DOI: 10.12731/2227-930X-2018-1-69-83
УДК 004.056

МОДЕЛИРОВАНИЕ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ НА РАСПРЕДЕЛЕННЫХ ОБЪЕКТАХ УПРАВЛЕНИЯ

Карпов А.В., Лепешкин О.М.

Значительное повышение требований к безопасности функционирования распределенных объектов управления не может быть реализовано только за счет расширения и ужесточения мер контроля за безопасностью. Первым шагом в обеспечении безопасности информации на таких объектах является анализ условий их функционирования и моделирование технических каналов утечки информации. Разработка моделей таких каналов по существу является единственным методом достаточно полного исследования их возможностей, и направлена на получение количественных оценок безопасности функционирования сложных объектов. Данные оценки необходимы для принятия решения о степени защищенности информации от утечки согласно действующему критерию. Существующие модели разработаны для типовых сосредоточенных объектов и позволяют оценить степень защищенности информации от утечки по каждому из каналов в отдельности, что влечет за собой значительное увеличение требуемого защитного ресурса и времени оценки защищенности информации на объекте в целом. В статье рассматривается логико-вероятностный метод оценки безопасности структурно-сложных объектов, на примере представлена модель канала утечки информации на распределенном объекте управления, рекомендовано использовать программный комплекс автоматизированного структурно-логического моделирования сложных систем, позволяющий оценить риск утечки информации в динамике. Рассчитывается вероятность утечки информации по техническим каналам, вычисляются такие дифференциальные характеристики

безопасного функционирования распределенных объектов управления как положительные и отрицательные вклады инициирующих событий и условий, приводящих к утечке.

***Цель** – количественная оценка риска утечки информации, необходимая для обоснования рационального состава организационно-технических мер защиты, а также варианта структуры системы защиты информации от утечки по техническим каналам.*

***Метод или методология проведения работы:** в статье использовался логико-вероятностный метод структурно-логического моделирования.*

***Результаты:** получены наиболее информативные параметры, позволяющие количественно оценить риск утечки информации.*

***Область применения результатов:** полученные результаты целесообразно применять для оценки безопасности функционирования структурно-сложных объектов, в том числе распределенных объектов управления, а также для рационального распределения сил и средств защиты информации от ее утечки по техническим каналам.*

***Ключевые слова:** логико-вероятностный метод оценки безопасности; вероятность утечки информации; логическая модель; вероятностный полином; булева функция.*

MODELING OF TECHNICAL CHANNELS OF INFORMATION LEAKAGE AT DISTRIBUTED CONTROL OBJECTS

Karpov A.V., Lepeshkin O.M.

The significant increase in requirements for distributed control objects' functioning can't be realized only at the expense of the widening and strengthening of security control measures. The first step in ensuring the information security at such objects is the analysis of the conditions of their functioning and modeling of technical channels of information

leakage. The development of models of such channels is essentially the only method of complete study of their opportunities and it is pointed toward receiving quantitative assessments of the safe operation of compound objects. The evaluation data are necessary to make a decision on the degree of the information security from a leak according to the current criterion. The existing models are developed for the standard concentrated objects and allow to evaluate the level of information security from a leak on each of channels separately, what involves the significant increase in the required protective resource and time of assessment of information security on an object in general. The article deals with a logical-and-probabilistic method of a security assessment of structurally-compound objects. The model of a security leak on the distributed control objects is cited as an example. It is recommended to use a software package of an automated structurally-logistical modeling of compound systems, which allows to evaluate risk of information leakage in the loudspeaker. A possibility of information leakage by technical channels is evaluated and such differential characteristics of the safe operation of the distributed control objects as positive and negative contributions of the initiating events and conditions, which cause a leak are calculated.

***Purpose**. The aim is a quantitative assessment of data risk, which is necessary for justifying the rational composition of organizational and technical protection measures, as well as a variant of the structure of the information security system from a leak over the technical channels.*

***Methodology:** a logical-and-probabilistic method of a structurally-logistical modeling is used in the article.*

***Results:** the most informative parameters, which allow to evaluate quantitatively data risk are received.*

***Practical implications:** the results are useful to assess the operational safety of structurally-compound objects, including the distributed control objects and also to distribute rationally the protection force and means from technical channels of information leakage.*

***Keywords:** logical-and-probabilistic method of a security assessment; probability of information leakage; logical model; probabilistic polynomial; Boolean function.*

Для исследования структурно-сложных объектов, к которым относятся и распределенные объекты управления (РОУ), используется как аналитическое, так и имитационное моделирование [1]. Однако эти формы решения задач высокой размерности для таких объектов обладают недостатками, в частности, высокой трудоемкостью, трудностью обеспечения корректности и недостаточной степенью точности [13].

Одним из вариантов решения данной проблемы является применение логико-вероятностного метода структурно-логического моделирования, ориентированного на решение широкого круга задач анализа и синтеза безопасности, риска и эффективности функционирования объекта с абсолютной математической корректностью [2, с. 7].

С помощью данного метода возможна разработка модели канала утечки информации (КУИ) на РОУ. Модель используется для проектной оценки защищенности при построении типовых вариантов системы защиты информации (СЗИ) либо эксплуатационной оценки безопасности информации (БИ) при функционировании данного объекта [6, с. 187].

По аналогии с теорией надежности, где анализ начинается с определения понятия работоспособности системы, логико-вероятностный метод оценки безопасности требует определить сценарий опасного состояния (СОС) РОУ. Под опасным состоянием (ОС) данного объекта будем понимать утечку информации по техническим каналам (ТК). Аналитическое описание ОС осуществляется с помощью логической функции опасности объекта (ФОО), аргументами которой выступают инициирующие опасность события и условия (ИС и ИУ) [9, с. 1].

На типовом РОУ защите подлежит речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе. Как показывает анализ функционирования такого объекта, наиболее опасными техническими кана-

лами утечки информации (ТКУИ) на нем являются: акустический, виброакустический, утечки за счет акустоэлектрических и акустооптических преобразований, каналы побочных электромагнитных излучений и наводок (ПЭМИН) и перехват оптического сигнала с волоконно-оптических линий связи (ВОЛС) контактным способом.

На рис. 1 представлен фрагмент СОС РОУ на примере утечки информации по акустическому каналу (АК).

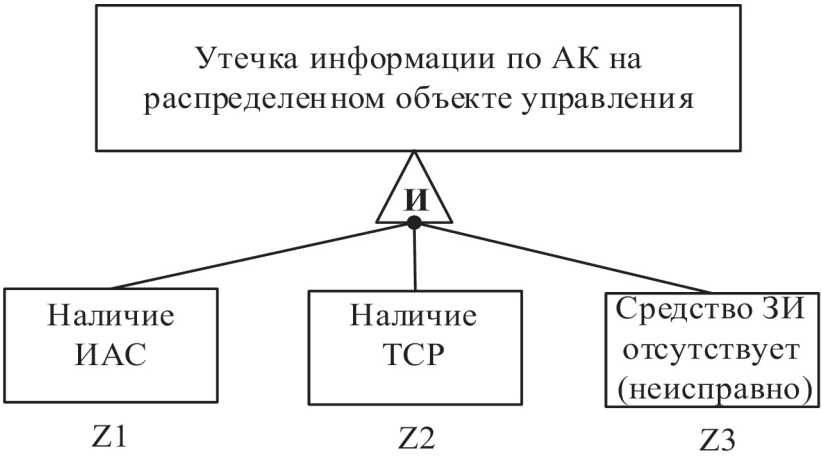

Рис. 1. Фрагмент сценария опасного состояния РОУ

Из данного рисунка видно, что утечка информации по АК произойдет, если имеют место информативный акустический сигнал (ИАС) (Z1), техническое средство разведки (ТСР) в зоне разведдоступности данного сигнала (Z2) и отсутствует (либо неисправно) средство защиты информации от утечки по АК (Z3) [3, с. 1118]. В данном случае конечное событие (опасное состояние) – утечка информации на объекте по АК, а инициирующими событиями и условиями являются соответственно Z1, Z2, Z3. Математической моделью КУИ на РОУ является логическая функция риска утечки информации (Л-функция), на основе которой строится расчётная вероятностная функция риска (В-полином). Л-функция риска утечки информации представляет собой строго математическое

описание СОС с помощью аппарата булевой алгебры [11]. Этап определения В-полинома риска утечки информации заключается в построении многочлена расчётной вероятностной функции с помощью специальных методов [15].

Л-функция риска утечки информации по ТК на РОУ в общем виде:

$$Y(Z) = \begin{vmatrix} K1 \\ K2 \\ K3 \\ K4 \\ K5 \\ K6 \end{vmatrix}. \quad (1)$$

В данном случае Л-функция риска утечки информации по АК K1(Z) имеет вид:

$$K1(Z) = Z1 \cap Z2 \cap Z3 = Z1Z2Z3, \quad (2)$$

где Z1 – наличие информативного акустического сигнала (ИАС);

Z2 – наличие ТСР акустического сигнала в зоне разведдоступности ИАС;

Z3 – средство защиты информации от утечки по АК отсутствует или неисправно.

Аналогично Л-функция риска утечки информации по виброакустическому каналу (ВАК):

$$K2(Z) = Z1 \cap Z4 \cap Z5 = Z1Z4Z5, \quad (3)$$

где Z1 – наличие ИАС (аналогично АК);

Z4 – наличие ТСР виброакустического сигнала в зоне разведдоступности ИАС;

Z5 – средство защиты информации от утечки по ВАК отсутствует или неисправно.

Л-функция риска утечки информации по каналу ПЭМИН:

$$K3(Z) = Z6 \cap Z7 \cap Z8 = Z6Z7Z8, \quad (4)$$

где Z6 – наличие опасного сигнала (побочного излучения);

Z7 – наличие ТСР сигналов ПЭМИН в зоне разведдоступности опасного сигнала;

Z8 – средство защиты информации от утечки по каналу ПЭМИН отсутствует или неисправно.

Л-функция риска утечки информации за счет акустоэлектрических преобразований (АЭП):

$$K4(Z) = Z1 \cap Z9 \cap Z10 \cap Z11 = Z1Z9Z10Z11, \quad (5)$$

где Z9 – наличие ТСР информации за счет АЭП в зоне разведдоступности ИАС;

Z10 – наличие микрофонного эффекта на РОУ;

Z11 – средство защиты информации от утечки за счет АЭП отсутствует или неисправно.

Л-функция риска утечки информации за счет акустооптических преобразований (АОП):

$$K5(Z) = Z1 \cap Z12 \cap Z13 \cap Z14 = Z1Z12Z13Z14, \quad (6)$$

где Z12 – наличие оптического сигнала в ВОЛС;

Z13 – наличие ТСР информации за счет АОП в зоне разведдоступности ИАС;

Z14 – средство защиты информации от утечки за счет АОП отсутствует или неисправно.

Л-функция риска утечки оптического сигнала с ВОЛС контактным способом:

$$K6(Z) = Z12 \cap Z15 \cap Z16 = Z12Z15Z16, \quad (7)$$

где Z15 – наличие ТСР оптического сигнала в зоне его разведдоступности;

Z16 – средство защиты оптического сигнала от утечки с ВОЛС отсутствует или неисправно.

Подставляя (2) – (7) в (1), получим:

$$Y(Z) = \begin{vmatrix} Z1Z2Z3 \\ Z1Z4Z5 \\ Z6Z7Z8 \\ Z1Z9Z10Z11 \\ Z1Z12Z13Z14 \\ Z12Z15Z16 \end{vmatrix}, \quad (8)$$

где конъюнкции стоят в строках, а знак дизъюнкции между строками;

Y(Z) – Л-функция риска утечки информации по ТК на РОУ;

Z1, Z2…Z16 – соответствующие инициирующие события и условия, приводящие к утечке информации по ТК.

Полученная Л-функция (8) представляет собой совокупность кратчайших путей опасного функционирования (КПОФ). КПОФ описывает один из вариантов утечки информации на РОУ от минимально возможного набора инициирующих событий и условий [12, с. 39]. Другими словами, существует только 6 способов организации утечки информации на данном объекте и ни одним больше.

Процесс вероятностного моделирования КУИ на РОУ заключается в построении расчетной вероятностной функции, которую будем называть В-полиномом риска.

Алгебра логики допускает непосредственный переход от логической к вероятностной функции заменой логических переменных Z_i вероятностями, а логических операций соответствующими арифметическими операциями [8, с. 69]. Данный переход возможен путем ортогонализации Л-функции, записанной в дизъюнктивной нормальной форме (ДНФ). После несложных преобразований получим ортогональную ДНФ (ОДНФ) булевой функции $Y(Z)$:

$$Y(Z) = \left[Z1Z2Z3\right) \cup \left(\overline{Z1} \cup Z1\overline{Z2} \cup Z1Z2\overline{Z3}\right)\Big] \cap \ldots$$

$$\ldots \cap \left[\left(\overline{Z1} \cup Z1\overline{Z1}2 \cup Z1Z1\,2\overline{Z1}3 \cup Z1Z1\,2Z1\,3\overline{Z1}4\right)\left(Z1\,2Z1\,5Z1\,6\right)\right], \quad (9)$$

где $Y(Z)$ – Л-функция риска утечки информации на РОУ в ОДНФ.

Ввиду громоздкости выражение (9) представляет собой фрагмент ОДНФ булевой функции $Y(Z)$. Только для ОДНФ вместо соответствующих переменных можно подставлять их вероятности, заменяя знаки дизъюнкции и конъюнкции на знаки сложения и умножения соответственно [14, с. 275]. На основании этого получим вероятностную функцию риска утечки информации:

$$B(Z) = p1p2p3 + \left[\left(q1 + p1q2 + p1p2q3\right)\right] \times \ldots$$

$$\ldots \times \left[\left(q1 + p1q12 + p1p12q13 + p1p12p13q14\right)\left(p12p15p16\right)\right], \quad (10)$$

где $B(Z)$ – вероятностная функция риска утечки информации на РОУ;

$p1$, $p2 \ldots p16$ – прямые вероятности событий $Z1$, $Z2 \ldots Z16$;

$q1$, $q2 \ldots q14$ – инверсные вероятности ($q_i = 1 - p_i$) событий $Z1$, $Z2 \ldots Z14$.

Функция (10) характеризует истинность Л-функции (8) и является обобщенным показателем защищенности информации на объекте от утечки по ТК. С помощью вероятностной функции (10) определяют вероятность утечки информации на РОУ при заданных исходных вероятностях инициирующих событий и условий, приводящих к данной утечке. Данный показатель необходим для принятия решения о состоянии защищенности информации на данном объекте в соответствии с действующим критерием [4, с. 1198].

Необходимым условием расчета вероятности истинности Л-функции является наличие исходных вероятностей ИС и ИУ, приводящих к утечке информации на РОУ. Такие данные могут генерироваться самым различным образом: на основе длительных наблюдений, по результатам статистических испытаний, путем экспертного оценивания [7].

Для распределения ресурсов и усилий по защите информации от ее утечки также необходимо знать, какое событие более значимо, а какое – менее. В системных исследованиях характеристики положительных и отрицательных вкладов в риск утечки информации на объекте играют особую и очень важную роль. Они позволяют количественно оценить, какую роль играет значение вероятности отдельных инициирующих событий и условий в реализации утечки информации на РОУ и насколько изменение этих значений может изменить обобщенный показатель защищенности (10) в целом.

Ввиду громоздкости функций (8), (10) для реализации модели используем программный комплекс автоматизированного структурно-логического моделирования сложных систем ПК АСМ 2001 [10].

После задания необходимых параметров запускается модель. Диаграмма вкладов аргументов Л-функции и значение вероятности утечки информации на РОУ представлены на рис. 2.

Рис. 2. Результаты моделирования и расчета вероятности утечки информации на РОУ

Результаты показывают, что вероятность утечки в условии дестабилизирующих факторов составляет *Pc*=0,78. Уменьшение вероятности утечки информации на РОУ в процессе эксплуатации достигается резервированием и применением дополнительных разнотипных средств защиты информации, контролем их состояния и качественным техническим обслуживанием, минимизацией времени работы источников информативных для ТСР сигналов (акустический, оптический, ПЭМИН) и ужесточением организационно-технических мер по контролю зон их разведдоступности, а также выбором рациональной периодичности и объема контролируемых параметров [5, с. 21].

Таким образом, представленный подход моделирования позволяет оценить риск утечки информации по ТК, а также обосновать рациональный вариант распределения защитного ресурса на РОУ. Подход учитывает влияние всех основных факторов и свойств, и позволяют вычислять системные характеристики безопасного функционирования структурно-сложных систем с высокой степенью точности и абсолютной математической корректностью.

Список литературы

1. Волков Д.В., Хилько В.О., Петухов А.В. Мультиагентное моделирование сети передачи данных специального назначения. В сбор-

нике: Прошлое, настоящее и будущее Российской цивилизации. Материалы всероссийской научно-практической конференции 28–29 апреля 2016 г. Ставрополь, 2016. 268 с.
2. Дурденко В.А., Рогожин А.А., Баторов Б.О. Логико-вероятностное математическое моделирование и оценка надежности системы контроля и управления доступом. Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2014. №1. С. 7–19.
3. Карпов А.В., Лепешкин О.М., Попов Н.А. Структура электромагнитного поля при нелинейной радиолокации. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1118.
4. Карпов А.В., Лепешкин О.М., Шостак Р.К. Актуальность осуществления сетевого контроля защищенности информационных сетей. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1198.
5. Князева Н.А., Грищенко И.В. Повышение живучести инфокоммуникационной сети путем структурного резервирования. Вестник ДУИКТ. 2013. №2. С. 21–25.
6. Корсунский А.С., Масленникова Т.Н., Лепешкин О.В., Чукариков А.Г., Карпов А.В. Направления развития подсистемы контроля состояния защиты информации объекта. В сборнике: Актуальные проблемы и перспективы развития радиотехнических и инфокоммуникационных систем. Сборник научных трудов III Международной научно-практической конференции. Московский технологический университет (МИРЭА). Москва, 2017. С. 187–192.
7. Котенко Д.А. Метод оценки риска информационной безопасности на основе сценарного логико-вероятностного моделирования: Автореф. дис. …канд. техн. наук. СПб.:2010. 25с.
8. Михайлов Р.Л., Макаренко С.И. Оценка устойчивости сети связи в условиях воздействия на нее дестабилизирующих факторов. Радиотехнические и телекоммуникационные системы. 2013. №4 (12). С. 69–79.
9. Можаев А.С. Технология автоматизированного структурно-логического моделирования надежности, живучести, безопасности,

эффективности и риска функционирования систем. Приборы и системы. Управление, контроль, диагностика. 2008. С. 1–14.
10. ПК АСМ-2001. Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности, живучести и безопасности систем /Автор Можаев А.С./ свидетельство об официальной регистрации №2003611099. М.: Роспатент РФ, 2001.
11. Поленин В.И., Рябинин И.А, Свирин С.К., Гладкова И.А. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства// Монография, научное издание /Под ред. А.С. Можаева// Проект в рамках Концепции социально-политического проекта РЕАН «Актуальные проблемы безопасности социума» / Российская академия естественных наук. Спб, 2011. 416 с.
12. Попков Г.В. О проблеме живучести телекоммуникационных сетей. Вестник Бурятского государственного университета. 2014. №9–3. С. 39–48.
13. Volkov D.V. Multiagent simulation modeling of special purpose communication system. International Journal of Advanced Studies, Volume 7, №1–2, 2017, 94 p.
14. Князева Н.А. Повышение структурной живучести телекоммуникационной сети. International Journal «Information Models and Analyses» vol.2/2013, number 3 pages 275–284.
15. Поленин В.И., Можаев А.С., Гладкова И.А. Общий логико-вероятностный метод моделирования сложных систем // Монография, научное издание – Германия, Саарбрюкен, Palmarium Academic Publishing, 2015. 688 p.

References

1. Volkov D.V., Khil'ko V.O., Petukhov A.V. Mul'tiagentnoe modelirovanie seti peredachi dannykh spetsial'nogo naznacheniya [Multiagent modeling of a special-purpose data network]. *Proshloe, nastoyashchee i budushchee Rossiyskoy tsivilizatsii* [The past, present and future of the Russian civilization], 2016, 268 p.
2. Durdenko V.A., Rogozhin A.A., Batorov B.O. Logiko-veroyatnostnoe matematicheskoe modelirovanie i otsenka nadezhnosti sistemy kon-

trolya i upravleniya dostupom [Logical and probabilistic mathematical modeling and assessment of the reliability of the access control system]. *Sistemnyy analiz i informatsionnye tekhnologii* [System analysis and information technology], 2014, no. 1, pp. 7–19.

3. Karpov A.V., Lepeshkin O.M., Popov N.A. Struktura elektromagnitnogo polya pri nelineynoy radiolokatsii [Structure of the electromagnetic field in nonlinear radar]. *Radiolokatsiya, navigatsiya, svyaz'* [Radar, navigation, communication], 2017, vol. 3, p. 1118.
4. Karpov A.V., Lepeshkin O.M., Shostak R.K. Aktual'nost' osushchestvleniya setevogo kontrolya zashchishchennosti informatsionnykh setey [The urgency of implementing network security monitoring of information networks]. *Radiolokatsiya, navigatsiya, svyaz'* [Radar, navigation, communication], 2017, vol. 3, p. 1198.
5. Knyazeva N.A., Grishchenko I.V. Povyshenie zhivuchesti infokommunikatsionnoy seti putem strukturnogo rezervirovaniya [Increasing the survivability of the infocommunication network through structural redundancy]. *Vestnik DUIKT* [Herald of DUICT], 2013, no. 2, pp. 21–25.
6. Korsunskiy A.S., Maslennikova T.N., Lepeshkin O.V., Chukarikov A.G., Karpov A.V. Napravleniya razvitiya podsistemy kontrolya sostoyaniya zashchity informatsii ob"ekta [Directions of development of a subsystem for monitoring the state of the information security of an object]. *Aktual'nye problemy i perspektivy razvitiya radiotekhnicheskikh i infokommunikatsionnykh system* [Actual problems and prospects of development of radio technical information systems], Moskow, 2017, pp. 187–192.
7. Kotenko D.A. *Metod otsenki riska informatsionnoy bezopasnosti na osnove stsenarnogo logiko-veroyatnostnogo modelirovaniya* [Method of assessing the risk of information security based on scenario-based logic-probabilistic modeling]. Saint-Petersburg, 2010. 25 p.
8. Mikhaylov R.L., Makarenko S.I. Otsenka ustoychivosti seti svyazi v usloviyakh vozdeystviya na nee destabiliziruyushchikh faktorov [Estimation of the stability of the communication network under the influence of destabilizing factors on it]. *Radiotekhnicheskie i telekommunikatsionnye sistemy* [Radio engineering and telecommunication systems], 2013, vol. 4, no. 12, pp. 69–79.

9. Mozhaev A.S. Tekhnologiya avtomatizirovannogo strukturno-logicheskogo modelirovaniya nadezhnosti, zhivuchesti, bezopasnosti, effektivnosti i riska funktsionirovaniya system [Technology of automated structural-logical modeling of reliability, survivability, safety, efficiency and risk of the functioning of systems]. *Pribory i sistemy. Upravlenie, kontrol', diagnostika* [Devices and systems. Management, control, diagnostics], Saint-Petersburg, 2008, pp. 1–14.
10. Mozhaev A.S. *PK ASM-2001. Programmnyy kompleks avtomatizirovannogo strukturno-logicheskogo modelirovaniya i rascheta nadezhnosti, zhivuchesti i bezopasnosti sistem* [Software complex of automated structural-logical modeling and calculation of reliability, survivability and safety of systems]. *Svidetel'stvo ob ofitsial'noy registratsii №2003611099. Rospatent RF* [Certificate of official registration №2003611099. Rospatent of the Russian Federation]. Moskow, 2001.
11. Polenin V.I., Ryabinin I.A., Svirin S.K., Gladkova I.A. *Primenenie obshchego logiko-veroyatnostnogo metoda dlya analiza tekhnicheskikh, voennykh organizatsionno-funktsional'nykh sistem i vooruzhennogo protivoborstva* [Software complex of automated structural-logical modeling and calculation of reliability, survivability and safety of systems]. *Aktual'nye problemy bezopasnosti sotsiuma* [Actual problems of social security]. Saint-Petersburg: RAEN Publ., 2011. 416 p.
12. Popkov G.V. O probleme zhivuchesti telekommunikatsionnykh setey [On the problem of the survivability of telecommunications networks]. *Vestnik Buryatskogo gosudarstvennogo universiteta* [Bulletin of the Buryat State University], 2014, vol. 9, no. 3, pp. 39-48.
13. Volkov D.V. Multiagent simulation modeling of special purpose communication system. *International Journal of Advanced Studies*, 2017, vol. 7, no.1–2, 94 p.
14. Knyazeva N.A. Povyshenie strukturnoy zhivuchesti telekommunikatsionnoy seti [Increase in the structural survivability of the telecommunications network]. *International Journal «Information Models and Analyses»*, 2013, vol. 2, no. 3, pp. 275–284.
15. Polenin V.I., Mozhaev A.S., Gladkova I.A. *Obshchiy logiko-veroyatnostnyy metod modelirovaniya slozhnykh system* [General logic-probabilistic method for modeling complex systems]. Germany Publ., 2015. 688 p.

ДАННЫЕ ОБ АВТОРАХ

Карпов Александр Владимирович, адъюнкт кафедры «Безопасность инфокоммуникационных систем специального назначения»
Военная академия связи имени С.М. Буденного
пр-т Тихорецкий, 3, г. Санкт-Петербург, 194064, Российская Федерация
a.kar1986@yandex.ru

Лепешкин Олег Михайлович, старший преподаватель кафедры «Безопасность инфокоммуникационных систем специального назначения», доктор технических наук, доцент
Военная академия связи имени С.М. Буденного
пр-т Тихорецкий, 3, г. Санкт-Петербург, 194064, Российская Федерация
a.kar1986@yandex.ru

DATA ABOUT THE AUTHORS

Karpov Aleksander Vladimirovich, adjunct (graduate student) of the department “Security of infocommunication systems of a special purpose”
Military academy of communications named after Marshal of the Soviet Union S.M. Budenny
3, Tihoreckii’ av., Saint-Petersburg, 194064, Russian Federation
a.kar1986@yandex.ru

Lepeshkin Oleg Mikhailovich, senior lecturer of the department “Security of infocommunication systems of a special purpose”, Doctor of Technical Sciences, Associate Professor
Military academy of communications named after Marshal of the Soviet Union S.M. Budenny
3, Tihoreckii’av., Saint-Petersburg, 194064, Russian Federation
a.kar1986@yandex.ru