

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004. 056

DOI: 10.21822/2073-6185-2024-51-1-46-60



Оригинальная статья/Original article

Методы оценивания связности неориентированного двухполюсного помеченного графа с учетом деструктивного воздействия внешних угроз на его вершины

В.А. Воеводин, Н.А. Крахотин

Национальный исследовательский университет
«Московский институт электронной техники»,
124498, г. Москва, г. Зеленоград, пл. Шокина, 1, Россия

Резюме. Цель. Обсуждаются основные аргументы, позиционирующие задачу оценивания связности двухполюсного графа применительно к условиям деструктивного воздействия внешних угроз, как актуальную для оценивания живучести информационных систем (ИС), функционирующих в условиях угроз информационной безопасности. **Метод.** Приводятся: постановка задачи оценивания связности для условий воздействия угроз; краткий обзор существующих методов структурного моделирования двухполюсных структур; итоги анализа применимости существующих методов для оценивания устойчивости функционирования (устойчивости) двухполюсных структур применительно к условиям воздействия угроз. Приняты исходные условия: устойчивость информационной системы в целом детерминировано зависит от устойчивости ее структурных элементов и самой сетевой структуры; задача оценивания связности двухполюсной структуры является базовой для оценивания связности соответствующих многополюсных структур; анализ устойчивости объекта воздействия проводится в минимаксных критериях, а результат представляется в виде минимального значения функции устойчивости и момента времени наступления этого события. **Результат.** Выявлены ограничивающие факторы, препятствующее применению существующих методов для решения поставленной задачи. Суть основного ограничивающего фактора заключается в том, что в основе существующих методов лежат вероятностные стационарные модели, которые требуют репрезентативной статистики. Вторым, не менее важным ограничивающим фактором, является, то, что обстановка, характеризующая воздействие угроз, является весьма динамичной (не стационарна), сами события весьма редки, а период оценивания соизмерим с периодом реагирования на угрозы, что не позволяет получить эффективные оценки устойчивости. Предлагается: обобщить существующие методы для условий нестационарности процесса функционирования для чего при оценивании учитывать изменения вероятностных характеристик узловых элементов во времени. В качестве показателя, характеризующего связность, использовать минимальное значение функции устойчивости, определенной на периоде воздействия угроз. Платой за обеспечение устойчивости функционирования объекта воздействия в условиях воздействия угроз является необходимость обеспечения структурной избыточности. **Вывод.** Результаты исследования могут быть востребованы лицами, осуществляющими моделирование как самого объекта воздействия, так и процессов его функционирования, для принятия решения по обеспечению непрерывности производственных процессов в условиях воздействия угроз.

Ключевые слова: устойчивость функционирования, функция устойчивости, двухполюсная структура, угрозы информационной безопасности, структурное моделирование, методы оценивания связности, неориентированный граф, помеченный граф

Для цитирования: В.А. Воеводин, Н.А. Крахотин. Методы оценивания связности неориентированного двухполюсного помеченного графа с учетом деструктивного воздействия внешних угроз на его вершины. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(1):46-60. DOI:10.21822/2073-6185-2024-51-1-46-60

Methods for assessing the connectivity of an undirected bipolar labeled graph taking into account the destructive impact of external threats on its vertices

V.A. Voevodin, N.A. Krahotin

National Research University of Electronic Technology,
1 Shokina Square, Moscow, Zelenograd 124498, Russia

Abstract. Objective. The main arguments that position the problem of assessing the connectivity of the bipolar graph in relation to the conditions of destructive impact of external threats (threats) as relevant for assessing the vitality of information systems (IS) are discussed operating under conditions of information security threats. **Method.** The following are presented: formulation of the problem of assessing connectivity for conditions of exposure to threats; a brief overview of existing methods for structural modeling of bipolar structures; results of the analysis of the applicability of existing methods for assessing the stability of functioning (stability) of bipolar structures in relation to conditions of exposure to threats. The initial conditions are accepted: the stability of the information system as a whole depends deterministically on the stability of its structural elements and the network structure itself; the problem of assessing the connectivity of a two-pole structure is basic for assessing the connectivity of the corresponding multi-pole structures; the stability analysis of the impacted object is carried out using minimax criteria, and the result is presented in the form of the minimum value of the stability function and the moment in time of the occurrence of this event. **Result.** Limiting factors that prevent the use of existing methods to solve the problem have been identified. The main limiting factor is that existing methods are based on probabilistic stationary models that require representative statistics. The second, no less important limiting factor is that the situation characterizing the impact of threats is very dynamic (not stationary), the events themselves are very rare, and the assessment period is comparable to the period of response to threats, which does not allow obtaining effective assessments of sustainability. It is proposed to: generalize existing methods for conditions of non-stationary functioning process, for which, when assessing, take into account changes in the probabilistic characteristics of nodal elements over time; as an indicator characterizing connectivity, use the minimum value of the stability function determined during the period of exposure to threats. The price to pay for ensuring the sustainability of the functioning of the affected object under the influence of threats is the need to ensure structural redundancy. **Conclusion.** The results of the study can be used by persons who simulate both the object of impact and the processes of its functioning, to make a decision on ensuring the continuity of production processes under the conditions of the impact of threats.

Keywords: Stability of functioning, stability function, bipolar structure, threats to information security, structural modeling, connectivity evaluation methods, undirected graph, labeled graph

For citation: V.A. Voevodin, N.A. Krahotin. Methods for assessing the connectivity of an undirected bipolar labeled graph taking into account the destructive impact of external threats on its vertices. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(1): 46-60. DOI:10.21822/2073-6185-2024-51-1-46-60

Введение. В силу требований законодательства различных юрисдикций обладатель информации обязан, в том числе: принимать меры по защите информации (ЗИ) и недопущению воздействия угроз информационной безопасности (угроз) на технические средства обработки информации, в результате которого нарушается их функционирование; обеспечить постоянный контроль над уровнем защищенности информации. Эти требования усиливаются для значимых объектов критической информационной инфраструктуры (объект воздействия) и проявляются в необходимости обеспечения устойчивости их функционирования в условиях воздействия угроз. Для управления этим процессом требуется соответствующий методический инструмент оценивания устойчивости функционирования объекта воздействия в условиях воздействия угроз.

Такой методический инструмент может быть востребован: органами управления информационной безопасностью (ИБ) при задании требований к устойчивости функционирования отдельных элементов объекта воздействия и объекта воздействия в целом; лицами, управляющими программами аудита информационной безопасности (ИБ), при формировании критериев аудита, а также при разработке программ и методик аудиторских испытаний; лицами, проводящими оценку рисков информационной безопасности ИБ с целью обоснования страховых тарифов [1]; лицами, управляющими рисками ИБ [2]; лицами, принимающими решение по обеспечению непрерывности бизнеса в условиях воздействия угроз.

Генезис понятия «устойчивость функционирования» и сопутствующих ему понятий приведены в [3]. При этом устойчивость функционирования (устойчивость) определяется как специальное свойство объекта воздействия, характеризующее его способность «выдерживать» внешние воздействия. Такими воздействиями могут быть природные воздействия (землетрясения, ураганы, наводнения) или враждебные действия противника (физические повреждения элементов объекта воздействия, компьютерные атаки), которые в совокупности позиционируются как угрозы.

Порядок моделирования и оценки актуальности угроз и возможные сценарии их реализации в информационных системах приводятся в методическом документе [4]. Результаты моделирования сценариев реализации угроз на основе описания шаблонов компьютерных атак и методические рекомендации по оцениванию актуальности угроз с учетом методики приводятся в [5]. Эти результаты служат исходными данными при моделировании процессов функционирования объекта воздействия в условиях угроз.

Предмет публикации в основном ориентирован на обеспечение безопасности значимых объектов критической информационной инфраструктуры, это обусловлено, прежде всего тем, что в силу закона принят руководящий принцип предотвращения компьютерных атак. Это утверждение не распространяется как обязательное на объекты, которые не входят в эту категорию и решение добровольно принимают, либо обладатель информации, либо оператор соответствующей информационной системы.

Исходные данные, необходимые для оценивания устойчивости, добываются в результате аудита информационной безопасности. Общие вопросы организации и проведения аудита систем управления информационной безопасностью для штатных условий рассмотрены достаточно глубоко и приведены в национальных стандартах [6, 7]. Общие вопросы оценивания устойчивости функционирования в штатных условиях применения объекта воздействия приведены в работах [8, 9]. Однако эти методы базируются на математической статистике, теории вероятностей, теории надежности технических систем [11, 13, 15, 16] и не могут быть применены без ограничений для условий воздействия угроз. Данное ограничение связано прежде всего с тем, что сами события нельзя, без грубых допущений, отнести к массовым, а их потоки позиционировать как стационарные и эргодические.

Таким образом, для оценивания устойчивости ИС, функционирующей в условиях угроз, требуется специальный методический инструмент. Для построения такого инструмента принимается аксиома, что устойчивость функционирования ИС, при заданных характеристиках воздействия угроз, находится в зависимости от устойчивости функционирования отдельных элементов, входящих в его состав, и от самой структуры ИС, объединяющей отдельные элементы в систему. Возможные характеристики угроз приведены в существующем банке данных угроз, которые могут быть конкретизированы с помощью экспертных методов [17, 18]. Методы оценивания устойчивости функционирования отдельных элементов ИС, функционирующих в условиях воздействия угроз, приведены в [19 - 23].

На практике для оценивания устойчивости функционирования объекта воздействия применяют методы: словесного описания (вербальные модели); графические методы (структурная схема ИС); аналитические методы (математические модели). Вербальные и графические методы нашли широкое применение для предварительного оценивания обстановки и

уяснения задачи оценивания, а также для получения информации о логике возникновения повреждений объекта воздействия в целом.

Для получения количественной оценки, характеризующей устойчивость функционирования объекта воздействия, на практике используются соответствующие аналитические модели, характеризующие его структуру. С помощью таких аналитических моделей возможно получить функциональную зависимость между устойчивостью функционирования отдельных элементов и устойчивостью объекта воздействия в целом.

На практике информационную структуру можно представить в виде 1–1, 1–N, N–N полюсников. Такие аналитические модели характерны для многосвязных информационных систем с несколькими источниками информационного обмена, при заданных характеристиках устойчивости ее элементов. Принимается утверждение, что объект воздействия считается функциональным (способным выполнять требуемый функционал) при наличии хотя бы одного пути для обмена информацией между его полюсами.

Постановка задачи. В настоящей статье обзор методов оценивания устойчивости сосредоточен на оценивании связности 1–1 (двухполюсной) структуры. Задача оценивания связности 1–N и N–N полюсных структур может быть сведена к совокупности задачи оценивания связности двухполюсных структур, поэтому основные усилия при исследовании были сосредоточены на двухполюсной структуре. Дополнительно в [3] предлагается анализ живучести объекта воздействия осуществлять не в вероятностных, а минимаксных показателях и сводить его к исследованию «узких мест», или «минимальных значений функции живучести. Мерой живучести в [22, 23] предлагается использовать показатель мощности множества элементов, разрушение которых приводит к потере функциональности ИС. В этом случае показателем живучести объекта воздействия авторы предлагают использовать минимальное

подмножество, X^* , такое, что:
$$X^* = \min_{X^* \in X} \{X : \Phi_{\bar{X}} = 0\},$$
 где X есть подмножество разрушенных элементов ИС, а $\bar{X}$ есть дополнительное подмножество.

Другими словами, множество X содержит подмножество пораженных элементов при которых объект воздействия теряет свою функциональность. Строго говоря, если следовать логике вещей, то живучесть объекта воздействия зависит не только от ее структуры, но и от защищенности от воздействия угроз отдельных его элементов и способности объекта воздействия восстанавливаться после воздействия угроз. Однако, предлагаемый в [22, 23] подход эти характеристики не учитывает.

Поэтому актуальной задачей является разработка метода оценивания с помощью которого можно было бы учесть: характеристики воздействия угроз; защищенность элементов от воздействия угроз; способность объекта воздействия реагировать на поражение отдельных элементов их восстановлением. В дальнейшем, для комплексного оценивания устойчивости, предполагается объединить эти два подхода в одном программном модуле.

Пусть заданы: структура объекта воздействия $S = \{A, L\}$, где $A = \{a_i\}$ — семейство элементов информационной сети ИС, $i = 1, 2, \dots, n$; $L = \{l_{ij}\}$ — семейство связей между элементами, $i, j = 1, 2, \dots, n$, $l_{ij} = 1$, если информационное направление существует и оно находится в состоянии «функционально», 0 — в противном случае; если $i = j$, то $l_{ij} = 1$, если соответствующий элемент находится в состоянии «функционален» и 0 — в противном случае. Такую структуру можно представить в виде двумерной матрицы связности или матрицы инцидентности. Для объектов значимой информационной структуры эта задача решена априори в силу закона.

Исходными данными для решения задачи являются:

- интервал времени воздействия угроз $(t_0, t_0 + T]$, где $t_0 = 0$ — момент времени начала отчета интервала времени воздействия угроз; T — момент окончания отчета времени воздействия угроз;
- двухполюсная структура информационной сети ИС, задаваемая в виде графа или структурной функции, которая в общем виде может быть записана следующим обра-

зом: $Z(t) = f[z_1(t), z_2(t), \dots, z_i(t), \dots, z_n(t)]$, где $z_i(t)$ — состояние i -го элемента в момент времени t , $i = 1, 2, \dots, n$, n — общее число элементов в информационной сети ИС, $z_i(t) = 1$, если элемент функционален в момент времени t и $z_i(t) = 0$, в противном случае;

- функции устойчивости i -го элемента [3, 19, 20] $v_i(t) = K_i(t) \phi_i(t)$, $j = 1, 2, \dots, n$, n — общее число элементов в информационной сети ИС, K_i — нестационарный коэффициент оперативной готовности i -го элемента, физически означает, что i -й элемент будет работоспособен в момент времени t_0 и будет функционален в момент времени $t = t_0 + \Delta t$, Δt — интервал времени от начала отчета $t_0 = 0$ до t ; $\phi_i(t)$ — функция живучести i -го элемента, возможность того, что i -й элемент будет находиться в состоянии «функционален» в момент времени $t_0 + t$.

В [20] предлагается для расчета функции устойчивости для условий воздействия угроз не учитывать $K_i(t_0, t_0 + T)$ при расчете $v_i(t)$ по причине того, что ее значение близко к единице и значительно превосходит значение $\phi_j(t)$. Принятие этого допущения значительно снижает сложность моделирования при обеспечении достоверности результата.

Задача оценивания устойчивости направления обмена информацией между полюсами a и b сводится к задаче построения соответствующей функции устойчивости. Порядок вывода функций устойчивости отдельных элементов ранее исследовался автором и приведен в [3, 19 - 21].

Методы исследования. Ретроспективный анализ методов оценивания вероятности связности двухполюсников разветвленной структуры, приведенных в [12 - 16], позволяет утверждать, что семейство существующих методов по точности получаемых результатов можно разделить на две группы: точные аналитические — методы последовательно-параллельных структур, прямого перебора состояний элементов, прямого перебора состояний путей, с применением теоремы разложения, логико-вероятностные; приближенные — методы статистического моделирования и граничных оценок.

Также результаты анализа показывают, что названные методы ориентированы на усредненное оценивание показателей надежности, при условии, что элемент функционирует достаточно долго в неизменных условиях и имеется репрезентативная статистика показателя наблюдаемого свойства при этом его статистическая оценка является состоятельной и не смещенной. Для условий же воздействия угроз такое допущение не приемлемо по нескольким причинам: условия обстановки динамичны; события не являются массовыми, что не позволяет собрать репрезентативную статистику; статистическая частота событий не может служить асимптотической оценкой их вероятности.

Для решения поставленной задачи требуется обобщение существующих методов для прогнозирования возможности того или иного случайного события в произвольный момент времени $t \in (0, T]$. Ниже приведен подход к обобщению существующих методов для условий воздействия угроз и для вычисления функции устойчивости объекта воздействия для названных условий.

Метод последовательно-параллельных структур. Общее описание метода для асимптотических вероятностных оценок приводится в [11-13, 24]. Метод применяется в тех случаях, когда в структуре информационной сети (структура) можно выделить фрагменты последовательно и параллельно соединенных элементов и на основе этого выделения вывести общее аналитическое соотношение. Для условий же воздействия требуется обобщение этих методов для произвольных моментов времени $t \in (0, T]$, следуя следующему алгоритму:

1. В структуре выделяются фрагменты N_i' последовательно соединенных элементов, каждый из фрагментов объединяется в один общий элемент с индексом i и для этого элемента определяется значение соответствующей характеристики $v_i'(t)$ по формуле

$$N_i'(t) = \prod_{j \in J_i} v_j(t),$$

где $N'_i(t)$ — функция устойчивости выделенного фрагмента N'_i (следует обратить внимание, что в обозначении $N'_i(t)$, N в наименовании — это заглавная буква греческого алфавита «ню» и обозначается прямым начертанием, а N'_i — это латинская заглавная N и обозначена курсивом), $v_i(t)$ — функция устойчивости i -го элемента, входящего в фрагмент $N'_i(t)$, J_i — семейство индексов элементов, входящих в выделенный фрагмент $N'_i(t)$. При этом индексы вновь формируемых общих элементов должны отличаться от индексов элементов исходной структуры и индексов, входящих ранее сформированные семейства. После завершения формирования фрагментов N'_i или случае их отсутствия осуществляется переход к п. 2.

2. Выделяются фрагменты N''_k , $k \neq i$ параллельно соединенных элементов, каждый из которых объединяется в один общий фрагмент N''_k и для этого фрагмента определяется значение соответствующего показателя устойчивости $N''_k(t)$ по формуле

$$N''_k(t) = 1 - \prod_{j \in J_k} [1 - v_j(t)],$$

где $v_j(t)$ — функция устойчивости i -го элемента, входящего в фрагмент N''_k , J_k — семейство индексов элементов фрагмента N''_k .

3. Формируется новая укрупненная структура, состоящая из общих i -х и k -х элементов, имеющих показатели устойчивости $N'_i(t)$ и $N''_k(t)$. Для новой структуры повторяются операции пп. 1 и 2.

Операции пп. 1 и 2 выполняются до тех пор, пока не будет получено искомое обобщающее аналитическое соотношение. Данный метод позволяет получить аналитическое соотношение, которое приспособлено для программирования и обеспечивает оперативное определение функциональных характеристик двухполюсных структур, имеющих большое число элементов.

Однако метод неприемлем для произвольных, например, мостиковых структур и требует ручных процедур для формирования фрагментов N'_i и N''_k .

Тестовый пример 1. Задана структура, включающая $m = 11$ элементов, приведенная на рис. 1. Определены функции устойчивости элементов $v_j(t)$, $j = 1, 2, \dots, 11$. Вывести аналитическое соотношение для вычисления функции устойчивости двухполюсника а–б. $N_{ab}(t) = F\{v_1(t), v_2(t), \dots, v_j(t), \dots, v_{11}(t)\}$.

Для чего выделяются фрагменты, содержащие последовательно соединенные элементы. К ним относятся $N'_{1,2} = \{1, 2\}$, $N'_{3,4} = \{3, 4\}$, $N'_{5-7} = \{5, 6, 7\}$, $N'_{8,9} = \{8, 9\}$.

Каждый фрагмент объединяем в один общий элемент, для которого определяется обобщенная функция устойчивости.

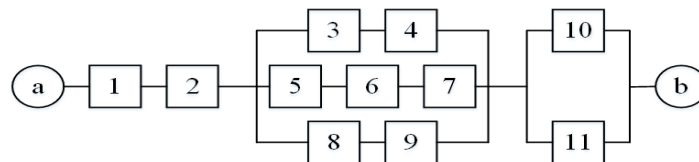


Рис. 1. Вариант исходной структуры
 Fig. 1. A variant of the original structure

В результате получаем четыре обобщенных элемента со значениями функции устойчивости $N'_{12}(t) = v_1(t)v_2(t)$, $N'_{13}(t) = v_3(t)v_4(t)$, $N'_{14}(t) = v_5(t)v_6(t)v_7(t)$, $N'_{15}(t) = v_8(t)v_9(t)$. Выделяем фрагмент $N''_{10,11}$, содержащий параллельно соединенные эле-

менты 10 и 11, для которого функция устойчивости будет иметь $N''_{16}(t) = 1 - [1 - v_{10}(t)][1 - v_{11}(t)]$.

Полученные обобщенные элементы формируются в эквивалентную, с точки зрения характеристик устойчивости, обобщенную двухполусную структуру первого уровня, представленную на рис. 2.

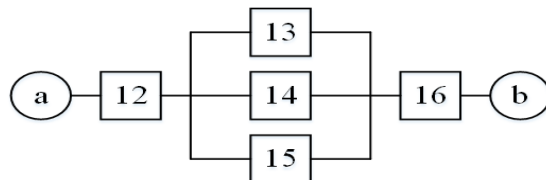


Рис. 2. Обобщенная двухполусная структура первого уровня

Fig. 2. Generalized bipolar structure of the first level

Обобщенная двухполусная структура первого уровня содержит только один фрагмент параллельно соединенных элементов, которому присваивается индекс $N''_{13,14,15}$, для которого функция устойчивости будет иметь вид $N''_{17}(t) = 1 - [1 - v_{13}(t)][1 - v_{14}(t)][1 - v_{15}(t)]$.

Из полученных элементов строится обобщенный вариант двухполусной структуры второго уровня, содержащий только последовательно соединенные элементы, структура которого приведена на рис. 3.

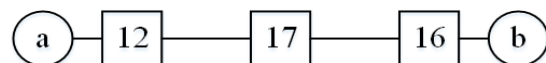


Рис. 3. Обобщенная двухполусная структура второго уровня

Fig. 3. Generalized bipolar structure of the second level

В результате функция устойчивости полученной обобщенной структуры может быть вычислена по формуле $N'_{ab}(t) = v_{12}(t)v_{17}(t)v_{16}(t)$. Последовательно подставляя полученные соотношения для обобщенных элементов, получаем формулу для вычисления функции устойчивости исходной двухполусной структуры:

$$N'_{ab}(t) = v_1(t)v_2(t) \left\{ 1 - [1 - v_3(t)v_4(t)][1 - v_5(t)v_6(t)v_7(t)][1 - v_8(t)v_9(t)] \right\} \cdot \left\{ 1 - [1 - v_{10}(t)][1 - v_{11}(t)] \right\}.$$

Метод перебора состояний элементов. Общее описание метода для асимптотических вероятностных оценок приводится в [11-13, 24].

При использовании метода перебора состояний элементов производится последовательное определение всех $k = 2m$ возможных i -х состояний двухполусной структуры при которых обеспечивается связность $z_i = \{z_1, z_2, \dots, z_j, \dots, z_m\}i$, где z_i — индикатор связности i -й комбинации состояний элементов, $z_i = 1$, если связность обеспечивается, $z_i = 0$ — в противном случае; z_j — индикатор состояния j -го элемента, $z_j = 1$, если j -й элемент позиционируется как «функционален», $z_j = 0$ — в противном случае; $i = 1, 2, \dots, k$, k — число возможных состояний; $j = 1, 2, \dots, m$, число элементов оцениваемой двухполусной структуры.

При этом для вычисления функции устойчивости выделяются только такие комбинации состояний элементов, при которых обеспечивается связность между концевыми полюсами а и б, вычисляются возможность реализации данных состояний:

$$H_i(t) = \prod_{j \in J_{i+}} v_j(t) \prod_{j \in J_{i-}} (1 - v_j(t)), \quad (1)$$

где $H_i(t)$ — вероятность связности i -й комбинации; J_{i+} — совокупность индексов, элементов, соответствующих состоянию «функционален» в i -й комбинации; J_{i-} — совокупность индексов, соответствующих состоянию «не функционален»; $v_j(t)$ — вероятность работоспособного состояния j -го элемента в момент времени t .

В итоге процедуру (1) определения значений u можно задать в виде формулы

$$H_{a-b} = \sum_{i \in I_1} Q_i \quad (2)$$

где I_1 — совокупность индексов состояний, при которых имеется хотя бы один путь (связь) между крайними полюсами исследуемой двухполюсной структуры.

Метод перебора состояний элементов может быть использован для любых структур, он достаточно просто программируется, однако требует значительных затрат времени при больших значениях m .

Например, для решения примера 1, где задается двухполюсная структура из 11 элементов ($m = 11$), требуется «перебрать» 211 комбинаций состояний элементов. Поэтому даже компьютерные программы, составленные на основе данного метода, целесообразно использовать для несложных структур, содержащих относительно небольшое число элементов $m \leq 20$.

Тестовый пример 1. Пусть задана двухполюсная структура, включающая $m = 2$ элемента, граф которой приведен на рис. 4. Определены функции устойчивости элементов $v_1(t)$, $v_2(t)$ [19, 20]. Требуется вывести аналитическое соотношение для вычисления функции устойчивости двухполюсной структуры, изображенной на рис. 4, $H_{a-b} = F\{v_1(t), v_2(t)\}$, используя метод перебора состояний элементов.

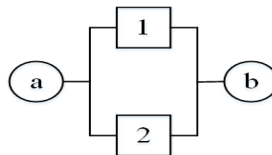


Рис. 4. Двухполюсная структура
 Fig. 4. Two-pole structure

Общее число возможных комбинаций состояний элементов данной двухполюсной структуры составляет $k = 2^2 = 4$.

Это следующие комбинации: $z = \{z_1, z_2\}$, $z_0 = \{0, 0\}$, $z_2 = \{0, 1\}$, $z_3 = \{1, 0\}$, $z_4 = \{1, 1\}$.

Связность между полюсами a и b обеспечивается при комбинациях z_2, z_3, z_4 .

Вероятности реализации данных состояний:

$$H_2(t) = [1 - v_1(t)]v_2, \quad H_3(t) = v_1(t)[1 - v_2(t)], \quad H_4 = v_1(t)v_2(t)$$

Используя формулы (1, 2), получаем следующие соотношения для вычисления функции устойчивости двухполюсной структуры, приведенной на рис. 4:

$$\begin{aligned} H_{ab}(t) &= H_2(t) + H_3(t) + H_4(t) = [1 - v_1(t)]v_2(t) + v_1(t)[1 - v_2(t)] + v_1(t)v_2(t) = \\ &= v_1(t) + v_2(t) - v_1(t)v_2(t) = 1 - [1 - v_1(t)][1 - v_2(t)]. \end{aligned}$$

Естественно, данные соотношения получить гораздо проще, применяя метод последовательно-параллельных структур. Метод перебора состояний путей. Общее описание метода для асимптотических вероятностных оценок приводится в [11-13, 24]. Метод основан на анализе всех 2^n возможных состояний n путей между конечными полюсами двухполюсника. Исходными данными являются: структура двухполюсника, заданная в виде графа, приведенная на рис. 5; функции устойчивости функционирования элементов двухполюсника (узлов).

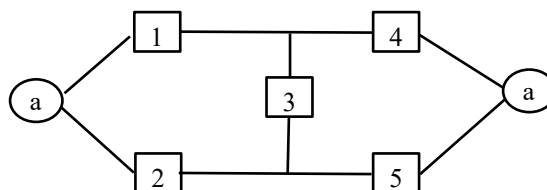


Рис. 5. Тестовая двухполюсная структура
 Fig. 5. Test two-pole structure

Метод включает в себя следующие операции:

1. Определение всех путей $\pi_1, \pi_2, \dots, \pi_n$, между конечными узлами a и b исследуемого двухполюсника. При этом каждый путь обозначается последовательностью индексов его элементов. Например, если путь π_1 содержит элементы 2, 5, 7, то он обозначается $\pi_1 = 2, 5, 7$.

2. Определение $r = 2n - 1$ последовательностей индексов элементов $\pi_i, \pi_{ik}, \pi_{12\dots n}$, полученных путем объединения минимальных путей в различных сочетаниях. В результате последовательности $\pi_i, i = 1, 2, \dots, n$, будут соответствовать полученным путям. Последовательности π_{ik} получаются посредством объединения путей по два, последовательности π_{ikr} — по три и т. д. Например, если объединяются пути $\pi_1 = 2, 5, 7, 12$; $\pi_2 = 3, 5, 7, 14$, $\pi_3 = 3, 4, 7, 12$, то в результате объединения получаем следующие последовательности: $\pi_{12} = 2, 3, 5, 7, 12, 14$, $\pi_{13} = 2, 3, 4, 5, 7, 12$, $\pi_{23} = 3, 4, 5, 7, 12, 14$; $\pi_{123} = 2, 3, 4, 5, 7, 12, 14$.

3. Вычисление вероятностей связности $v_1(t), v_{1k}(t), \dots, v_{12\dots n}(t)$ двухполюсной структуры, включающих один путь, полученный на основе объединенных путей $\pi_1, \pi_{1k}, \dots, \pi_{12\dots n}$. Для этого следует вместо индексов элементов j подставлять и умножать значения функций устойчивости $v_j(t)$. Например, если в результате выполнения алгоритма получили $\pi_{13} = 2, 3, 4, 5, 7, 12$, то $v_{13}(t) = v_2(t) v_3(t) v_4(t) v_5(t) v_7(t) v_{12}(t)$.

4. Сложение вычисленных вероятностей и определение значений:

$$S_1 = \sum_{i=1}^n v_i(t), S_2 = \sum_{i < k}^n v_{ik}(t), \dots, S_n = v_{12\dots n}(t), \quad (3)$$

где число слагаемых при определении S_2 равно числу сочетаний C_n^3 и т. д. При определении S_n имеем одно значение $v_{12\dots n}$.

5. Определение вероятности связности двухполюсной структуры по формуле

$$H = \sum_{i=1}^n (-1)^{i-1} S_i. \quad (4)$$

При небольшом количестве путей получается существенный выигрыш в сложности расчета для любых двухполюсных структур.

При равном числе путей и элементов объем вычислений при использовании метода перебора путей сравним с методом перебора состояний элементов, однако при меньшем числе путей можно получить существенный выигрыш во времени расчета. Преимуществом метода является возможность формализовать алгоритм расчета устойчивости функционирования двухполюсной структуры, а также приспособленной к оцениванию мостиковых структур.

Тестовый пример 2. Пусть задана мостиковая двухполюсная структура, включающая $m = 9$ элементов, которая приведена на рис. 5. Конечными узлами являются узлы 1 и 4. Определены функции устойчивости элементов $v_1(t), v_2(t), v_3(t), v_4(t), v_5(t), v_6(t), v_7(t), v_8(t), v_9(t)$. Требуется вывести формулу для расчета устойчивости функционирования направления информационного обмена между конечными полюсами 1 и 4. Определены функции устойчивости элементов $H_{14} = F\{v_1(t), v_2(t), v_3(t), v_4(t), v_5(t), v_6(t), v_7(t), v_8(t), v_9(t)\}$, используя метод перебора состояний путей. Для чего определяется семейство путей между полюсами 1 и 4. В результате получаем $\pi_1 = 1, 5, 2, 8, 4$; $\pi_2 = 1, 6, 3, 9, 4$; $\pi_3 = 1, 5, 2, 7, 3, 9, 4$; $\pi_4 = 1, 6, 3, 7, 2, 8, 4$. Число путей $n = 4$.

Определяем последовательности $\pi_i, \pi_{ik}, \pi_{1234}$, полученные путем объединения путей в различных сочетаниях. В результате, выделяя вначале узлы по возрастанию, а затем ребра, получаем, что путям π_i соответствуют следующие последовательности индексов элементов: $\pi_1 = 1, 2, 4, 5, 8$; $\pi_2 = 1, 3, 4, 6, 9$; $\pi_3 = 1, 2, 3, 4, 5, 7, 9$; $\pi_4 = 1, 2, 3, 4, 6, 7, 8$.

При объединении π_{ik} по два получаем:

$\pi_{12} = 1, 2, 3, 4, 5, 6, 8, 9$; $\pi_{13} = 1, 2, 3, 4, 5, 7, 8, 9$; $\pi_{14} = 1, 2, 3, 4, 5, 6, 7, 8$; $\pi_{23} = 2, 3, 4, 5, 6, 7, 9$; $\pi_{24} = 1, 2, 3, 4, 6, 7, 8, 9$; $\pi_{34} = 1, 2, 3, 4, 5, 6, 7, 8, 9$.

При объединении π_{ikr} по три получаем:

$\pi_{123} = 1, 2, 3, 4, 5, 6, 7, 8, 9$; $\pi_{124} = 1, 2, 3, 4, 5, 6, 7, 8, 9$; $\pi_{234} = 1, 2, 3, 4, 5, 6, 7, 8, 9$;

$\pi_{134} = 1, 2, 3, 4, 5, 6, 7, 8, 9$.

При объединении π_{1234} по четыре получаем:

$\pi_{1234} = 1, 2, 3, 4, 5, 6, 7, 8, 9$.

Таким образом, $\pi_{123} = \pi_{124} = \pi_{234} = \pi_{134} = \pi_{1234}$

Посредством подстановки вместо индексов элементов функций устойчивости элементов $v_j(t)$ и их перемножения значения функции вероятностей связности последовательных структур в момент времени t $q_i(t)$, $q_{ik}(t)$, $q_{ikr}(t)$, $q_{1234}(t)$.

В результате получаем:

$H_1(t) = v_1(t)v_2(t)v_4(t)v_5(t)v_8(t)$;

$H_2(t) = v_1(t)v_3(t)v_4(t)v_6(t)v_9(t)$;

$H_3(t) = v_1(t)v_2(t)v_3(t)v_4(t)v_5(t)v_7(t)v_9(t)$; $H_4(t) = v_1(t)v_2(t)v_3(t)v_4(t)v_6(t)v_7(t)v_8(t)$;

$H_{12}(t) = v_1(t)v_2(t)v_3(t)v_4(t)v_5(t)v_6(t)v_8(t)v_9(t)$; $H_{13}(t) = v_1(t)v_2(t)v_3(t)v_4(t)v_5(t)v_7(t)v_8(t)v_9(t)$;

$H_{14}(t) = v_1(t)v_2(t)v_3(t)v_4(t)v_5(t)v_6(t)v_7(t)v_8(t)$; $H_{23}(t) = v_1(t)v_2(t)v_3(t)v_4(t)v_5(t)v_6(t)v_7(t)v_9(t)$;

$H_{24}(t) = v_1(t)v_2(t)v_3(t)v_4(t)v_6(t)v_7(t)v_8(t)v_9(t)$; $H_{34}(t) = v_1(t)v_2(t)v_3(t)v_4(t)v_5(t)v_6(t)v_7(t)v_8(t)v_9(t)$;

$H_{123}(t) = H_{124}(t) = H_{234}(t) = H_{134}(t) = H_{1234}(t) = v_1(t)v_2(t)v_3(t)v_4(t)v_5(t)v_6(t)v_7(t)v_8(t)v_9(t)$.

Складывая полученные значения функций вероятностей связности последовательных структур для моментов времени t и определяем значения $S_i(t)$ по формуле (3) и получаем:

$S_1(t) = H_1(t) + H_2(t) + H_3(t) + H_4(t)$;

$S_2(t) = H_{12}(t) + H_{13}(t) + H_{14}(t) + H_{23}(t) + H_{24}(t) + H_{34}(t)$; $S_3(t) = 3H_{123}(t)$; $S_4(t) = 4H_{1234}(t)$.

Определяем вероятность связности по формуле (4). В результате получаем $H_{14}(t) = S_1(t) - S_2(t) + S_3(t) - S_4(t)$. Если функции устойчивости функционирования отдельных элементов равны, т. е. $v_j(t) = v(t)$, то формула для расчета упрощается и имеет вид: $H_{14}(t) = [v(t)]^5 \{2 + 2[v(t)]^2 - 5[v(t)]^3 + 2[v(t)]^3\}$.

Рассмотренный метод в основном применим для автоматизации расчетов.

Логико-вероятностный метод. Общее описание метода для асимптотических вероятностных оценок приводится в [11-13, 24]. Методы основаны на представлении структур-

ной функции в виде логической функции $Z = f(z) = f(z_1, z_2, \dots, z_j, \dots, z_m)$, где z_j рассматриваются как булевы переменные, $j = 1, 2, \dots, m$. Решение задачи заключается в использовании широко известных и достаточно формализованных методов математической логики для упрощения логической функции $f(z)$ с последующей заменой z_j на $v_j(t)$ и переходом к выражению $v(t) = B\{v_1(t), v_2(t), \dots, v_j(t), \dots, v_m(t)\}$.

При переходе от логической функции $f(z)$ к выражению для оператора B необходимо учитывать специальные соотношения теории вероятностей и математической логики, используемые при разработке логико-вероятностных методов.

Достоинством данных методов является возможность применения хорошо разработанного аппарата булевой алгебры при упрощении структурной функции [14, 15]. Однако при большом числе переменных z_j получаются достаточно громоздкие выражения для булевых функций, что требует дополнительных ресурсов оперативной памяти при реализации компьютерных программ. Методы обеспечивают некоторое снижение времени вычислений, однако из-за сложности получаемых выражений не имеют в целом существенного преимущества перед вышеизложенными методами перебора состояний элементов и путей.

Метод статистического моделирования. Общее описание метода для асимптотических вероятностных оценок применительно к воздействию угроз приводится в [25]. Методы статистического моделирования используются в тех случаях, когда точные аналитические методы приводят к большим затратам времени при определении вероятности связности

сложных структур с большим количеством мостиковых соединений. Для реализации метода статистического моделирования определяется множество возможных минимальных путей между полюсами двухполюсной структуры и для каждого i -го пути формируется структурная функция

$$\pi_i = \prod_{j \in J_i} z_j, \quad i = 1, 2, \dots, n, \quad (5)$$

где J_i — множество индексов элементов i -го пути; z_j — состояние j -го элемента.

С учетом полученных частных структурных функций π_i , общая структурная функция двухполюсной структуры будет иметь вид

$$Z = 1 - \prod_{i=1}^n (1 - \pi_i), \quad i = 1, 2, \dots, n. \quad (6)$$

Состояние z_j каждого элемента определяется с помощью датчика случайных чисел $x_j = R_j(0, 1)$ и заданных значений $v_j(t)$.

При этом, если $x_j \leq v_j(t)$, то $z_j = 1$; в противном случае $z_j = 0$.

В результате процедура получения оценок функции устойчивости функционирования двухполюсной структуры N_{ab} будет включать следующие этапы:

- 1) задание числа реализаций r , по которым производится оценка значений $v_j(t)$, $s = 1, 2, \dots, r$; s — номер реализации;
- 2) определение множества состояний $z_s = \{z_j\}_s$, $s = 1, 2, \dots, r$, с помощью заданных значений $v_j(t)$ и датчика случайных чисел;
- 3) определение значений структурной функции Z_s с помощью (5) и (6), $Z_s = f(z_s)$;
- 4) определение оценки $\hat{v}_j(t)$ по формуле

$$\hat{v}_j(t) = r^{-1} \sum_{s=1}^r Z_s(t).$$

Задание требуемого числа реализаций производится в соответствии с допустимой ошибкой вычисления оценки $\hat{v}_j(t)$.

Метод граничных оценок. Общее описание метода применительно к точечным оценкам вероятности приведено в [24]. Метод основан на вычислении верхней и нижней границ значений $H(t)$. Для этого определяются между заданными абонентами сети все минимальные пути (или просто пути) и сечения.

Здесь под путем понимается последовательное соединение неповторяющихся элементов сети, обеспечивающее связь между заданной парой абонентов. Для двухполюсной структуры, изображенной на рис. 5, имеются следующие пути: $\pi_1 = 1, 4$; $\pi_2 = 2, 5$; $\pi_3 = 1, 3, 5$; $\pi_4 = 2, 3, 4$. Число путей $n = 4$. Для сохранения связи между абонентами достаточно иметь все исправные элементы хотя бы одного пути.

Под сечением двухполюсной структуры понимается совокупность неповторяющихся элементов, в которой отказ всех элементов приводит к нарушению связи между крайними полюсами. Для структуры, изображенной на рис. 5, имеются следующие сечения; $s_1 = 1, 2$; $s_2 = 4, 5$; $s_3 = 1, 3, 5$; $s_4 = 2, 3, 4$.

При этом отдельные сечения могут совпадать с путями. Тогда мостиковую двухполюсную структуру, приведенную на рис. 5, можно представить в виде двух эквивалентных, приближенно описывающих ее схем: параллельно соединенных путей, изображенную на рис. 6, и последовательно соединенных сечений, изображенную на рис. 6.

В качестве исходных данных для реализации метода используется перечень всех путей двухполюсной структуры, где каждый из путей включает множество элементов, имеющих индексы J_i , $i = 1, \dots, n$, и перечень сечений двухполюсной структуры, где каждое сечение включает множество элементов, имеющих L_k , $k = 1, \dots, r$.

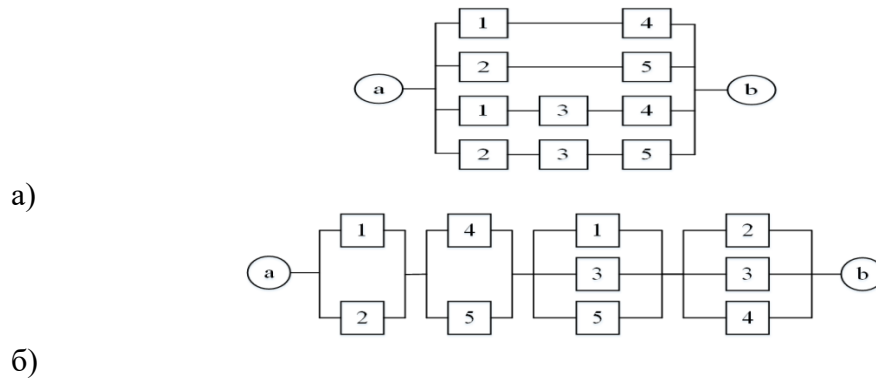


Рис. 6. Эквивалентные схемы мостиковой двухполюсной структуры
а) параллельно соединенные пути, б) последовательно соединены сечения

Fig. 6. Equivalent schemes of a two-pole bridge structure

a) parallel connected paths, b) sections connected in series

Для каждого i -го пути и k -го сечения вводятся вероятности их безотказной работы $p_i(t)$ и $q_k(t)$ соответственно по формулам

$$p_i(t) = \prod_{j \in J_i} v_j(t), \quad q_k(t) = 1 - \prod_{j \in L_k} [1 - v_j(t)]$$

где $v_j(t)$ — функция устойчивости j -го элемента, входящего в соответствующий путь или сечение.

Генезис понятия «функция устойчивости» приведен в [3]. Функция устойчивости для каждого элемента вычисляется с помощью методов, изложенных в [11-13, 24]. В результате действительное значение $v_j(t)$ в каждый момент времени t будет удовлетворять неравенству:

$$\prod_{k=1}^r q_k(t) \leq v_j(t) \leq 1 - \prod_{i=1}^n [1 - p_i(t)].$$

Метод в отдельных случаях, особенно при больших значениях $v_j(t)$, позволяет получить достаточно высокую точность оценок, однако требует предварительного определения перечня путей и сечений.

Пример 3. Задана мостиковая двухполюсная структура, включающая $m = 5$ элементов, приведенная на рис. 5. Определены функции устойчивости элементов $v_1(t)$, $v_2(t)$, $v_3(t)$; $v_4(t)$ $v_5(t)$. Задан момент времени $t = 8$ для которого требуется определить вероятность связности двухполюсной структуры $v_1(8) = 0,5$, $v_2(8) = 0,6$, $v_3(8) = 0,7$, $v_4(8) = 0,8$, $v_5(8) = 0,9$. Определить верхнюю и нижнюю оценку показателя связности двухполюсной структуры N_{ab} . Решение: определяем значения p_i для всех путей. Получаем

$$p_1(8) = v_1(8)v_4(8) = 0,5 \cdot 0,8 = 0,4; \quad p_2(8) = v_2(8)v_5(8) = 0,6 \cdot 0,9 = 0,54;$$

$$p_3(8) = v_1(8)v_3(8)v_5(8) = 0,5 \cdot 0,7 \cdot 0,9 = 0,315; \quad p_4(8) = v_2(8)v_3(8)v_4(8) = 0,6 \cdot 0,7 \cdot 0,8 = 0,336;$$

В результате верхняя граница

$$v_{up}(8) = 1 - [1 - p_1(8)][1 - p_2(8)][1 - p_3(8)][1 - p_4(8)] = 1 - 0,6 \cdot 0,46 \cdot 0,685 \cdot 0,664 = 1 - 0,125 = 0,875.$$

Определяем значения q_k для всех путей, Получаем

$$q_1(8) = 1 - [1 - v_1(8)][1 - v_2(8)] = 1 - 0,5 \cdot 0,4 = 0,8;$$

$$q_2(8) = 1 - [1 - v_4(8)][1 - v_5(8)] = 1 - 0,2 \cdot 0,1 = 0,98;$$

$$q_3(8) = 1 - [1 - v_1(8)][1 - v_3(8)][1 - v_5(8)] = 1 - 0,5 \cdot 0,3 \cdot 0,1 = 0,985;$$

$$q_4(8) = 1 - (1 - v_2(8))(1 - v_3(8))(1 - v_4(8)) = 1 - 0,4 \cdot 0,3 \cdot 0,2 = 0,976.$$

В результате нижняя граница будет равна

$$v_{low}(8) = q_1(8)q_2(8)q_3(8)q_4(8) = 0,8 \cdot 0,98 \cdot 0,985 \cdot 0,976 = 0,754.$$

В результате вычислений получили, что действительное значение $v(8)$ удовлетворяет неравенству $0,754 \leq v(8) \leq 0,875$.

Обсуждение результатов. Результаты исследования позволяют утверждать, что перспективным является объединение двух подходов, приведенных в [22, 23] и рассмотренных в настоящей статье под единой целью оценивания устойчивости объектов воздействия, функционирующих в условиях угроз. Перспективным направлением исследования является исследование устойчивости функционирования объекта воздействия для различных условий информационной неопределенности, при которых решение по воздействию угроз противником принимается в условиях информационной неопределенности.

При принятии решение противнику: неизвестно множество элементов объекта воздействия (IP адреса); известно множество элементов ИС, входящих в состав объекта воздействия (IP адреса); известна структура объекта воздействия (конфигурация); известны результаты воздействия угроз. Решив эти задачи, возможно обосновывать внедрение методов обеспечения конфиденциальности структуры объекта воздействия и его текущего состояния.

Вывод. Существующие методы, ориентированные на исследование стационарных потоков отказов, характерные для штатных условий эксплуатации объекта воздействия, в прямой постановке не могут быть применены для оценивания устойчивости их функционирования, для условий воздействия угроз. Исследования показали, что требуются их обобщение для нестационарных потоков случайных событий, связанных с воздействием угроз. Также результаты исследования позволяют утверждать, что среди рассмотренных методов не существует универсального. Каждый метод имеет свои достоинства и недостатки, которые не пересекаются, поэтому для каждого случая нужно осуществлять целенаправленный выбор и требуется соответствующая методика. Перспективным направлением является автоматизация расчетов и интерпретации полученных результатов.

Благодарности. Исследование выполнено при поддержке Фонда Потанина.

Acknowledgments. The study was supported by the Potanin Foundation.

Библиографический список:

1. ГОСТ Р 59516–2021. Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 420-ст. М.: Стандартинформ. 2021. – 20 с.
2. ГОСТ Р ИСО/МЭК 27005–2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст. М.: Стандартинформ. 2012. – 91 с.
3. Воеводин В. А. Генезис понятия структурной устойчивости информационной инфраструктуры автоматизированной системы управления производственными процессами к воздействию целенаправленных угроз информационной безопасности // Вестник Воронежского института ФСИИ России. 2023. № 2. С. 30–41.
4. Методика оценки угроз безопасности информации. Методический документ ФСТЭК России от 5 февраля 2021 г. // Официальный сайт ФСТЭК России [Электронный ресурс]. – URL: <https://fstec.ru/component/attachments/download/2919> (дата обращения 08.04.2021).
5. Васильев В. И., Вульфин А. М., Кириллова А. Д., Кучкарова Н. В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. № 3. С. 110–134. DOI: 10.24412/2410-9916-2021-3-110-134.
6. ГОСТ Р ИСО 19011–2021 Руководящие указания по проведению аудита систем менеджмента. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 21 апреля 2021 г. N 261-ст. М.: Стандартинформ. 2021. – 42 с.
7. ГОСТ Р ИСО/МЭК 27007—2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 1.06.2015 М.: ФГУП «Стандартинформ», 2015. – 27 с.
8. Zhang Y., Wang L., Xiang Y., Ten C. W. Power System Reliability Evaluation with SCADA Cybersecurity Considerations // IEEE Transactions on Smart Grid. 2015. vol. 6. no. 4. pp. 1707–1721. DOI: 10.1109/TSG.2015.2396994.
9. Haring I., Ebenhoch S., Stolz A. Quantifying Resilience for Resilience Engineering of Socij Technical Systems. *European Journal for Security Research*. 2016; 1: 21–58. DOI: 10.1007/s41125-015-0001-x.

10. Haque M. A., Shetty S., Krishnappa B. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2019. pp. 273–281. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2019.00058.
11. Kete N., Punzo G., Linkov I. Enhancing resilience within and between critical infrastructure systems // Environment Systems and Decisions. 2018. vol. 38. pp. 275–277. DOI: 10.1007/s10669-018-9706-5.
12. Надежность и эффективность в технике. Справочник Том № 5. Проектный анализ надежности/ под ред. В.И. Патрушева и А.И. Рембезы. – М.: Машиностроение, 1989, – 376 с.
13. Hammad A.W., Haddad A. Infrastructure Resilience: Assessment, Challenges and Insights // Industry, Innovation and Infrastructure. Encyclopedia of the UN Sustainable Development Goals. Springer. Cham, 2021. pp. 1–13. DOI: 10.1007/978-3-319-71059-4_25-1.
14. Рябинин И.А. Надежность и безопасность структурно-сложных систем. Спб.: Политехника. 2000. 248 с.
15. Шубинский И. Б. Структурная надежность информационных систем. Методы анализа / И. Б. Шубинский // М.: «Журнал Надежность». 2012. – 216 с.
16. Шубинский И. Б. Функциональная надежность информационных систем. Методы анализа / И. Б. Шубинский // М.: «Журнал Надежность». 2012. – 296 с.
17. Коробов В. Б. Теория и практика экспертных методов: монография. – М.: ИНФРА-М, 2019. – 282 с.
18. Гуцыкова С. В. Метод экспертных оценок. Теория и практика. Серия «Методы психологии». М.: Институт психологии РАН, 2011. – 212 с.
19. Воеводин В. А. Математическая модель оценивания устойчивости функционирования элемента информационной инфраструктуры автоматизированной системы управления, подверженной воздействию угроз информационной безопасности// Информационные технологии, №1. Том 30. 2024. DOI: 10.17587/it.30.23-31. С. 23–31.
20. Воеводин В. А. Модель оценки функциональной устойчивости элементов информационной инфраструктуры для условий воздействия множества компьютерных атак. Информатика и автоматизация. 2023. Том 22 № 3. – С. 691–715. <https://DOI 10.15622/ia.22.3.8>.
21. Воеводин В. А., Виноградов И. В., Волков Д. И. Об оценке устойчивости функционирования объекта информатизации в условиях компьютерных атак при экспоненциальном законе распределения времени до воздействия противника и восстановления работоспособности. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(3): 39-51. DOI:10.21822/2073-6185-2022-49-3-39-51.
22. Черкесов Г. Н., Недосекин А. О., Виноградов В.В. Анализ функциональной живучести структурно-сложных технических систем // Надежность. 2018. Том 18, № 2. С. 17-24. DOI: 10.21683/1729-2646-2018-18-2-17-24.
23. Черкесов Г.Н., Недосекин А. О. Описание подхода к оценке живучести сложных структур при много-разовых воздействиях высокой точности // Надежность. 2016. Том 16, № 2(57). С. 3–15.
24. Хохлачев Е. Н. Организация и технологии выработки решений при управлении системой и войсками связи. Часть 2. Выработка решений при восстановлении сетей связи. – М.: ВА РВСН, 2009. 241 с.
25. Voevodin V. A. Monte Carlo method for predicting the stability of the functioning of the informatization object in the conditions of massive computer attacks. International Conference «Marchuk Scientific Readings 2021» (MSR-2021) Journal of Physics: Conference Series 2099 (2021). DOI 10.1088/1742-6596/2099/1/012070.

References

1. GOST R 59516–2021. Information Technology. Information security management. Rules for insurance of information security risks. *Approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology* dated May 20, 2021 N 420-st. M.: Standardinform. 2021: 20. (In Russ)
2. GOST R ISO/IEC 27005–2010 Information technology. Methods and means of ensuring safety. Information security risk management. *Approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology* dated November 30, 2010 N 632-p. Standardinform. 2012: 91. (In Russ)
3. Voevodin V. A. Genesis of the concept of structural stability of the information infrastructure of an automated production process management system to the impact of targeted threats to information security. *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*. 2023; 2: 30–41. (In Russ)
4. Methodology for assessing threats to information security. Methodological document of the FSTEC of Russia dated February 5, 2021 // Official website of the FSTEC of Russia [Electronic resource]. – URL: <https://fstec.ru/component/attachments/download/2919> (access date 04/08/2021). (In Russ)
5. Vasilyev V. I., Vulfin A. M., Kirillova A. D., Kuchkarova N. V. Methodology for assessing current threats and vulnerabilities based on cognitive modeling and Text Mining technologies. *Control, Communication and Security Systems*. 2021; 3: 110–134. DOI: 10.24412/2410-9916-2021-3-110-134. (In Russ)
6. GOST R ISO 19011–2021 Guidelines for conducting audits of management systems. *Approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology* dated April 21, 2021; 261-p. M.: Standardinform. 2021: 42. (In Russ)

7. GOST R ISO/IEC 27007—2014. Information technology. Methods and means of ensuring security. Guidelines for auditing information security management systems. Approved and put into effect by order of the Federal Agency for Technical Regulation and Metrology dated June 1, 2015 M.: FSUE “Standartinform”, 2015: 27. (In Russ)
8. Zhang Y., Wang L., Xiang Y., Ten C. W. Power System Reliability Evaluation with SCADA Cybersecurity Considerations. *IEEE Transactions on Smart Grid*. 2015; 6(4):1707–1721. DOI: 10.1109/TSG.2015.2396994.
9. Haring I., Ebenhoch S., Stolz A. Quantifying Resilience for Resilience Engineering of Socij Technical Systems. *European Journal for Security Research*. 2016; 1: 21–58. DOI: 10.1007/s41125-015-0001-x.
10. Haque M. A., Shetty S., Krishnappa B. ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems. IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2019; 273–281. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2019.00058.
11. Kete N., Punzo G., Linkov I. Enhancing resilience within and between critical infrastructure systems. *Environment Systems and Decisions*. 2018; 38: 275–277. DOI: 10.1007/s10669-018-9706-5.
12. Reliability and efficiency in technology. Handbook Volume No. 5. Design reliability analysis / ed. IN AND. Patrushev and A.I. Rembezas. M.: Mechanical Engineering, 1989; 376. (In Russ)
13. Hammad A.W., Haddad A. Infrastructure Resilience: Assessment, Challenges and Insights. *Industry, Innovation and Infrastructure. Encyclopedia of the UN Sustainable Development Goals*. Springer. Cham, 2021; 1–13. DOI: 10.1007/978-3-319-71059-4_25-1.
14. Ryabinin I. A. Reliability and safety of structurally complex systems. St. Petersburg: Polytechnic. 2000: 248. (In Russ)
15. Shubinsky I. B. Structural reliability of information systems. Methods of analysis. I. B. Shubinsky M.: “Reliability Magazine”. 2012: 216. (In Russ)
16. Shubinsky I. B. Functional reliability of information systems. Methods of analysis. M.: “Journal Reliability”. 2012: 296. (In Russ)
17. Korobov V. B. Theory and practice of expert methods: monograph. M.: INFRA-M, 2019: 282. (In Russ)
18. Gutsykova S. V. Method of expert assessments. *Theory and practice. Series "Methods of Psychology"*. M.: Institute of Psychology RAS, 2011: 212. (In Russ)
19. Voevodin V. A. Mathematical model for assessing the stability of the functioning of an element of the information infrastructure of an automated control system exposed to information security threats. *"Information Technologies"*, 2024; 30(1): 23–31. DOI: 10.17587/it.30.23 -31(In Russ)
20. Voevodin V. A. Model for assessing the functional stability of information infrastructure elements under conditions of exposure to multiple computer attacks. *Computer science and automation*. 2023; 22(3): 691–715. <https://DOI 10.15622/ia.22.3.8>. (In Russ)
21. Voevodin V. A., Vinogradov I. V., Volkov D. I. On assessing the stability of the functioning of an informatization object in the conditions of computer attacks under the exponential law of distribution of time before the enemy's influence and restoration of performance. *Herald of the Dagestan State Technical University. Technical Sciences*. 2022; 49(3): 39-51. DOI:10.21822/2073-6185-2022-49-3-39-51. (In Russ)
22. Cherkosov G.N., Nedosekin A.O., Vinogradov V.V. Analysis of the functional survivability of structurally complex technical systems. *Reliability*. 2018;18(2):17-24.DOI:10.21683/1729-2646-2018-18-2-17-24. (In Russ)
23. Cherkosov G.N., Nedosekin A.O. Description of the approach to assessing the survivability of complex structures under repeated high-precision impacts.. *Reliability*. 2016; 16(2)(57): 3–15. (In Russ)
24. Khokhlachev E. N. Organization and technology for developing solutions in the management of the system and communications troops. Part 2. Development of solutions when restoring communication networks. M.: VA Strategic Missile Forces, 2009:241. (In Russ)
25. Voevodin V. A. Monte Carlo method for predicting the stability of the functioning of the informatization object in the conditions of massive computer attacks. International Conference “Marchuk Scientific Readings 2021” (MSR-2021) *Journal of Physics: Conference Series* 2099 (2021). DOI 10.1088/1742-6596/2099/1/012070.

Сведения об авторах:

Воеводин Владислав Александрович, кандидат технических наук, доцент кафедры информационной безопасности; vva541@mail.ru

Крахотин Никита Александрович, студент; nikita.krahotin@mail.ru

Information about authors:

Vladislav A. Voevodin, Cand. Sci. (Eng.), Assoc. Prof., Department of Information Security; vva541@mail.ru

Nikita A. Krahotin, Student; nikita.krahotin@mail.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 26.12.2023.

Одобрена после рецензирования/ Revised 17.01.2024.

Принята в печать/Accepted for publication 17.01.2024.