *T- Comm*. 2014, no. 6, pp. 40–43 (in Russ.).

## Примеры библиографического описания статьи

1. Попков Г.В. К вопросу оценки устойчивости функционирования элементов сети связи // Программные продукты и системы. 2018. Т. 31. № 2. С. 316–320. DOI: 10.15827/0236-235X.122.316-320.

2. Popkov G.V. On the issue of assessing stability of functioning of communication network elements. *Programmnye produkty i sistemy* [Software & Systems]. 2018, vol. 31, no. 2, pp. 316–320 (in Russ.). DOI: 10.15827/0236-235X.122.316-320.