КОМПЬЮТЕРНОЕ ОБЕСПЕЧЕНИЕ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

COMPUTER SOFTWARE AND COMPUTING EQUIPMENT

Научная статья
УДК 004.942
https://doi.org/10.24143/2072-9502-2022-2-33-40

Информационные и телекоммуникационные ресурсы критически важных инфраструктур: особенности интервального анализа защищенности

***Игорь Витальевич Котенко*[1], *Игорь Борисович Паращук*[2] ***

[1, 2]*Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, Россия, shchuk@rambler.ru* *

Аннотация. Объектом исследования является новый методологический подход к решению задачи интервального анализа защищенности информационных и телекоммуникационных ресурсов критически важных инфраструктур. Данный подход представляет собой один из вариантов практического приложения методов теории интервальных средних (интервальных вычислений). Проведен анализ особенностей этого подхода, определяющих его применимость и полезность в вопросе оценки показателей защищенности подобных сложных технических систем на интервале времени. Рассмотрены теоретические аспекты построения алгоритмов вычислений интервальных средних значений уровней защищенности информационных и телекоммуникационных ресурсов критически важных инфраструктур, особенности вычислений верхнего и нижнего средних значений уровней защищенности. Предложена последовательность вычислений и аналитические выражения для расчетов на примере конкретного показателя защищенности. Подход предполагает учет современных требований подсистем управления безопасностью сложных технических систем, требований должностных лиц (аудиторов, администраторов безопасности), связанных с инерционностью процессов принятия решения, с длительностью циклов контроля защищенности и управления безопасностью систем такого класса. Он позволяет получать не точечные (мгновенные), а интервальные оценки показателей защищенности, при этом анализ осуществляется с заранее заданной периодичностью и учитывает неопределенность исходных данных – наблюдаемых и управляемых показателей защищенности. При этом интервальный анализ не обладает большой математической и вычислительной сложностью, но позволяет получать адекватные задачам контроля и управления интервальные оценки защищенности ресурсов, экономить вычислительный ресурс и, в конечном итоге, работает на повышение достоверности контроля безопасности современных критически важных инфраструктур.

Ключевые слова: интервальный анализ, защищенность, метод, интервальные средние, показатель, информационные и телекоммуникационные ресурсы, критически важные инфраструктуры

Благодарности: работа выполнена при частичной финансовой поддержке бюджетной темы 0073-2019-0002.

Для цитирования: *Котенко И. В., Паращук И. Б.* Информационные и телекоммуникационные ресурсы критически важных инфраструктур: особенности интервального анализа защищенности // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2022. № 2. С. 33–40. https://doi.org/10.24143/2072-9502-2022-2-33-40.

Original article

Information and telecommunication resources of critical infrastructures: features of interval security analysis

Igor V. Kotenko[1], Igor B. Parashchuk[2] *

*[1, 2]St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg, Russia, shchuk@rambler.ru **

Abstract. The object of the research is a new methodological approach to solving the problem of interval analysis of the security of information and telecommunication resources of critical infrastructures. This approach is one of the variants of practising the methods of the class midvalues (interval calculations). The approach characteristics were analyzed to determine its validity and usefulness for assessing the security indicators of such complex technical systems over a time interval. There have been considered theoretical aspects of building the algorithms for calculating the class midvalues of security levels of information and telecommunication resources of critical infrastructures, factors of calculating the upper and lower class midvalues of security levels. A sequence of calculations and analytical expressions for calculations on the example of a specific security indicator are proposed. The approach offers taking into account the modern requirements of security management subsystems of complex technical systems, the requirements of officials (auditors, security administrators) related to the inertia of decision-making processes, with the duration of cycles of security control and security management of systems of this class. It allows one to obtain not point (instantaneous), but interval estimates of security indicators, while the analysis is carried out with a predetermined frequency and takes into account the uncertainty of the initial data – observed and controlled security indicators. At the same time, interval analysis does not have great mathematical and computational complexity, but it allows one to obtain interval estimates of resource security adequate to control and management tasks, saves computing resources and, ultimately, works to increase the reliability of security control of modern critical infrastructures.

Keywords: interval analysis, security, method, interval averages, indicators, information and telecommunication resources, critical infrastructure

Acknowledgment: the study was carried out under the partial financial support of the budget subject 0073-2019-0002.

For citation: Kotenko I. V., Parashchuk I. B. Information and telecommunication resources of critical infrastructures: features of interval security analysis. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*. 2022;2:33-40. (In Russ.) https://doi.org/10.24143/2073-5529-2022-2-33-40.

Введение

Создание и совершенствование критически важных инфраструктур любой страны затруднено, а зачастую невозможно без одновременного и, в ряде случаев, опережающего развития информационных и телекоммуникационных систем и комплексов, являющихся одним из ключевых элементов таких инфраструктур и обеспечивающих материальную основу своевременного, достоверного и безопасного обмена данными между их пользователями.

Под критически важной инфраструктурой (КВИ) понимается экономическая, производственная, энергетическая, информационная и/или телекоммуникационная инфраструктура, прекращение или нарушение функционирования которой приводит к чрезвычайной ситуации или к значительным негативным последствиям на длительный период времени для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства страны либо для жизнедеятельности населения, проживающего на соответствующей территории [1, 2]. При этом к информационным ресурсам КВИ относят всю совокупность данных, организованных для эффективного получения достоверной информации в интересах обеспечения бесперебойного функционирования КВИ. Это совокупность отдельных документов и массивов документов, а также множество документов и массивов документов в информационных подсистемах КВИ – библиотеках, архивах, фондах, банках данных и других информационных подсистемах [3, 4].

К телекоммуникационным ресурсам КВИ могут быть отнесены все имеющиеся в телекоммуникационных сетях, системах и комплексах абонентские номера, IP-адреса и адреса доменов, количество и пропускная способность линий связи (проводных, оптических, радио- и спутниковых линий), каналов и трактов для передачи информации в КВИ, маршрутизаторов, коммутационных станций и узлов, а также радиочастотный ресурс [5, 6].

При этом задачи анализа защищенности информационных и телекоммуникационных ресурсов (ИиТР) современных КВИ заслуживают особого внимания. Они являются ключевым вопросом теории и практики управления защитой данных в КВИ и обеспечения их безопасного функционирования [7, 8].

Вместе с тем существующие трудности создания безопасных ИиТР КВИ, сложности решения задачи многокритериального анализа их защищен-

ности обусловлены, в том числе, отсутствием универсальных методов, учитывающих целый ряд свойств и особенностей подсистем защиты элементов этих ресурсов, неполноту и неоднородность исходной информации о качестве защиты информации в ИиТР КВИ в целом. Поэтому разработка новых методов расчета и многокритериального интервального анализа защищенности ИиТР современных КВИ при неполной исходной информации является важной, актуальной задачей.

Анализ релевантных работ

Разработке методов анализа защищенности ИиТР сложных управляемых информационных и организационно-технических систем посвящено множество современных научных исследований [9–23]. В данных исследованиях сформулированы и детально описаны различные подходы к анализу защищенности. Вместе с тем практическое применение этих подходов для сравнительного анализа уровня защищенности различных ресурсов КВИ и для выработки перспективных направлений совершенствования защиты информации в КВИ становится проблематичным. В частности, это связано с учетом протекающих в КВИ переходных процессов, многокритериальным характером современных требований, предъявляемых к защищенности ИиТР КВИ и управлению процессом обеспечения информационной безопасности, которые обуславливают постановку не только векторной [9–11], но и динамической задачи анализа защищенности ресурсов инфраструктур такого класса, подходы к решению которой в рамках существующих методик не исследовались.

В работе [12] анализ защищенности предложено осуществлять с учетом алгоритмов управления рисками, но достоинства такого метода нивелируются большими вычислительными затратами, необходимыми на его практическую реализацию. Кроме того, предложенные в работах [13–15] частные методики анализа защищенности в подавляющем своем большинстве не обеспечивают учета параметров органов и процессов управления защитой ИиТР КВИ при разработке систем показателей защищенности (ПЗ) ресурсов такого класса. В случае, когда подобная задача все-таки решалась, например в работе [16], анализировались абсолютные значения ПЗ, но не учитывались значения отклонений этих ПЗ от требований к ним, что для анализа защищенности ресурсов таких сложных инфраструктур является существенным.

Из анализа работ [17–19] следует, что предусмотренный в существующих методиках сбор большого количества гетерогенных данных о состоянии ПЗ сложных технических систем обуславливает большие временные затраты на сбор статистики, что отрицательно влияет на оперативность анализа. Это, в свою очередь, влияет на время реакции подсистемы защиты ИиТР, увеличивает ее «время отклика» на реализуемые нарушителем угрозы и вводимые управляющие воздействия, ориентированные на инициацию тех или иных средств защиты ИиТР КВИ.

Особого внимания заслуживает анализ релевантных работ с точки зрения точности анализа защищенности. Так, например, в существующих методиках [20, 21] традиционный критерий точности – дисперсия ошибки оценивания – равна априорной дисперсии самого исследуемого процесса обеспечения защищенности ИиТР, что не может быть приемлемым для современных высокоточных систем контроля. Для повышения достоверности анализа ПЗ используются искусственные нейронные сети [22, 23]. Они позволяют учесть одну немаловажную грань неопределенности исходных данных – неполноту и противоречивость измерительной (наблюдаемой) информации о значениях ПЗ, но, к сожалению, не способны учесть нечеткость такой информации и ее «зашумленность». С другой стороны, исследования в интересах анализа защищенности сложных систем в условиях неопределенности хотя уже и проводились, но не были универсальными, они были посвящены в основном текущей оценке показателей безопасности информации в рамках одного какого-либо вида неопределенности (например, нечеткости) [24].

Таким образом, анализ релевантных работ позволяет говорить об объективной необходимости развития существующих методик анализа защищенности ИиТР КВИ на случай учета современных требований подсистемы управления безопасностью КВИ, требований должностных лиц (аудиторов, администраторов), связанных с длительностью циклов контроля защищенности и управления безопасностью систем такого класса. Иными словами, существует объективная необходимость в получении не точечных, а интервальных оценок ПЗ, анализ защищенности может и должен осуществляться с определенной периодичностью, должен учитывать все виды неопределенности исходных данных. Математической и методологической основой такого анализа могут выступать алгоритмы вычислений интервальных средних ПЗ ИиТР КВИ. Это позволит экономить вычислительный ресурс, повышать достоверность и адекватность анализа.

Теоретические аспекты построения алгоритмов вычислений интервальных средних значений уровней защищенности ИиТР КВИ

Инерционность циклов контроля защищенности ИиТР и процедур управления безопасностью информации, циркулирующей и хранящейся в КВИ, подчеркивает необходимость получения не точечных (мгновенных), а интервальных оценок защищенности. Важным элементом научной и практической новизны данных исследований, на наш взгляд, является тот факт, что их отличает от существующих работ наличие комплексной, двоякой – как «го-

ризонтальной», так и «вертикальной» – интервальности анализа. Иными словами, оценивание ПЗ ИиТР КВИ производится как на временных интервалах («по горизонтали»), так и определяются интервальные средние (нижние и верхние границы) значения параметров защищенности («по вертикали»). При этом интервальность во времени («горизонтальная») обеспечивается использованием математических моделей на основе непрерывных цепей Маркова, когда смена дискретных состояний (значений) ПЗ происходит в случайные моменты времени, но оценивается на заранее определенном временном интервале. А интервальность анализа ПЗ («вертикальная») обусловлена применением методов теории интервальных средних, позволяющих вычислять верхнее и нижнее средние значения (уровней) конкретного ПЗ ИиТР КВИ на этом интервале времени.

Рациональным методологическим и аналитическим инструментом для решения подобных задач, на наш взгляд, могут служить алгоритмы интервальных вычислений (интервального оценивания, вычислений интервальных средних), являющиеся одним из ключевых математических методов теории интервальных средних. Алгоритмы вычислений интервальных средних (АВИС) способны математически корректно объединить способы описания различных видов неопределенности, рассматривая их как частные случаи. С помощью АВИС можно обрабатывать разнородную неполную, нечеткую и противоречивую информацию [24–26].

Алгоритмы вычислений интервальных средних позволяют производить интервальные расчеты и получать итоговую интервальную оценку ПЗ ИиТР КВИ, причем физический смысл и порядок работы АВИС состоит в следующем. Исходными данными для работы АВИС являются заранее заданные временные интервалы Δt, в рамках которых будет осуществляться интервальный анализ ПЗ ИиТР КВИ. Эти интервалы Δt могут составлять от одной до 20 минут в зависимости от длительности цикла управления (инерционности управления) безопасностью ИиТР КВИ.

Следующий шаг работы АВИС – на множестве всех идентифицированных значений ПЗ путем анализа статистики за время Δt мгновенных (точечных, пошаговых) значений параметров защищенности ИиТР КВИ определяют показатели для каждого состояния защищенности $\psi(\Theta_n)$ на этом временном интервале. При этом в качестве ПЗ ИиТР КВИ могут выступать численные значения параметров, характеризующих различные аспекты информационной безопасности: доступность, конфиденциальность, целостность. Например, для конфиденциальности показателем защищенности может выступать время $\acute{A}_{\text{в. кп}}(\Delta t)$ взлома и компрометации паролей доступа к ИиТР; для доступности – время безопасного предоставления ИиТР $\acute{A}_{\text{б. пр}}(\Delta t)$ пользователям и подсистемам КВИ; для целостности – время восстановления доступа $\acute{A}_{\text{в. д}}(Dt)$ пользователей и подсистем КВИ к ИиТР после взлома и компрометации паролей [27].

Очередной шаг работы АВИС – вычисление верхнего и нижнего средних значений (уровней) конкретного ПЗ ИиТР КВИ на интервале времени Δt. Вычисление осуществляется на основе статистического анализа измеряемых и наблюдаемых на интервале Δt параметров защищенности с использованием математических выражений, лежащих в основе методов теории интервальных средних [25, 26]. Например, для конкретного ПЗ, характеризующего целостность ресурсов – времени восстановления доступа пользователей и подсистем КВИ к ИиТР после взлома и компрометации паролей – вычисляют точное верхнее $\overline{\acute{A}}_{\text{в. д}}(\Delta t)$ и нижнее $\underline{\acute{A}}_{\text{в. д}}(\Delta t)$ значение его среднего уровня, наблюдаемого на интервале времени Δt. Анализ, например, времени $\acute{A}_{\text{в. д}}(\Delta t)$ восстановления доступа пользователей и подсистем КВИ к ИиТР после взлома и компрометации паролей, с использованием АВИС, имеет ряд особенностей. В частности, предполагается, что ПЗ изначально имеет N возможных состояний (значений): $\{\Theta_1, \Theta_2, \ldots, \Theta_n, \ldots, \Theta_N\}$. При этом ПЗ для каждого состояния $\psi(\Theta_n)$ на интервале времени Δt определяется на множестве всех возможных состояний этого ПЗ ИиТР КВИ.

Вычисление верхнего и нижнего средних значений уровней защищенности ИиТР КВИ на интервале времени

Поиск верхнего и нижнего средних значений ПЗ ИиТР КВИ на определенном временном интервале также подчинен правилам работы АВИС: следующий шаг работы АВИС – в рамках нашего примера, для конкретного ПЗ, характеризующего целостность телекоммуникационных ресурсов (для времени восстановления доступа пользователей и подсистем КВИ к ИиТР после взлома и компрометации паролей), данный показатель $\acute{A}_{\text{в. д}}(\Delta t)$ на временном интервале Δt с использованием идентифицированных состояний (значений) вычисляется как

$$\acute{A}_{\text{в. д}}(Dt) = \sum_{n=1}^{N} \psi(Q_n)\, p_n(Dt) =$$

$$= (\psi(Q_1)\, p_1(Dt)) + (\psi(Q_2)\, p_2(Dt)) + \ldots + (\psi(Q_n)\, p_n(Dt)) + \ \ldots + (\psi(Q_N)\, p_N(Dt)),$$

где $\psi(\Theta_n)$ – показатель, который характеризует n-е (n = 1, … , N) состояние на интервале времени Δt; $p_n(\Delta t)$ – вероятность того, что конкретный ПЗ ИиТР КВИ $\text{Á}_{\text{в. д}}(\Delta t)$ на интервале времени Δt находится в состоянии (имеет идентифицированное значение) Θ_n.

Даже если вероятности $p_n(\Delta t)$ для данного конкретного ПЗ $\text{Á}_{\text{в. д}}(\Delta t)$ не определены, неизвестны, всегда существует возможность априори задать, определить на основе экспертного анализа верхнюю $\overline{\text{Á}}_{\text{в. д}}(\Delta t)$ и нижнюю $\underline{\text{Á}}_{\text{в. д}}(\Delta t)$ границы среднего уровня защищенности, в нашем случае – с точки зрения значений времени восстановления доступа пользователей и подсистем КВИ к ИиТР после взлома и компрометации паролей, наблюдаемых на интервале времени Δt. В этом случае ПЗ ИиТР КВИ ψ будет рассматриваться как некий «признак» (идентифицированный ПЗ), а функции $\overline{\text{Á}}_{\text{в. д}}(\Delta t)$ и $\underline{\text{Á}}_{\text{в. д}}(\Delta t)$ – как верхнее и нижнее средние этого признака. С точки зрения АВИС это можно записать математически как

$$\begin{cases} \overline{\text{Á}}_{\text{в. д}}(\Delta t) = \overline{\hat{\text{A}}}(\psi); \\ \underline{\text{Á}}_{\text{в. д}}(\Delta t) = \underline{\hat{\text{A}}}(\psi), \end{cases}$$

где $\overline{\hat{\text{A}}}(\psi)$ и $\underline{\hat{\text{A}}}(\psi)$ – верхнее и нижнее интервальные средние.

При этом АВИС предусматривают, что в случае полного отсутствия каких-либо априорных сведений о значениях ПЗ верхняя $\overline{\text{Á}}_{\text{в. д}}(\Delta t)$ и нижняя $\underline{\text{Á}}_{\text{в. д}}(\Delta t)$ границы среднего уровня защищенности равны единице и нулю соответственно $\hat{\text{A}}_{\text{в. д}}(f)$ [25]:

$$\begin{cases} \overline{\text{Á}}_{\text{в. д}}(\Delta t) = 1; \\ \underline{\text{Á}}_{\text{в. д}}(\Delta t) = 0. \end{cases}$$

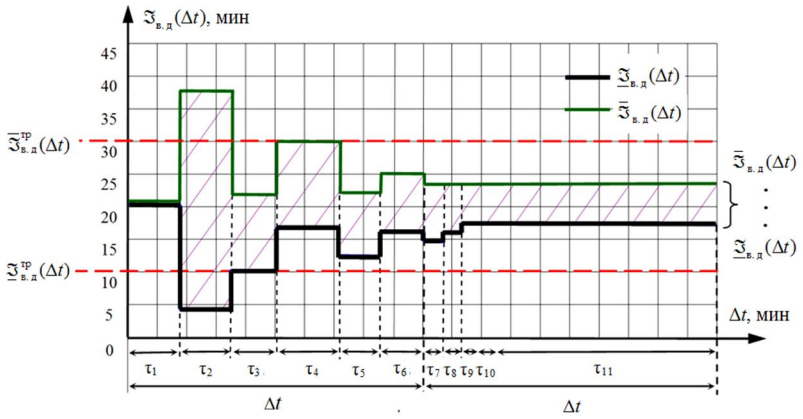
С учетом того, что в рамках АВИС «признаком» случайного события (случайной переменной) принято называть произвольную числовую функцию $f(y)$ (причем $y \in Y$, а Y – пространство элементарных исходов значений ПЗ), в нашем случае «признаком» выступает уровень (значение) конкретного ПЗ ИиТР КВИ на интервале времени Δt.

Тогда понятие «интервальные средние» адекватно характеризует верхний и нижний средние уровни защищенности ИиТР КВИ на интервале времени Δt, а для конкретного ПЗ, например времени $\text{Á}_{\text{в. д}}(\Delta t)$ восстановления доступа пользователей и подсистем КВИ к ИиТР после взлома и компрометации паролей, можно определить его «точное» среднее $\hat{\text{A}}_{\text{в. д}}(f)$ [25]:

$$\hat{\text{A}}_{\text{в. д}}(f) = \int_Y f(y)\,dF(y),$$

где $F(y)$ – функция распределения случайной переменной – значений ПЗ, а интервальным средним нашего конкретного «признака» называется интервал $[\hat{\text{A}}_{\text{в. д}}(f) \dots \overline{\hat{\text{A}}}_{\text{в. д}}(f)]$, который без учета понятия «признак» можно записать $[\underline{\text{Á}}_{\text{в. д}}(\Delta t) \dots \overline{\text{Á}}_{\text{в. д}}(\Delta t)]$.

Частный пример применения методов теории интервальных средних с точки зрения определения «точного» среднего в рамках интервала $[\underline{\text{Á}}_{\text{в. д}}(\Delta t) \dots \overline{\text{Á}}_{\text{в. д}}(\Delta t)]$ для времени восстановления доступа пользователей и подсистем КВИ к ИиТР после взлома и компрометации паролей приведен на рис.



Графическая интерпретация определения «точного» интервального среднего времени $\text{Á}_{\text{в. д}}(\Delta t)$ восстановления доступа пользователей и подсистем КВИ к ИиТР после взлома и компрометации паролей

Graphical interpretation of determining “accurate” midvalue mean time $\text{Á}_{\text{в. д}}(\Delta t)$ of restoring access of users and subsystems of critical infrastructure (CI) to information and telecommunication resources (ITR) after hacking and password compromising

Графики иллюстрируют, что при априори неизвестной функции распределения $F(y)$ возможно вести разговор только о «границах» $\underline{F}(y) \le F(y) \le \overline{F}(y)$ для всех значений $y \in Y$, а в пределах

$$\hat{\underline{A}}_{в.д}(f) \le \hat{A}_{в.д}(f) \le \hat{\overline{A}}_{в.д}(f),$$

характеризующих верхнюю $\overline{A}_{в.д}(\Delta t)$ и нижнюю $\underline{A}_{в.д}(\Delta t)$ интервальные средние,

$$\underline{A}_{в.д}(\Delta t) \le A_{в.д}(\Delta t) \le \overline{A}_{в.д}(\Delta t)$$

находится «точное» среднее для конкретного ПЗ ИиТР КВИ, в нашем примере – для времени $A_{в.д}(\Delta t)$ восстановления доступа пользователей и подсистем КВИ к ИиТР после взлома и компрометации паролей.

Анализ графиков (см. рис.) позволяет увидеть, что с учетом начального, стартового времени восстановления доступа пользователей $A_{в.д}(\Delta t)$ = 20 мин (заданного в качестве примера), состояние $A_{в.д}(\Delta t)$ может принимать значения от 0 до 45 мин, и его оценка достигает стабильного состояния уже на 8-м шаге (τ_8) функционирования и на 2-м шаге (временном отрезке) интервального анализа Δt.

Графики, помимо наблюдения за сменой оценочных интервальных значений $A_{в.д}(\Delta t)$ (т. е. за его переходом из одного состояния в другое в случайные интервалы времени τ), позволяют получить ответ на вопрос, имеющий важное значение для анализа защищенности: находятся ли полученные интервальные нижнее $\underline{A}_{в.д}(\Delta t)$ и верхнее $\overline{A}_{в.д}(\Delta t)$ значения анализируемого ПЗ ИиТР КВИ (заштрихованный сектор) в границах допустимых, требуемых средних нижних $\underline{A}^{тр}_{в.д}(\Delta t)$ и верхних $\overline{A}^{тр}_{в.д}(\Delta t)$ значений, задаваемых политикой безопасности организации или администратором безопасности критически важных инфраструктур.

Заключение

Таким образом, существует практическая возможность анализа защищенности ИиТР КВИ с учетом современных требований подсистем управления безопасностью КВИ, требований должностных лиц (аудиторов, администраторов безопасности), связанных с инерционностью процессов принятия решения, с длительностью циклов контроля защищенности и управления безопасностью систем такого класса. Рассмотренный подход базируется на алгоритмах вычислений интервальных средних и позволяет получать не точечные (мгновенные), а интервальные оценки показателей защищенности, при этом анализ защищенности осуществляется с заранее заданной периодичностью и учитывает неопределенность исходных данных.

Предложенный методологический подход не обладает большой математической и вычислительной сложностью, но позволяет получить адекватные задачам контроля и управления интервальные оценки защищенности ресурсов КВИ, при этом учесть неопределенность наблюдаемых и управляемых параметров защищенности и экономить вычислительный ресурс, что в конечном итоге позволяет повысить достоверность анализа безопасности современных критически важных инфраструктур.

Список источников

1. *Setola R., Luiijf E., Theoharidou M.* Critical Infrastructures, Protection and Resilience // Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control. Springer, 2016. P. 1–18.

2. *Cogwell M. T.* Critical Infrastructures. N.Y.: Nova Publishers, 2003. 143 p.

3. *Блюмин А. М., Феоктистов Н. А.* Мировые информационные ресурсы: учеб. пособие. М.: Дашков и К°, 2010. 296 с.

4. *О безопасности* критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ. М. 36 с. URL: http://www.kremlin.ru/acts/bank/42128 (дата обращения: 15.01.2022).

5. *Гребешков А. Ю.* Вычислительная техника, сети и телекоммуникации: учеб. пособие для вузов. М.: Горячая линия-Телеком, 2016. 190 с.

6. *Bouras C. J.* Trends in Telecommunications Technologies. Patras (Greece): InTech, 2010. 778 p.

7. *Kotenko I. V., Parashchuk I. B.* Evaluation of Information Security of Industrial Automation Systems Using Fuzzy Algorithms and Predicates // International Russian Automation Conference (RusAutoCon), Sochi, Russia (5-11 Sept. 2021). IEEE Xplore Digital Library: Browse Conferences, 2021. V. (Doc.) 9537332. P. 261–266.

8. *Kotenko I., Stepashkin M., Doynikova E.* Security Analysis of Information Systems taking into account Social Engineering Attacks // Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011). 2011. P. 611–618.

9. *Kamara M. K.* Securing Critical Infrastructures. Bloomington: Xlibris US, 2020. 385 p.

10. *Complying* with the European NIS Directive // Cybersecurity for critical infrastructures. KPMG, 2019. 8 p.

11. *Erbach G.* Cybersecurity of critical energy infrastructure. EPRS, European Parliament, 2019. 13 p.

12. *Arnold R.* Cybersecurity: A Business Solution: An executive perspective on managing cyber risk. Winston-Salem: Threat Sketch, LLC, 2017. 100 p.

13. *O'Neil M. J., Dempsey J. X.* Critical infrastructure protection: Threats to privacy and other civil liberties and

concerns with government mandates or industry // Depaul Business Law Journal. 2000. N. 12. P. 97–111.

14. *Kotenko I., Saenko I., Branitskiy A.* Machine Learning and Big Data Processing for Cybersecurity Data Analysis // Data Science in Cybersecurity and Cyberthreat Intelligence. Cham: Springer, 2020. V. 177. P. 61–85.

15. *Al-Mhiqani M. N.* Cyber-security incidents: a review cases in cyber-physical systems // International Journal of Advanced Computer Science and Applications. 2018. N. 1. P. 499–508.

16. *Doynikova E., Fedorchenko A., Kotenko I.* A Semantic model for security evaluation of information systems // Journal of Cyber Security and Mobility. 2019. V. 9 (2). P. 301–330.

17. *NIST* Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide, January 16, 2020. URL: https://www.nist.gov/privacy-framework/nist-sp-800-61 (дата обращения: 14.01.2022).

18. *ISO/IEC 27043:2015* Information technology. Security techniques. Incident investigation principles and processes, 2015-03. URL: https://www.iso.org/ru/standard/44407.html (дата обращения: 15.01.2022).

19. *Ekpo U.* Introduction to Cyber Security. Fundamentals. N. Y.: Independently published, 2018. 92 p.

20. *Gabber H*. The 2020 CyberSecurity & Cyber Law Guide. N. Y.: Independently published, 2020. 435 p.

21. *Arthur C*. Cyber Wars. Hacks that Shocked the Business World. L.: Kogan Page, 2018. 246 p.

22. *Desnitsky V. A., Kotenko I. V., Parashchuk I. B.* Neural Network Based Classification of Attacks on Wireless Sensor Networks // 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (27-30 Jan. 2020, St. Petersburg and Moscow, Russia, 2020). IEEE Xplore Digital Library (19 March 2020). P. 284–287. DOI: 10.1109/EIConRus49466.2020.9039275.

23. *Meeuwisse R.* Cybersecurity Exposed: The Cyber House Rules. L.: Cyber Simplicity Ltd., 2017. 175 p.

24. *Авраменко В. С., Бушуев С. Н.* Оценка защищенности информации на основе теории нечетких множеств // Вопр. радиоэлектроники. 2014. Т. 3. № 1. С. 142–148.

25. *Гуров С. В., Уткин Л. В.* Надежность систем при неполной информации. СПб.: Любавич, 1999. 160 с.

26. *Alefeld G., Mayer G*. Interval analysis: theory and applications // Journal of Computational Applied Mathematics. 2000. V. 121. P. 421–464.

27. *Десницкий В. А., Паращук И. Б.* Показатели доступности, целостности и конфиденциальности данных пользователей беспроводных сенсорных сетей в интересах анализа и обеспечения их защищенности // Информационная безопасность регионов России (ИБРР-2019): материалы XI Санкт-Петербург. межрегион. конф. (Санкт-Петербург, 23–25 октября 2019 г.). СПб.: Изд-во СПОИСУ, 2019. С. 114–116.

References

1. Setola R., Luiijf E., Theoharidou M. Critical Infrastructures, Protection and Resilience. *Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control*. Springer, 2016. Pp. 1-18.

2. Cogwell M. T. *Critical Infrastructures*. New York, Nova Publishers, 2003. 143 p.

3. Bliumin A. M., Feoktistov N. A. *Mirovye informatsionnye resursy: uchebnoe posobie* [World information resources: textbook]. Moscow, Dashkov i K° Publ., 2010. 296 p.

4. *O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii. Federal'nyi zakon ot 26 iiulia 2017 g. № 187-FZ* [On security of the critical information infrastructure of the Russian Federation. Federal Law of July 26, 2017 No. 187-FZ]. Moscow, 36 p. Available at: http://www.kremlin.ru/acts/bank/42128 (accessed: 15.01.2022).

5. Grebeshkov A. Iu. *Vychislitel'naia tekhnika, seti i telekommunikatsii: uchebnoe posobie dlia vuzov* [Computer engineering, networks and telecommunications: textbook for universities]. Moscow, Goriachaia liniia-Telekom, 2016. 190 p.

6. Bouras S. J. *Trends in Telecommunications Technologies*. Patras (Greece), InTech, 2010. 778 p.

7. Kotenko I. V., Parashchuk I. B. Evaluation of Information Security of Industrial Automation Systems Using Fuzzy Algorithms and Predicates. *International Russian Automation Conference (RusAutoCon), Sochi, Russia (5-11 Sept. 2021)*. IEEE Xplore Digital Library: Browse Conferences, 2021. Vol. (Doc.) 9537332. Pp. 261-266.

8. Kotenko I., Stepashkin M., Doynikova E. Security Analysis of Information Systems taking into account Social Engineering Attacks. *Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2011)*. 2011. Pp. 611-618.

9. Kamara M. K. *Securing Critical Infrastructures*. Bloomington, Xlibris US, 2020. 385 p.

10. Complying with the European NIS Directive. *Cybersecurity for critical infrastructures*. KPMG, 2019. 8 p.

11. Erbach G. *Cybersecurity of critical energy infrastructure*. EPRS, European Parliament, 2019. 13 p.

12. Arnold R. *Cybersecurity: A Business Solution: An executive perspective on managing cyber risk.* Winston-Salem, Threat Sketch, LLC, 2017. 100 p.

13. O'Neil M. J., Dempsey J. X. Critical infrastructure protection: Threats to privacy and other civil liberties and concerns with government mandates or industry. *Depaul Business Law Journal*, 2000, no. 12, pp. 97-111.

14. Kotenko I., Saenko I., Branitskiy A. Machine Learning and Big Data Processing for Cybersecurity Data Analysis // Data Science in Cybersecurity and Cyberthreat Intelligence. Cham, Springer, 2020. Vol. 177. Pp. 61-85.

15. Al-Mhiqani M. N. Cyber-security incidents: a review cases in cyber-physical systems. *International Journal of Advanced Computer Science and Applications*, 2018, no. 1, pp. 499-508.

16. Doynikova E., Fedorchenko A., Kotenko I. A Semantic model for security evaluation of information systems. *Journal of Cyber Security and Mobility*, 2019, vol. 9 (2), pp. 301-330.

17. *NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide, January 16, 2020*. Available at: https://www.nist.gov/privacy-framework/nist-sp-800-61 (accessed: 14.01.2022).

18. *ISO/IEC 27043:2015 Information technology. Security techniques. Incident investigation principles and processes, 2015-03*. Available at: https://www.iso.org/ru/standard/44407.html (accessed: 15.01.2022).

19. Ekpo U. *Introduction to Cyber Security. Fundamentals*. New York, Independently published, 2018. 92 p.

20. Gabber H. *The 2020 CyberSecurity & Cyber Law Guide*. New York, Independently published, 2020. 435 p.

21. Arthur C. *Cyber Wars. Hacks that Shocked the Business World*. London, Kogan Page, 2018. 246 p.

22. Desnitsky V. A., Kotenko I. V., Parashchuk I. B. Neural Network Based Classification of Attacks on Wireless Sensor Networks. *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (27-30 Jan. 2020, St. Petersburg and Moscow, Russia, 2020). IEEE Xplore Digital Library (19 March 2020).* Pp. 284-287. DOI: 10.1109/EIConRus49466.2020.9039275.

23. Meeuwisse R. *Cybersecurity Exposed: The Cyber House Rules*. London, Cyber Simplicity Ltd., 2017. 175 p.

24. Avramenko V. S., Bushuev S. N. Otsenka zashchishchennosti informatsii na osnove teorii nechetkikh mnozhestv [Estimation of information security based on fuzzy sets theory]. *Voprosy radioelektroniki*, 2014, vol. 3, no. 1, pp. 142-148.

25. Gurov S. V., Utkin L. V. *Nadezhnost' sistem pri nepolnoi informatsii* [Reliability of systems with incomplete information]. Saint-Petersburg, Liubavich Publ., 1999. 160 p.

26. Alefeld G., Mayer G. Interval analysis: theory and applications. *Journal of Computational Applied Mathematics*, 2000, vol. 121, pp. 421-464.

27. Desnitskii V. A., Parashchuk I. B. Pokazateli dostupnosti, tselostnosti i konfidentsial'nosti dannykh pol'zovatelei besprovodnykh sensornykh setei v interesakh analiza i obespecheniia ikh zashchishchennosti [Parmeters of availability, integrity and confidentiality of data of users of wireless sensor networks in terms of analysis and ensuring their security]. *Informatsionnaia bezopasnost' regionov Rossii (IBRR-2019): materialy XI Sankt-Peterburgskoi mezhregional'noi konferentsii (Sankt-Peterburg, 23–25 oktiabria 2019 g.).* Saint-Petersburg, Izd-vo SPOISU, 2019. Pp. 114-116.

Статья поступила в редакцию 19.01.2022; одобрена после рецензирования 28.02.2022; принята к публикации 01.04.2022
The article is submitted 19.01.2022; approved after reviewing 28.02.2022; accepted for publication 01.04.2022

Информация об авторах / Information about the authors

Игорь Витальевич Котенко – доктор технических наук, профессор; заведующий лабораторией проблем компьютерной безопасности; Санкт-Петербургский Федеральный исследовательский центр Российской академии наук; ivkote@comsec.spb.ru

Игорь Борисович Паращук – доктор технических наук, профессор; ведущий научный сотрудник лаборатории проблем компьютерной безопасности; Санкт-Петербургский Федеральный исследовательский центр Российской академии наук; shchuk@rambler.ru

Igor V. Kotenko – Doctor of Technical Sciences, Professor; Head of the Laboratory of Computer Security Problems; St. Petersburg Federal Research Center of the Russian Academy of Sciences; ivkote@comsec.spb.ru

Igor B. Parashchuk – Doctor of Technical Sciences, Professor; Leading Researcher of the Laboratory of Computer Security Problems; St. Petersburg Federal Research Center of the Russian Academy of Sciences; shchuk@rambler.ru