



DOI: <https://doi.org/10.15688/NBIT.jvolsu.2018.4.5>

УДК 004.056

ББК 32.81

МЕТОДИКА ОЦЕНКИ УСТОЙЧИВОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ

Михаил Антонович Коцыняк

Доктор военных наук, профессор,
Военная академия связи им. Маршала Советского Союза С.М. Буденного,
kot-c@yandex.ru
Тихорецкий просп., 6, 194064 г. Санкт-Петербург, Российская Федерация

Александр Петрович Нечепуренко

Адъюнкт,
Военная академия связи им. Маршала Советского Союза С.М. Буденного
brother-aks@yandex.ru
Тихорецкий просп., 6, 194064 г. Санкт-Петербург, Российская Федерация

Валерий Михайлович Московченко

Доктор экономических наук, профессор, профессор кафедры информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) им. М.И. Платова,
fvo.urgpu.npi@yandex.ru
ул. Просвещения, 132, 346428 г. Новочеркасск, Российская Федерация

Аннотация. В статье представлена методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия. Представленный подход позволяет определить очередность и вид воздействия на каждый элемент ИТКС, что позволит оценить комплексный показатель устойчивости сети (коэффициент простоя или исправного действия).

Ключевые слова: информационно-телекоммуникационная сеть, информационное воздействие, устойчивость сети, коэффициент простоя, комплексный показатель.

В современной войне первоочередными объектами направленного противодействия и поражения стали не войска и оружие, а системы управления противника. Прогнозируемый характер воздействия противника на систему военного управления и информационно-телекоммуникационную сеть (далее – ИТКС) как ее техническую основу обуславливает появ-

ление новых требований к показателям качества функционирования ИТКС.

Использование в ИТКС технологий, средств связи и программного обеспечения иностранного производства, интеграция ИТКС в сеть связи общего пользования (далее – ССОП), а ССОП – в мировое информационное пространство предопределили сме-

шение акцентов на достижение превосходства над противником на основе применения компьютерных атак (далее – КА).

Результатом воздействия КА является блокирование управляющей и внедрение ложной информации, нарушение установленных регламентов сбора, обработки и передачи информации, отказы оборудования, сбои в работе ИТКС, а также компрометация передаваемой (получаемой) информации. По оценке зарубежных экспертов эффект воздействия КА сравним с применением оружия массового поражения.

Воздействие на ИТКС путем применения противником КА приведет к существенному снижению устойчивости ИТКС и, как следствие, снижению эффективности информационного обмена между органами управления. Составляющими устойчивости являются живучесть, надежность и помехоустойчивость, которые не учитывают воздействие КА.

Учитывая вышеизложенное, предлагается ввести четвертую самостоятельную составляющую устойчивости ИТКС – киберустойчивость. Под киберустойчивостью понимается способность ИТКС поддерживать управление в условиях воздействия КА.

Таким образом, составляющие устойчивости будут оцениваться: живучесть – коэффициентом исправного действия ИТКС по живучести; помехоустойчивость – коэффициентом исправного действия по помехоустойчивости; надежность – коэффициентом исправного действия по надежности; киберустойчивость – коэффициентом исправного действия по киберустойчивости.

Поскольку перерывы связи из-за воздействия помех, ядерного оружия, компьютерных атак, а также по технико-эксплуатационным причинам события независимые, устойчивость ИТКС можно оценить как произведение всех составляющих ее показателей.

Анализ возможностей противника и взглядов зарубежных военных специалистов

на современные методы ведения войны показывает, что существующие способы защиты ИТКС не в полной мере могут обеспечить ее устойчивое функционирование в условиях информационного противоборства. С учетом приведенных выше данных возникает необходимость разработки комплексной методики оценки устойчивости ИТКС.

С этой целью первоначально требуется определить наиболее опасные средства воздействия для ИТКС на определенный момент времени, то есть найти матрицу назначения средств воздействия, показывающую очередность воздействия и вероятность. Для решения этой задачи предлагается использовать метод максимального элемента [1]. Полученные в матрице назначения являются исходными данными при обосновании структуры системы защиты и принятии мер по защите элементов. С этой целью предлагается определить вероятностно-временные характеристики (далее – ВВХ) комплексного информационного воздействия с использованием метода топологического преобразования стохастических сетей (далее – ТПСС) [2; 3].

Для определения ВВХ с использованием метода ТПСС на первом этапе необходимо произвести четкое разложение процесса информационного воздействия на несколько физических процессов, то есть построить профильную модель. Учитывая значения, полученные в матрице построим ее профильную и математическую модель (рис. 1).

Используя правила преобразования профильных моделей по методу ТПСС [4], получены расчетные выражения для интегральной функции распределения вероятности и среднего времени реализации воздействия:

$$F(t) = \sum_{k=1}^{10} \frac{b \cdot P_I \cdot n \cdot P_{II} \cdot c \cdot P_{III} \cdot p \cdot P_{IV} \cdot m \cdot P_V \cdot l \cdot P_{VI} \cdot (z + s_k)^6}{\varphi'(s_k)} \cdot \frac{1 - \exp[-s_k t]}{-s_k}$$

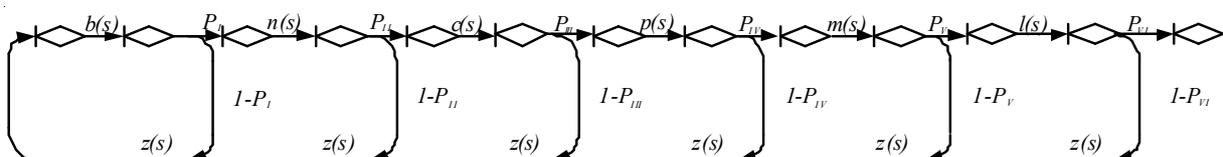


Рис. 1. Стохастическая сеть воздействия на ИТКС

$$\bar{t}_B = \sum_{k=1}^{10} \frac{b \cdot P_1 \cdot n \cdot P_{II} \cdot c \cdot P_{III} \cdot p \cdot P_{IV} \cdot m \cdot P_V \cdot l \cdot P_{VI} \cdot (z + s_k)^6}{\varphi'(s_k) \cdot \frac{1}{(-s_k)^2}}$$

Результаты расчетов ВВХ представлены на рисунке 2. В качестве исходных данных используются следующие значения: $\bar{t}_A = 29$ мин; $\bar{t}_B = 29$ мин; $\bar{t}_C = 170$ мин; $\bar{t}_D = 14$ мин; $\bar{t}_E = 120$ мин; $\bar{t}_F = 5$ мин; $\bar{t}_{\text{повт.}} = 1$ мин, $P_I = 0,8$; $P_{II} = 0,64$; $P_{III} = 0,64$; $P_{IV} = 0,53$; $P_V = 0,36$; $P_{VI} = 0,35$.

Полученные зависимости позволяют оценить влияние вероятности воздействия на значения функции распределения времени реализации применения средств воздействия на ИТКС, то есть вероятность того, что в произвольный момент времени сеть окажется неработоспособной.

Таким образом, представленный подход позволяет определить очередность и вид воздействия на каждый элемент ИТКС, что позволит оценить комплексный показатель устойчивости сети (коэффициент простоя или исправного действия).

СПИСОК ЛИТЕРАТУРЫ

1. Берзин, Е. А. Оптимальное распределение ресурсов и элементы синтеза систем / Е. А. Берзин. – М. : Советское радио, 1974. – 304 с.
2. Методика обоснования мер противодействия инфракрасной разведке высокоточного оружия / М. А. Коцыняк, В. В. Карганов, А. П. Нечепуренко, О. С. Лаута // Высшая школа. – 2016. – № 10. – С. 125–127.
3. Методика обоснования мер противодействия фото (телевизионной) разведке высокоточного оружия / М. А. Коцыняк, В. В. Карганов, А. П. Нечепуренко, О. С. Лаута // Материалы конференций ГНИИ «Нацразвитие»: сб. избр. ст. – СПб., 2016. – С. 13–20.
4. Привалов, А. А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ / А. А. Привалов. – СПб. : ВМА, 2000. – 240 с.

REFERENCES

1. Berzin E.A. *Optimalnoe raspredelenie resursov i elementy sinteza sistem* [The Optimal Allocation of Resources and Elements of Systems' Synthesis]. Moscow, Sovetskoe radio Publ., 1974. 304 p.

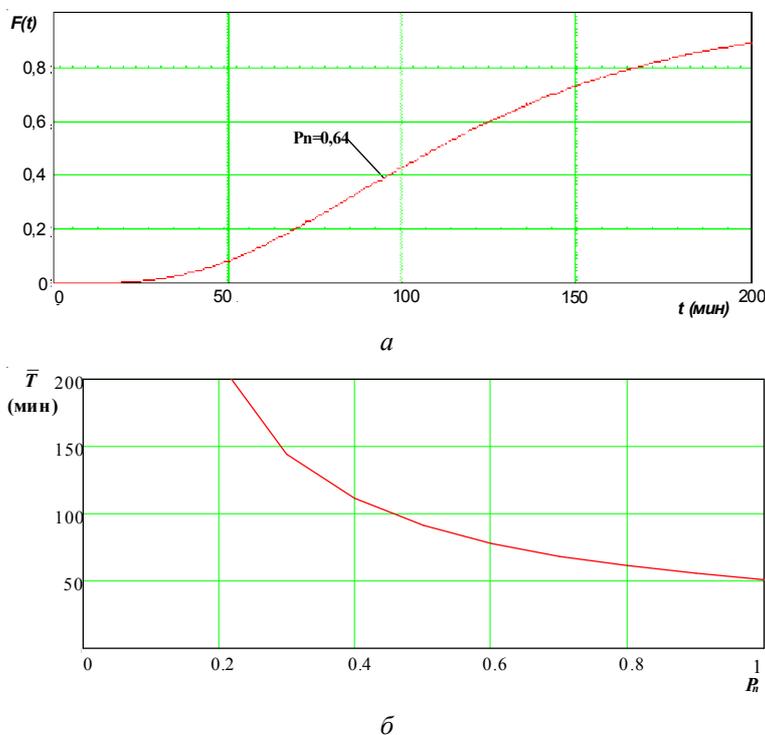


Рис. 2. Вероятностно-временные характеристики системы воздействия противника:
 а – зависимость интегральной функции распределения вероятности от времени;
 б – зависимость среднего времени реализации воздействия от вероятности воздействия

2. Kotsynyak M.A., Karganov V.V., Nechepurenko A.P., Lauta O.S. Metodika obosnovaniya mer protivodeystviya infrakrasnoy razvedke vysokotochnogo oruzhiya [The Methods of Substantiation of Measures of Counteraction to Infrared Reconnaissance of High-Precision Weapons]. *Vysshaya shkola*, 2016, no. 8, pp. 125-127.

3. Kotsynyak M.A., Karganov V.V., Nechepurenko A.P., Lauta O.S. Metodika obosnovaniya mer protivodeystviya foto (televizionnoy) razvedke vysokotochnogo oruzhiya [The Methods of Substantiation of Measures of

Counteraction to Photo (Video) Reconnaissance of High-Precision Weapons]. *Materialy konferentsiy GNI «Natsrazvitie»: sb. izbr. st.* [Proceedings of Conferences ‘National Development’: Collection of Selected Articles]. Saint Petersburg, 2016, pp. 13-20.

4. Privalov A.A. *Metod topologicheskogo preobrazovaniya stokhasticheskikh setey i ego ispolzovanie dlya analiza sistem svyazi VMF* [The Method of Topological Transformation of Stochastic Networks and Its Use for the Analysis of Communication Systems of the Navy]. Saint Petersburg, VMA Publ., 2000. 240 p.

THE METHODS OF ASSESSING THE SUSTAINABILITY OF INFORMATION AND TELECOMMUNICATION NETWORKS IN TERMS OF INFORMATIONAL INFLUENCE

Mikhail A. Kotsynyak

Doctor of Military Sciences, Professor,
Military Academy of Communication named after Marshal of the Soviet Union S.M. Budyonny
kot-c@yandex.ru
Prosp. Tikhoretskiy, 6, 194064 Saint Petersburg, Russian Federation

Aleksandr P. Nechepurenko

Postgraduate Student,
Military Academy of Communication named after Marshal of the Soviet Union S.M. Budyonny
brother-aks@yandex.ru
Prosp. Tikhoretskiy, 6, 194064 Saint Petersburg, Russian Federation

Valeriy M. Moskovchenko

Doctor of Sciences (Economics), Professor, Department of Information Security,
South-Russian State Polytechnic University (NPI) named after M.I. Platov
fvo.urgpu.npi@yandex.ru
Prosveshcheniya St., 132, 346428 Novocherkassk, Russian Federation

Abstract. The article presents a method of assessing the stability of the information and telecommunication network in terms of informational impact.

In modern war, the primary objects of directed counteraction and defeat are presented with control systems rather than troops and weapons. The predicted nature of the enemy’s impact on the military control system and the information and telecommunication network as its technical basis leads to the emergence of new requirements for the quality of the latter.

The presented approach allows us to determine the order and type of impact on each element of the TCS, which in turn will allow us to assess the comprehensive indicator of the stability of the network (the coefficient of downtime or serviceable action).

Key words: information and telecommunication network, informational impact, sustainability of the network, idle factor, comprehensive indicator.