www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.4.2

УДК 621.322
ББК 32.973

ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ ПРОТОКОЛЬНОЙ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Владислав Евгеньевич Дементьев

Кандидат технических наук, докторант кафедры тридцать два,
Военная академия связи им. Маршала Советского Союза С.М. Буденного
dem-vlad@rambler.ru
Тихорецкий просп., 6, 194064 г. Санкт-Петербург, Российская Федерация

Олег Сергеевич Лаута

Кандидат технических наук, преподаватель,
Военная академия связи им. Маршала Советского Союза С.М. Буденного
laos-82@yandex.ru
Тихорецкий просп., 6, 194064 г. Санкт-Петербург, Российская Федерация

Владимир Витальевич Баранов

Кандидат военных наук, доцент, заведующий кафедрой информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) им. М.И. Платова
baranov.vv.2015@yandex.ru
ул. Просвещения, 132, 346428 г. Новочеркасск, Российская Федерация

Александр Сергеевич Максимов

Студент кафедры информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) им. М.И. Платова
ул. Просвещения, 132, 346428 г. Новочеркасск, Российская Федерация

Аннотация. В современных условиях увеличивается количество воздействий, направленных непосредственно на протоколы обмена данными и информационного обмена. Задача расчета критерия эффективности может быть решена методом статистического моделирования функционирования системы протокольной защиты информационно-телекоммуникационной сети. Рассчитанный критерий используется при проверке соответствия реальной системы заданным тактико-техническим требованиям или при сравнительной оценке проектов различных вариантов системы протокольной защиты данной сети.

Ключевые слова: информационно-телекоммуникационная сеть, информационный обмен, протоколы обмена данными, система протокольной защиты, статистическое моделирование.

В современных условиях увеличивается количество воздействий, направленных непосредственно на протоколы обмена данными и информационного обмена. Особую актуальность приобретает способность информационно-телекоммуникационной сети (далее – ИТКС) поддерживать целевые показатели функционирования на требуемом уровне, а также способность системы ее защиты обеспечивать необходимую эффективность противодействия. В связи с этим увеличивается важность проведения исследований в указанном направлении и разработки адекватных подходов к защите и оценке их эффективности. Данному вопросу и посвящена настоящая статья, в которой предлагается подход к оценке разработанной системы защиты от протокольных воздействий (далее – ПВ) на ИТКС [1; 2; 6].

Поток ПВ на ИТКС будет простейшим из-за следующих особенностей.

Во-первых, он обладает свойством стационарности, то есть в определенный интервал времени количество ПВ зависит от выбранной стратегии воздействия и не зависит от времени, в течение которого это воздействие осуществляется.

Во-вторых, поток ПВ обладает свойством ординарности, поскольку за интервал времени Δt может быть выполнено только одно ПВ на один протокол.

В-третьих, стратегия ПВ управляется автоматизированной системой воздействия, то есть поток ПВ обладает отсутствием последействия, а попадание каждого ПВ не зависит от результатов предыдущего.

Таким образом, поток ПВ на ИТКС достаточно точно описывается законом распределения Пуассона. В дальнейшем будем полагать, что поступающий поток ПВ и процесс противодействия им являются пуассоновскими, то есть интервалы между поступлениями ПВ взаимно независимы и распределены по показательному закону.

Под эффективностью системы протокольной защиты (далее – СПЗ) ИТКС будем понимать степень ее приспособленности к выполнению возложенных на нее задач [2]. Основной особенностью таких систем является то, что при выходе из строя отдельных элементов система не выходит из строя полностью, а продолжает выполнять возложенные на нее функции в несколько меньшем объеме. Поэтому для количественной оценки эффективности таких систем используется некий обобщенный показатель, называемый критерием эффективности – $K_э$. Этот критерий характеризует некоторый средний успех, который достигается в результате функционирования системы.

В соответствии с данной особенностью для оценки эффективности СПЗ ИТКС предлагается использовать следующую методику [3–5].

1-й этап – подготовительный – анализ назначения, задач и условий функционирования ИТКС. На этом этапе конкретизируется назначение и задачи ИТКС с учетом особенностей выполнения технологического цикла.

2-й этап – выбор критерия эффективности. Для ИТКС наиболее целесообразным критерием эффективности можно рассматривать математическое ожидание числа функционирующих в ИТКС протоколов в заданное время:

$$K_э = M[S], \qquad (1)$$

где S – число протоколов, функционирующих в ИТКС в течение заданного времени Δt.

3-й этап – составление структурно-функциональной схемы и расчет надежностных показателей протоколов ИТКС. ИТКС представляется как набор протоколов, которые могут находиться в одном из двух возможных состояний – «работа» и «отказ». В результате такого разбиения удается построить структурно-функциональную схему, которая воспроизводится в виде ориентированного графа и матриц.

Надежностные характеристики протоколов ИТКС задаются в виде вероятности на них в течение заданного времени Δt. Конкретные значения этих показателей получены в разделе 2 при определении стратегии воздействия на протоколы ИТКС и характера ПВ. В результате получаем последовательность вероятностей p_k (k = 1, 2, ..., S). Здесь p_k – вероятность воздействия на k-й протокол, а S – общее число протоколов ИТКС.

4-й этап – определение возможных состояний ИТКС и показателей эффективности каждого состояния. Если ИТКС включает S протоколов, а каждый из них может находиться в одном из двух возможных состоя-

ний, то общее число всех возможных состояний системы будет равно:

$$N = 2^s, \quad (2)$$

Если обозначить через X_r – состояние, при котором первые r протоколов системы находятся в состоянии «работа», а остальные m-r протоколов – в состоянии отказа, то вероятность такого состояния определиться по формуле:

$$P(X_r) = \prod_{k=1}^{r} p_k \prod_{k=r+1}^{S} (1 - p_k). \quad (3)$$

Используя формулу (3), можно вычислить вероятности всех возможных состояний ИТКС. В каждом из них ИТКС функционирует с определенным числом протоколов. Таким образом, каждому состоянию системы x_j ($j = 1, 2, ..., N$) можно поставить в соответствие вероятность такого состояния $P(x_j)$ и количество протоколов S_j в этом состоянии.

5-й этап – расчет критерия эффективности ИТКС. Общий критерий эффективности ИТКС определяется как математическое ожидание числа протоколов, которые функционируют в течение заданного времени Δt [6]. Вероятностью перехода из одного состояния в другое в течение времени Δt пренебрегаем.

Тогда:

$$K_э = M[S] = \sum_{j=1}^{N} P(X_j) S_j. \quad (4)$$

При достаточно большом числе ПВ на ИТКС расчет становится достаточно трудным. Поэтому на практике возможно использование различных способов упрощения вычислений. Например, при симметричной структуре и одинаковых характеристиках ПВ достаточно произвести расчет для части ИТКС. При этом, как правило, исключают из рассмотрения маловероятные состояния СПЗ ИТКС.

Задача расчета критерия эффективности может быть решена методом статистического моделирования функционирования СПЗ ИТКС.

Рассчитанный критерий эффективности используется при проверке соответствия реальной системы заданным тактико-техническим требованиям или при сравнительной оценке проектов различных вариантов СПЗ ИТКС.

СПИСОК ЛИТЕРАТУРЫ

1. Берзин, Е. А. Оптимальное распределение ресурсов и элементы синтеза систем / Е. А. Березин. – М. : Советское радио, 1974. – 304 с.

2. Давыдов, Г. Б. Сети электросвязи / Г. Б. Давыдов, В. Я. Рогинский, А. Я. Гопчин. – М. : Связь, 1978. – 38 с.

3. 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.

4. 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.

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

6. Сеидов, Т. М. Автоматизированные системы управления войсками и связью / Т. М. Сеидов, А. Н. Румянцев. – М. : МО СССР, 1983. – 52 с.: ил.

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.

2. Davydov G.B., Roginskiy V.Ya., Gopchin A.Ya. *Seti elektrosvyazi* [Telecommunication Networks]. Moscow, Svyaz Publ., 1978. 38 p.

3. 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.

4. 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 GNII «Natsrazvitie»: sb. izbr. st.* [Proceedings of Conferences 'National Development': Collection of Selected Articles]. Saint Petersburg, 2016, pp. 13-20.

5. 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.

6. Seidov T.M., Rumyantsev A.N. *Avtomatizirovannye sistemy upravleniya voyskami i svyazyu* [Automated Systems of Command, Control and Communication]. Moscow, MO SSSR Publ., 1983. 52 p.: il.

THE APPROACH TO ASSESSING THE SYSTEM OF PROTOCOL PROTECTION OF INFORMATION AND TELECOMMUNICATION NETWORKS

Vladislav E. Dementyev

Candidate of Sciences (Engineering), Candidate for a Doctor's Degree, Department 32,
Military Academy of Communication named after Marshal of the Soviet Union S.M. Budyonny
dem-vlad@rambler.ru
Prosp. Tikhoretskiy, 6, 194064 Saint Petersburg, Russian Federation

Oleg S. Lauta

Candidate of Sciences (Engineering), Lecturer,
Military Academy of Communication named after Marshal of the Soviet Union S.M. Budyonny
laos-82@yandex.ru
Prosp. Tikhoretskiy, 6, 194064 Saint Petersburg, Russian Federation

Vladimir V. Baranov

Candidate of Military Sciences, Associate Professor, Head of Department of Information Security,
South-Russian State Polytechnic University (NPI) named after M.I. Platov
baranov.vv.2015@yandex.ru
Prosveshcheniya St., 132, 346428 Novocherkassk, Russian Federation

Aleksandr S. Maksimov

Student, Department of Information Security,
South-Russian State Polytechnic University (NPI) named after M.I. Platov
Prosveshcheniya St., 132, 346428 Novocherkassk, Russian Federation

Abstract. In modern conditions, the number of impacts directly on the protocols of data exchange and information exchange is increasing. Of particular relevance is the ability of the information and telecommunications network to maintain performance targets at the required level, and its protection system to ensure the necessary effectiveness of counteraction. In this regard, it is of high importance to conduct research in this direction and to develop adequate approaches to the protection and evaluation of their effectiveness. The present article is devoted to this issue, an applies the approach to the evaluation of the developed system of protection against protocol effects on the information and telecommunication networks.

The problem of calculating the criterion of efficiency can be solved by statistical modeling of the system of protocol protection of information and telecommunication networks. The calculated efficiency criterion is used to verify the compliance of the real system with the specified tactical and technical requirements or in the comparative evaluation of projects of different variants of the system of protocol protection of information and telecommunication networks.

Key words: information and telecommunication network, information exchange, data exchange protocols, protocol protection system, statistical modeling.