www.volsu.ru

DOI: https://doi.org/10.15688/jvolsu10.2017.2.2

УДК 004.056
ББК 32.81

МЕТОДИКА ОЦЕНКИ УСТОЙЧИВОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ

Владимир Витальевич Баранов

Кандидат военных наук, доцент,
заведующий кафедрой информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) им. М.И. Платова
fvo.urgpu.npi@yandex.ru
ул. Просвещения, 132, 346400 г. Новочеркасск, Российская Федерация

Михаил Антонович Коцыняк

Доктор технических наук, профессор 32-й кафедры,
Военная академия связи им. С.М. Буденного
vas@mail.ru
просп. Тихорецкий, 3, К-64, 194064 г. Санкт-Петербург, Российская Федерация

Олег Сергеевич Лаута

Преподаватель 32-й кафедры,
Военная академия связи им. С.М. Буденного
vas@mail.ru
просп. Тихорецкий, 3, К-64, 194064 г. Санкт-Петербург, Российская Федерация

Валерий Михайлович Московченко

Кандидат военных наук, доктор экономических наук, профессор,
проректор по военному образованию и делам казачества,
Южно-Российский государственный политехнический университет (НПИ) им. М.И. Платова
fvo.urgpu.npi@yandex.ru
ул. Просвещения, 132, 346400 г. Новочеркасск, Российская Федерация

Аннотация. В статье описывается методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия. Разработанная методика позволяет оценить влияние вероятности воздействия на значения функции распределения времени реализации применения средств воздействия на информационно-телекоммуникационную сеть, то есть вероятность того, что в произвольный момент времени сеть окажется неработоспособной, или, иначе говоря, коэффициент простоя.

Ключевые слова: информационно-коммуникационная сеть, информационная безопасность, сеть общего пользования, компьютерная атака, стохастическая сеть.

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 обусловливает появление новых требований к показателям качества функционирования ИТКС.

Использование в ИТКС технологий, средств связи и программного обеспечения иностранного производства, интеграция ИТКС с сетью связи общего пользования (далее – ССОП), а ССОП – с мировым информационным пространством предопределили смещение акцентов на достижение превосходства над противником на основе применения компьютерных атак (далее – КА).

Результатом воздействия КА является блокирование управляющей информации 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 эффектом применения оружия массового поражения.

Воздействие на ИТКС путем применения противником КА приведет к существенному снижению устойчивости ИТКС и, как следствие, к 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 следующим образом: живучесть – коэффициентом исправного действия ИТКС по живучести; помехоустойчивость – коэффициентом исправного действия по помехоустойчивости; надежность оценивается коэффициентом исправного действия по надежности; киберустойчивость – коэффициентом исправного действия по киберустойчивости.

Так как перерывы связи из-за воздействия помех, ядерного оружия, КА и по технико-эксплуатационным причинам – события независимые, то устойчивость ИТКС можно оценить как произведение всех показателей составляющих устойчивости.

Анализ возможностей противника и взглядов зарубежных военных специалистов на современные способы ведения войны показывает, что существующие способы защиты ИТКС не в полной мере обеспечат 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 [1–3]. Полученные в матрице назначения значения 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 (ТПСС) (рис. 1).

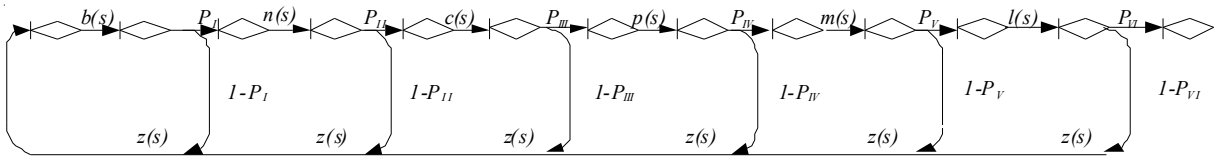

Рис. 1. Стохастическая сеть воздействия на ИТКС

С целью 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.

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

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

$$\overline{t_B}=\sum_{k=1}^{10}\frac{b\cdot P_{\text{I}}\cdot n\cdot P_{\text{II}}\cdot c\cdot P_{\text{III}}\cdot p\cdot P_{\text{IV}}\cdot m\cdot P_{\text{V}}\cdot l\cdot P_{\text{VI}}\cdot(z+s_k)^6}{\varphi'(s_k)}\cdot\frac{1}{(-s_k)^2}.$$

Результаты расчетов ВВХ представлены на рисунке 2. В качестве исходных данных используются следующие значения:

$\overline{t_A}=29$ мин, $\overline{t_B}=29$ мин, $\overline{t_C}=170$ мин, $\overline{t_D}=14$ мин, $\overline{t_E}=120$ мин, $\overline{t_F}=5$ мин, $\overline{t_{\text{ПОВТ}}}=1$ мин, $P_{\text{I}}=0{,}8$, $P_{\text{II}}=0{,}64$, $P_{\text{III}}=0{,}64$, $P_{\text{IV}}=0{,}53$, $P_{\text{V}}=0{,}36$, $P_{\text{VI}}=0{,}35$.

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, или, иначе говоря, коэффициент простоя.

Таким образом, представленный подход позволяет определить очередность и вид воздействия на каждый элемент ИТКС, что в свою очередь 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. Нечепу-

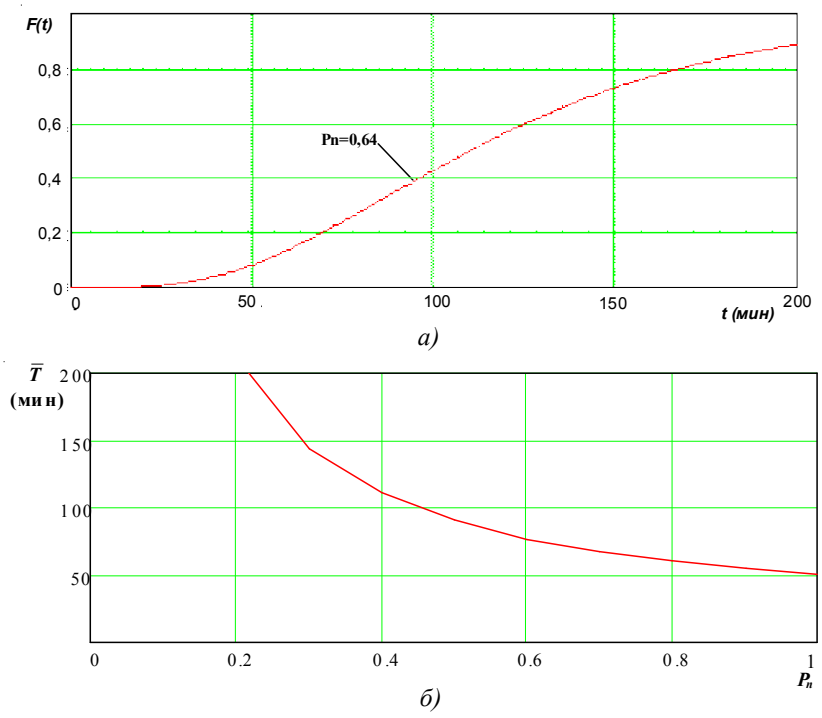

Рис. 2. Вероятностно-временные характеристики системы воздействия противника:

а – зависимость интегральной функции распределения вероятности от времени;

б – зависимость среднего времени реализации воздействия от вероятности воздействия

ренко, О. С. Лаута // Высшая школа. – 2016. – № 8. – С. 125–127.

3. Методика обоснования мер противодействия фото (телевизионной) разведке высокоточного оружия : материалы конференций ГНИИ «Нацразвитие» : сб. избр. ст. / М. А. Коцыняк, В. В. Карганов, А. П. Нечепуренко, О. С. Лаута. – 2016. – С. 13–20.

4. Привалов, А. А. Метод топологического преобразования стохастических сетей и его использование для анализа связи ВМФ / А. А. Привалов. – СПб. : ВМА, 2000. – 240 с.

REFERENCES

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

2. Kotsynyak M.A., Karganov V.V., Nechepurenko A.P., Lauta O.S. Metodika obosnovaniya mer protivodeystviya infrakrasnoy razvedke vysokotochnogo oruzhiya [Methods of Justification of Countermeasures to Infrared Intelligence 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 [Methods of Justification of Countermeasures to Photo (Television) Intelligence Precision Weapons]. *Materialy konferentsiy GNII «Natsrazvitie»: sb. izbr. st.* [Proceedings of the Conference GNII "National Development": Collection of Selected Articles], 2016, pp. 13-20.

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

ASSESSMENT OF INFORMATION AND TELECOMMUNICATION NETWORKS STABILITY IN TERMS OF INFORMATIONAL INFLUENCE

Vladimir Vitalyevich Baranov

Candidate of Military Sciences, Associate Professor, Head of the Department of Information Security,
South-Russian State Polytechnic University named after M.I. Platov
fvo.urgpu.npi@yandex.ru
Prosveshcheniya St., 132, 346400 Novocherkassk, Russian Federation

Mikhail Antonovich Kotsynyak

Doctor of Technical Sciences, Professor, Department 32,
Military Academy of Communications named after S.M. Budenny
vas@mil.ru
Prosp. Tikhoretskiy, 3, K-64, 194064 Saint Petersburg, Russian Federation

Oleg Sergeevich Lauta

Lecturer, Department 32,
Military Academy of Communications named after S.M. Budenny
vas@mil.ru
Prosp. Tikhoretskiy, 3, K-64, 194064 Saint Petersburg, Russian Federation

Valeriy Mikhaylovich Moskovchenko

Candidate of Military Sciences, Doctor of Economic Sciences, Professor,
Vice-Rector for Military Education and the Cossacks,
South-Russian State Polytechnic University named after M.I. Platov
fvo.urgpu.npi@yandex.ru
Prosveshcheniya St., 132, 346400 Novocherkassk, Russian Federation

Abstract. The article describes the methodology of assessing telecommunication networks stability in terms of informational influence.

In modern warfare conditions, the systems of monitoring the enemy are primary objects of combat along with troops and weapons. The projected impact of the enemy on the military administration and information-telecommunications network as its technical foundation, introduces new requirements for indicators of quality of functioning.

The use of foreign technologies, communications and software in telecommunications network determined the shift of emphasis on achieving superiority over the enemy through the use of computer attacks.

The result of the impact of computer attacks is blocking management information and the introduction of false information, violation of the established regulations for the collection, processing and transfer of information, equipment failures, failures in the information and telecommunications network, as well as the compromise of transmitted (received) information. According to foreign experts, the impact of computer attack is comparable to the effect of the use of weapons of mass destruction.

The developed method allows assessing the influence of probability impact on the function of distributing time of applying means of impact on information and telecommunication network, i.e. the probability that at any moment the network will be inoperable.

Key words: information and communication network, information security, public network, computer attack, stochastic network.