И. Б. ПАРАЩУК, И. В. КОТЕНКО
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
Санкт-Петербург

ОПЕРАТИВНАЯ ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ РЕСУРСОВ НА ОСНОВЕ ДВУХЭТАПНОЙ ОБРАБОТКИ НЕОПРЕДЕЛЕННЫХ ИСХОДНЫХ ДАННЫХ

В докладе предложен подход к реализации двухэтапной процедуры устранения неопределенности (неполноты и противоречивости) оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов. Рассмотрены различные виды неопределенности исходных данных, необходимых для реализации процесса оценки. Предложенный подход позволяет повысить достоверность оперативного анализа защищенности за счет поэтапного применения методов и алгоритмов обработки неполных, противоречивых и нечетких знаний и данных.

Введение. Непростая задача создания и внедрения эффективного комплекса мер по поддержанию высокого уровня защищенности информационных, телекоммуникационных и других критически важных ресурсов страны по-прежнему стоит сегодня перед государством, обществом и конкретными профильными специалистами. Ключевую роль при решении этой задачи играет предварительная или динамическая оперативная оценка защищенности объектов такого класса. Оперативная и достоверная оценка позволяет построить адекватную защиту таких ресурсов, а значит, поставить надежный заслон нарушителям [1–3].

Под информационным ресурсом понимается вся совокупность данных, организованных для эффективного получения достоверной информации в интересах обеспечения бесперебойного функционирования критически важных инфраструктур. Это совокупность отдельных документов и массивов документов, а также множество документов и массивов документов в информационных подсистемах критически важных инфраструктур – библиотеках, архивах, фондах, банках данных и других информационных подсистемах [4, 5].

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

При этом задачи оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов в условиях неопределенности исходных данных заслуживают особого внимания. Они являются ключевым вопросом теории и практики управления защитой данных в системах такого класса и основой обеспечения их безопасного функционирования.

Весь практический опыт в области получения достоверных оценок защищенности сложных технологических систем, оценок показателей информационной безопасности телекоммуникационных сетей и систем показывает, что объективный и оперативный анализ защищенности невозможен без предварительной обработки исходных данных и, соответственно, получаемых на ее основе выводов в условиях неопределенности, без привлечения алгоритмов анализа противоречивых и динамичных (изменяющихся) данных о текущих значениях параметров безопасности. Использование таких методов и алгоритмов позволяет повысить достоверность оценки защищенности информационных и телекоммуникационных ресурсов за счет дополнительной обработки неполных, противоречивых и нечетких исходных данных, а значит, в конечном итоге, повысить обоснованность принимаемых решений по реализации политики безопасности [7].

Рассматривается гипотеза, заключающаяся в том, что методы и алгоритмы обработки неполных, противоречивых и нечетких исходных данных для задач оперативной оценки защищенности могут быть использованы в комплексе. При этом задача интеграции и объединенного использования моделей, алгоритмов и методов обработки неполных, противоречивых и нечет-

ких исходных данных в интересах устранения неполноты и противоречивости оперативной оценки защищенности информационных и телекоммуникационных ресурсов, решается в такой постановке впервые. Данные исследования являются дальнейшим развитием методологии оценки параметров различных сложных информационно-технических объектов, производственных и телекоммуникационных процессов, а также процессов принятия решения в условиях различного вида неопределенности. При этом под неопределенностью понимают недостаточную осведомленность людей и подсистем, которые принимают решения на управление. Это неполное или неточное представление о текущих значениях различных параметров защищенности информационных и телекоммуникационных ресурсов, порождаемое различными причинами и, прежде всего, неполнотой или неточностью информации об условиях контроля защищенности [8].

Этапы повышения достоверности оперативной оценки защищенности информационных и телекоммуникационных ресурсов. Обработку неопределенных исходных данных в интересах оперативной оценки защищенности информационных и телекоммуникационных ресурсов предлагается реализовать раздельно для различных типов неопределенности, и на различных этапах, например: с помощью методов теории нечетких множеств [9, 10]; искусственных нейронных сетей [11, 12], либо нейро-нечетких сетей [13–14].

В этой связи особую роль приобретают алгоритмы достоверной, оперативной, многоаспектной и, как минимум, двухэтапной оценки защищенности информационных и телекоммуникационных ресурсов. На основе этих алгоритмов (двухэтапных процедур устранения неопределенности) предлагается обрабатывать неполные, противоречивые или нечеткие исходные данные. Особенность таких алгоритмов в рамках оперативной оценки защищенности информационных и телекоммуникационных ресурсов заключается в том, что анализ осуществляются в условиях неопределенности различного характера и физической природы. Например, в условиях неполноты, противоречивости или нечеткости данных о реальных, истинных текущих значениях параметров защищенности. Другими словами, такие алгоритмы обеспечивают повышение достоверности оценки защищенности на основе обработки неполных, противоречивых и нечетких исходных данных.

Для этого на основе мнений экспертов и аналитических преобразований нечетких и неполных (противоречивых) данных о среде (природная неопределенность), стратегиях противодействия (неопределенность поведения), целях работы (неопределенность цели) и о предпочтениях, оказываемых тем или иным аспектам защищенности, которые необходимо оценить, осуществляется дополнительная обработка исходных данных.

В рамках оперативной оценки защищенности информационных и телекоммуникационных ресурсов на основе двухэтапной обработки неопределенных исходных данных (двухэтапных процедур устранения неопределенности), первым реализуется этап, ориентированный на наличие в исходных данных неопределенности, имеющей характер неоднозначности (нечеткости). Такие задачи обычно решаются на основе математики нечетких множеств.

Процедура преобразования данных на основе математики нечетких множеств подробно описана в работе [9]. Данный («нечеткий») этап подразумевает отказ от применения классических математических методов, ориентированных на стандарты точности и строгости, отказ от языка математики уравнений, а использование математического языка, основанного на понятиях нечетких множеств и лингвистических переменных. На «нечетком» этапе процедуры обработки неопределенных исходных данных на основе мнений, предпочтений экспертов и лиц, принимающих решения, а также на основе аналитических преобразований этих нечетких данных реализуются подэтапы повышения достоверности оперативной оценки защищенности: начиная с формулировки функций принадлежности нечетких множеств, характеризующих нечетко заданные данные для оценки защищенности информационных и телекоммуникационных ресурсов, и заканчивая формулировкой результатов «нечеткой» оценки – выводом классов подобия оценок показателей защищенности ресурсов и полученной системы непересекающихся подмножеств таких оценок.

При оперативной оценке защищенности информационных и телекоммуникационных ресурсов с использованием двухэтапной обработки неопределенных исходных данных, вторым по очереди реализуется этап, ориентированный на наличие в таких исходных данных неопределенности, имеющей характер недостаточности (неполноты). Подобные задачи принято решать

на основе математики искусственных нейронных сетей. При этом состояние нейронов входного, промежуточного, либо выходного слоя нейронной сети имеет физический смысл наличия или отсутствия в конкретном наборе исходных данных (например, в конкретном множестве измеренных параметров защищенности) признаков угроз безопасности для конкретных информационных и/или телекоммуникационных ресурсов. Механизм преобразований и физический смысл процесса работы с недостаточными (неполными) данными для примера однослойной нейронной сети детально описан в работе [12].

Процедуры второго этапа преобразования неопределенных исходных данных в интересах повышения достоверности оперативной оценки защищенности основаны на возможности обработки неполных и противоречивых данных и экспертных мнений об этих данных с помощью методов теории искусственный нейронных сетей. Для нашего конкретного примера, когда характер информации о наличии или отсутствии в конкретном наборе исходных данных признаков угроз безопасности для конкретных информационных и/или телекоммуникационных ресурсов не связан с лингвистической и физической неопределенностью, одним из действенных и математически корректных подходов к обработке неполной и противоречивой информации является использование нейросетевых алгоритмов идентификации данных. При этом на «нейросетевом» этапе процедуры обработки неопределенных исходных данных на основе нейросетевых методов повышения достоверности реализуются как подэтапы синтеза данных для нейронной сети, генерации входного слоя нейронной сети, так и определение наличия или отсутствия в конкретном наборе исходных данных (например, в конкретном множестве измеренных параметров защищенности) признаков угроз безопасности для конкретных информационных и/или телекоммуникационных ресурсов.

В результате последовательной реализации рассмотренных двух этапов процедуры повышения достоверности оперативной оценки защищенности информационных и телекоммуникационных ресурсов с учетом неопределенности, опираясь на функции принадлежности нечетких множеств и синаптические веса нейронных сетей, сформулированные с учетом анализа исходных данных, предпочтений экспертов и текущих потребностей в количественных оценочных значениях параметров защищенности, могут быть получены варианты непересекающихся множеств оценок параметров защищенности, может быть получен ряд оценок, безусловно характеризующих однозначное наличие или отсутствие в конкретном наборе исходных данных (например, в конкретном множестве измеренных параметров защищенности) признаков угроз безопасности для конкретных информационных и/или телекоммуникационных ресурсов.

Заключение. Таким образом, необходимость решения задач оперативной оценки защищенности информационных и телекоммуникационных ресурсов в среде не только многокритериальности, но и неопределенности, обуславливает актуальность решения задачи повышения достоверности такой оценки с безусловным учетом разнородной и разноплановой неопределенности условий анализа защищенности, вызванной нестационарностью функционирования критически важных инфраструктур, использующих и предоставляющих пользователям эти ресурсы, воздействиями дестабилизирующих (часто антагонистических) факторов, внешней среды, нечеткостью целей и несогласованностью задач оценки защищенности и др. Проведенный анализ показывает, что на современном этапе недостаточно развиты алгоритмы оперативной оценки защищенности информационных и телекоммуникационных ресурсов в условиях нестохастической неопределенности исходных данных, а именно, неоднозначности (нечеткости) и недостаточности (неполноты и противоречивости) исходной информации для объективного контроля.

Предложен подход на основе двухэтапной обработки (двухэтапных процедур устранения неопределенности) данных, он базируется на реализации алгоритмов поэтапного устранения неоднозначности (нечеткости), неполноты и противоречивости исходных данных, необходимых для оперативной оценки защищенности информационных и телекоммуникационных ресурсов. Предложенный подход позволяет повысить достоверность оценки защищенности за счет применения методов и алгоритмов предварительной обработки неполных, противоречивых и нечетких исходных данных.

Возможным направлением предполагаемых дальнейших исследований может быть синтез общей архитектуры системы контроля защищенности сложных информационно-технических систем и генерируемого ими цифрового сетевого контента.

Работа проводилась при поддержке гранта РНФ (проект № 21-71-20078) в СПб ФИЦ РАН.

ЛИТЕРАТУРА

1. **Котенко И.В., Котухов М.М., Марков А.С.** и др. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под редакцией И.В. Котенко. Санкт-Петербург, 2000. 190 с.
2. **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.
3. **Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В.** Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра. *Труды СПИИРАН*. 2016. № 5 (48). С. 5–31.
4. **Блюмин А.М., Феоктистов Н.А.** Мировые информационные ресурсы: Учебное пособие М.: Издательско-торговая корпорация «Дашков и К°», 2010. 296 с.
5. Basch E.M., Thaler H.T., Shi W., Yakren S., Schrag D. Use of information resources by patients with cancer and their companions. *Cancer: Interdisciplinary International Journal of the American Cancer Society*, 100(11), 2004. P. 2476–2483.
6. Bouras C.J. Trends in Telecommunications Technologies. Patras: (Greece), InTech, 2010. 778 p.
7. 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.
8. **Паращук И.Б., Башкирцев А.С., Михайличенко Н.В.** Анализ уровней и видов неопределенности, влияющей на принятие решений по управлению информационными системами. *Информация и космос*. №1, 2017. С. 112–120.
9. Kosko B. Neural Networks and Fuzzy Systems. A Dynamical Systems Approach to Machine Intelligence. *Englewood Cliffs: Prentice-Hall*, 1992. 346 p.
10. Kotenko I.B., Saenko I.B., Ageev S.A., Kopchak Y.M. Abnormal Traffic Detection in networks of the Internet of things based on fuzzy logical inference. *XVIII International Conference on Soft Computing and Measurements* (SCM'2015) IEEE Xplore. 2015. P. 5–8.
11. Kriesel D. A Brief Introduction to Neural Networks. Cambridge: Cambridge Press, 2010. 226 p.
12. **Паращук И.Б., Иванов Ю.Н., Романенко П.Г.** Нейросетевые методы в задачах моделирования и анализа эффективности функционирования сетей связи: Учебно-методическое пособие. СПб.: ВАС, 2010. 103 с.
13. **Булдакова Т.И., Миков Д.А.** Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели. // Наука и образование. № 11, 2013. // [Электронный ресурс]: http://technomag.edu.ru/doc/645489.html. (дата обращения 16.05.2022).
14. **Паращук И.Б., Михайличенко Н.В.** Нейро-нечеткие модели в интересах управления данными в ЦОД и интеллектуального анализа информации в региональных телекоммуникационных сетях. *Юбилейная XV-ая Санкт-Петербургская Международная Конференция «Региональная информатика-2016 (РИ-2016)»*. Материалы конференции. СПб.: СПОИСУ, 2016г. 599 с., С. 117–118.

I.B.Parashchuk, I.V.Kotenko (St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg)

Operational assessment of the security of information and telecommunications resources based on two-stage processing of uncertain source data

The report proposes an approach to the implementation of a two-stage procedure for eliminating uncertainty (incompleteness and inconsistency) of the operational assessment of the security of information, telecommunications and other critical resources. Various types of uncertainty of the initial data necessary for the implementation of the evaluation process are considered. The proposed approach makes it possible to increase the reliability of operational security analysis through the phased application of methods and algorithms for processing incomplete, contradictory and fuzzy knowledge and data.

Авторы готовы представить текст на английском языке для сборника материалов мультиконференции, который будет подан для индексирования в Scopus