DOI: 10.25586/RNU.V9187.21.03.P.091 УДК 658

Е.П. Грабчак, Е.Л. Логинов

СОЗДАНИЕ НОВЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ МОНИТОРИНГА И ДИАГНОСТИКИ: ОБНАРУЖЕНИЕ ЛАТЕНТНЫХ АТАК НА ЦИФРОВЫЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТОВ

Рассматриваются проблемы обеспечения безопасности информационно-управляющих систем энергетических объектов. Обоснована необходимость разработки масштабируемого по производительности программно-аппаратного комплекса автоматизированного мониторинга и диагностики с нейросетевой компонентой. Сформулированы ключевые характеристики комплекса, решаемые задачи, архитектура, основные методы анализа данных для выявления признаков несанкционированного вмешательства в работу функциональных узлов энергетического оборудования. Показана эффективность нейронных сетей в задачах идентификации атаки, формирования стратегии блокирования атаки, принятия решения о введении режима критической ситуации с переходом на технические средства непрограммируемой логики, а также прогнозирования поведения целевых функциональных узлов оборудования энергетических объектов для последующего возврата в штатные режимы и восстановления работоспособности оборудования.

Ключевые слова: энергетика, информационно-управляющие системы, атаки, мониторинг, анализ, нейросетевые технологии, безопасность.

E.P. Grabchak, E.L. Loginov

CREATION OF NEW AUTOMATED MONITORING SYSTEMS AND DIAGNOSTICS: DETECTION OF LATENT ATTACKS ON DIGITAL INFORMATION AND CONTROL SYSTEMS OF ENERGY FACILITIES

The article deals with the problems of ensuring the safety of information and control systems of power facilities. The necessity of developing a performance-scalable software and hardware complex for automated monitoring and diagnostics with a neural network component has been substantiated. The key characteristics of the complex, the tasks to be solved, the architecture, the main methods of data analysis to identify signs of unauthorized interference in the operation of functional units of power equipment are formulated. The effectiveness of neural networks in the tasks of identifying an attack, forming a strategy for blocking an attack, deciding on the introduction of a critical situation mode with the transition to technical means of non-programmable logic, as well as predicting the behavior of target functional units of equipment of energy facilities for the subsequent return to normal modes and restoration of equipment operability is shown.

Keywords: energy, information management systems, attacks, monitoring, analysis, neural network technologies, security.

Введение

В последний период в энергетике в связи с цифровизацией актуализировался новый спектр сложных задач обнаружения латентных, сложно выявляемых атак на цифровые информационно-управляющие системы энергетических объектов [1; 2; 6]. Для противодействия этим атакам предлагается использовать нейросетевые технологии в рамках автоматизированных систем мониторинга и диагностики [8; 9]. Совокупность программных средств, реализующих нейросетевые алгоритмы решения задач мониторинга и диагно-

© Е.П. Грабчак, Е.Л. Логинов, 2021

Грабчак Евгений Петрович
кандидат экономических наук, заместитель министра энергетики Российской Федерации, Москва. Сфера научных интересов: энергетика, информатика, безопасность. Автор 102 опубликованных научных работ.
E-mail: grabchak.eug@gmail.com

Логинов Евгений Леонидович
доктор экономических наук, профессор РАН, дважды лауреат Премии Правительства РФ в области науки и техники, начальник экспертно-аналитической службы Ситуационно-аналитического центра Минэнерго России, Москва. Сфера научных интересов: энергетика, информатика, безопасность. Автор 589 опубликованных научных работ.
E-mail: loginovel@mail.ru

стики для обнаружения и парирования некорректного поведения интеллектуальных элементов информационно-управляющих систем вследствие латентных, сложно выявляемых атак, и адекватных им аппаратных средств, представляет собой нейросетевую систему.

Описание комплекса

Нейросетевая компонента программно-аппаратного комплекса автоматизированного мониторинга и диагностики ориентирована на решение широкого круга задач интеллектуального анализа поступающих данных для выявления признаков несанкционированного вмешательства в работу функциональных узлов энергетического оборудования. Программная среда, реализующая функции мониторинга и диагностики с опорой на специализированные средства аппаратной поддержки, интегрированно формирует программно-аппаратный комплекс.

Нейросетевые компоненты в составе программно-аппаратного комплекса автоматизированного мониторинга и диагностики позволяют увеличить его производительность [15; 20].

Среди прочих наиболее реально и интенсивно развивающихся технологий анализа и моделирования выделяются нейросетевые технологии, которые принципиально строятся на параллельности выполняемых операций [19]. При этом, как показывает анализ зарубежных и отечественных публикаций, использование нейросетевых технологий в рамках автоматизированных систем мониторинга и диагностики позволяет добиться уменьшения на порядок времени счета при использовании одинаковых вычислительных средств [18; 21].

Подобная архитектура позволяет не только удовлетворить требованиям интеллектуального анализа больших и сверхбольших объемов данных, но и достаточно просто реализовать масштабируемость вычислительной мощности в зависимости от характеристик решаемых классов задач мониторинга и диагностики для обнаружения и парирования некорректного поведения интеллектуальных элементов информационно-управляющих систем вследствие латентных, сложно выявляемых атак (в том числе наиболее опасных сетевых попыток перехвата управления).

Отдельным вопросом является разработка базовых средств классификации, распознавания и кластеризации данных при обнаружении атак и поиска скрытых аномальных закономерностей в потоках и массивах технологических данных, включая выявление ин-

формативного обобщенного параметра состояния объекта и выработки управляющих сигналов стабилизации работы его оборудования [4; 7; 14].

Поскольку разрабатываемые вычислители ориентированы на самый широкий круг решения сложных задач мониторинга и диагностики путем интеллектуального анализа поступающих данных для выявления признаков несанкционированного вмешательства в работу функциональных узлов энергетического оборудования, весьма актуальным является предоставление подобных возможностей как неотъемлемой части программно-аппаратных средств.

Перспективные задачи

Таким образом, крайне востребованной является разработка цифровой технологии, которая включает:

– разработку архитектуры вычислительной системы, позволяющую модульно наращивать производительность системы в зависимости от требований задачи, обеспечивая, таким образом, наиболее оптимальное соотношение производительности к стоимости программно-аппаратного комплекса;

– определение состава доступных компонент из числа модулей цифровой обработки информации и чипов с учетом приоритетов импортозамещения и локализаци выпускаемых серийно лидирующими компаниями-производителями, а также стандартных конструктивов для размещения вычислительных модулей и блоков программно-аппаратного комплекса;

– разработку и изготовление материнской платы и контроллеров управления параллельными вычислительными процессами, необходимость самостоятельной разработки которых обуславливается спецификой модульной и легко наращиваемой параллельной архитектуры вычислительной системы программно-аппаратного комплекса;

– разработку системного и прикладного программного обеспечения в виде программного комплекса, ориентированного на решение сложных инженерных задач мониторинга и диагностики для обнаружения и парирования некорректного поведения интеллектуальных элементов информационно-управляющих систем вследствие латентных, сложно выявляемых атак, включающего библиотеки параллельных алгоритмов, в том числе нейросетевых, оптимизированных под архитектуру программно-аппаратного комплекса;

– разработку и программную реализацию алгоритмов решения ресурсоемких задач мониторинга и диагностики путем интеллектуального анализа всех поступающих данных для выявления признаков несанкционированного вмешательства в работу функциональных узлов энергетического оборудования, включая задачи обработки больших объемов информации, в том числе телеметрической, выявления признаков изменения сигнала с определением вероятности атаки, задачи комплексного мониторинга и интеллектуального управления (слияния данных от интеллектуальных датчиков).

Основными решаемыми задачами для создания рассматриваемого программно-аппаратного комплекса являются следующие:

– разработка новой алгоритмической базы, специально ориентированной на разработку параллельных алгоритмов решения сложных задач мониторинга и диагностики для обнаружения и парирования некорректного поведения интеллектуальных элементов информационно-управляющих систем вследствие латентных, сложно выявляемых атак;

– разработка адаптивных архитектурных решений для реализации созданных алгоритмов, в том числе снижением требований по весогабаритным ограничениям присущим кластерным конфигурациям;

– разработка комплексного набора методик компоновки аппаратно-программных комплексов в соответствии с решаемыми классами задач;

– разработка интеллектуальных средств классификации, распознавания и кластеризации данных для обнаружения атак и поиска скрытых аномальных закономерностей в потоках и массивах технологических данных, в том числе выявления и проверки нештатной (аномальной) ситуации, идентификацию атаки, ввод в действие алгоритма блокирования атаки, выработка решения о введении режима критической ситуации с переходом на технические средства непрограммируемой логики для локализации отказов и последующего возврата в штатные режимы для восстановления работоспособности функциональных узлов оборудования, а также прогнозирование поведения целевых функциональных узлов оборудования на основе анализа поведения коррелирующих параметров, ориентированные на широкий спектр используемого энергетического оборудования;

– обеспечение доступа к вычислительным ресурсам на рабочих местах операторов системы и иных специалистов и реализация возможности их взаимодействия в реальном масштабе времени с решаемой проблемой;

– разработка аппаратно-программного комплекса с характеристиками масштабируемой сверхвысокой производительности.

Основными задачами в части средств задания определенных параметров для поиска совпадений, аномалий, параметрических возмущений при анализе потоков данных (в том числе характеристик входов, выходов, весов связей и пр.) являются:

– разработка и реализация программных инструментальных средств для выявления информативного обобщенного параметра состояния объекта с целью обнаружения атак, а также классификации, распознавания и кластеризации данных для идентификации атак и поиска скрытых аномальных закономерностей в потоках и массивах технологических данных, включая выработку управляющих команд для стабилизации работы оборудования;

– разработка и реализация аппаратно-программных подсистем для выявления признаков изменения сигнала с определенной вероятностью атаки и задания определенных параметров для поиска совпадений, аномалий, параметрических возмущений при анализе потоков данных на базе доступных по стоимости вычислителей в реальном масштабе времени;

– разработка технических предложений и решений по созданию масштабируемых подсистем, в том числе для локализации отказов и задания определенных параметров для восстановления работоспособности функциональных узлов оборудования на базе доступных по стоимости вычислителей.

Ключевые характеристики комплекса

Система низкоуровневого управления представляет собой управляющий контроллер, реализующий внешние, высокоскоростные интерфейсы обмена данными, а также управляющий работой всех модулей, входящих в состав нейросетевого вычислителя. Управляющий контроллер осуществляет загрузку обрабатываемых данных в вычислительные модули и собирает результаты расчетов, передавая их в систему высокоуровневого управления.

Для высокоуровневого управления нейросетевым вычислителем необходим блок, реализующий системное и прикладное программное обеспечение.

Системное шасси обеспечивает совместную работу всех блоков в рамках одного конструктивного блока. Также оно обеспечивает питание модулей. Функционально системное шасси представляет собой линии связи для приема и передачи сигналов между блоками, входящими в состав нейросетевого вычислителя.

Разрабатываемый комплекс должен обладать гибкой конфигурируемой архитектурой, чтобы использоваться при решении широкого спектра задач мониторинга и диагностики для обнаружения и парирования некорректного поведения интеллектуальных элементов информационно-управляющих систем вследствие латентных, сложно выявляемых атак [2; 10].

Одной из особенностей данного класса задач является то, что в результате вычислений получается большой объем данных, тяжелый для восприятия человеком-оператором [11; 12]. Это, в свою очередь, требует привлечения достаточно развитых вычислительных средств для автоматизированного поиска совпадений, аномалий, параметрических возмущений при анализе потоков данных для выявления признаков изменения сигнала с определением вероятности атаки, ее идентификации и выработки управляющих команд для стабилизации работы оборудования [16; 17].

Наиболее значимыми составляющими работы комплекса являются следующие:

– интеллектуальный анализ всех поступающих данных для выявления признаков несанкционированного вмешательства в работу функциональных узлов энергетического оборудования;

– использование комплексного набора инструментальных средств для задания определенных параметров с целью поиска совпадений, аномалий, параметрических возмущений при анализе потоков данных, характеристик входов, выходов, весов связей и др.;

– выявление информативного обобщенного параметра состояния объекта и проверка нештатной (аномальной) ситуации, идентификацию атаки;

– ввод в действие алгоритма блокирования атаки, выработка решения о введении режима критической ситуации с переходом на технические средства непрограммируемой логики;

– прогнозирование поведения целевых функциональных узлов оборудования на основе анализа поведения коррелирующих параметров, ориентированного на широкий спектр используемого оборудования для последующего возврата в штатные режимы и восстановления работоспособности функциональных узлов оборудования;

– обеспечение доступа к вычислительным ресурсам на рабочих местах операторов и реализация возможности их взаимодействия в реальном масштабе времени с решаемой проблемой.

Требуемые результаты:

– программно-аппаратный комплекс на базе компьютера с высоким уровнем параллелизма, масштабируемости и возможности к модернизации, предназначенный для решения сложных задач интеллектуального анализа больших и сверхбольших объемов поступающих данных;

– формирование кластерных архитектур для расчета сложных задач мониторинга и диагностики путем интеллектуального анализа всех поступающих данных для выявления признаков несанкционированного вмешательства в работу функциональных узлов энергетического оборудования;

– алгоритмы решения задач обработки больших объемов информации, выявления признаков изменения сигнала с определенной вероятностью атаки, задачи комплексного мониторинга и интеллектуального управления (слияние данных), включая их программную реализацию, оптимизированную под разрабатываемый супервычислитель;

– библиотеки математических функций и параллельных алгоритмов обработки данных, оптимизированных под разработанный компьютер, включая разработку модулей для проектирования конструкции и основных технологических систем энергетических объ-

ектов. Данные библиотеки должны обеспечить эффективную разработку новых приложений, не входящих в состав разрабатываемого пакета программ, предназначенных для исполнения на разрабатываемом компьютере.

Заключение

В отрасли востребовано создание масштабируемого по производительности программно-аппаратного комплекса автоматизированного мониторинга и диагностики с нейросетевой компонентой, ориентированных на реализацию высокопроизводительных вычислений с пиковой производительностью до нескольких десятков терафлоп (в рамках сверхбольших энергетических систем)] [5; 13].

Этот комплекс должен решать самые разнообразные прикладные задачи мониторинга и диагностики путем интеллектуального анализа всех поступающих данных для выявления признаков несанкционированного вмешательства в работу функциональных узлов энергетического оборудования в рамках конкретного объекта и групп объектов. За счет наличия комплексных эффективных средств должна реализовываться классификация, распознавание и кластеризация данных для обнаружения и идентификации атак и поиск скрытых аномальных закономерностей в потоках и массивах технологических данных.

Результатом должно являться выявление информативного обобщенного параметра состояния объекта, проверка выявленной нештатной (аномальной) ситуации, идентификация атаки, ввод в действие алгоритма блокирования атаки, выработка решения о введении режима критической ситуации с переходом на технические средства непрограммируемой логики, а также прогнозирование поведения целевых функциональных узлов оборудования на основе анализа поведения коррелирующих параметров для последующего возврата в штатные режимы и восстановления работоспособности функциональных узлов оборудования.

Литература

1. *Агеев А.И.* Smart-коллапс в цифровой энергетике будущего: угрозы глобального обрушения информационных систем управления в условиях возможной самоорганизованной информационной блокады // Энергетик. 2020. № 6. С. 10–14.

2. *Астаулов Р.А., Жуков В.Г.* Защита периметра сети распределенной системой обнаружения вторжений // Решетневские чтения. 2018. Т. 2. С. 316–318.

3. *Балановская А.В., Волкодаева А.В.* Информационная безопасность критически важных объектов в автоматизированных системах управления технологическими процессами // Вестник Самарского муниципального института управления. 2017. № 1. С. 74–81.

4. *Буренин А.Н., Легков К.Е.* Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: управление безопасностью сетей // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7, № 4. С. 42–51.

5. *Васильев Ю.С., Зегжда П.Д., Зегжда Д.П.* Обеспечение безопасности автоматизированных систем управления технологическими процессами на объектах гидроэнергетики // Известия Российской академии наук. Энергетика. 2016. № 3. С. 49–61.

6. *Воробьев А.Е., Фральцова Т.А., Томашев М.С.* О повышении уровня защищенности потенциально опасных объектов ТЭК от террористических атак // Бурение и нефть. 2017. № 6. С. 68–73.

7. *Грабчак Е.П., Григорьев В.В., Логинов Е.Л., Деркач А.К.* Формирование территориально распределенной сети катастрофоустойчивых дата-центров: концентрация защищенных систем управления в энергетике, адаптированных для работы в условиях чрезвычайных ситуаций и в особый период // Проблемы безопасности и чрезвычайных ситуаций. 2020. № 5. С. 75–81.

8. *Грабчак Е.П., Логинов Е.Л.* Цифровая энергетика: повышение надежности управления электро- и теплоэнергетическими системами на основе внедрения цифровых технологий. М.: МНИИПУ, ИНЭС, 2020. 222 с.

9. *Грабчак Е.П.* Цифровая трансформация электроэнергетики. М.: Кнорус, 2018. 340 с.

10. *Жиленков А.А., Черный С.Г.* Система безаварийного управления критически важными объектами в условиях кибернетических атак // Вопросы кибербезопасности. 2020. № 2 (36). С. 58–66.

11. *Иванов С.Н.* Энергосбережение: проблемы достижения энергоэффективности. М.: НИЭБ, 2009. 329 с.

12. *Корнеев А.В.* Безопасность энергетических сетей США: проблемы борьбы с кибернетическим терроризмом // США и Канада: экономика, политика, культура. 2011. № 7 (499). С. 25–46.

13. *Корнеев А.В.* Защита инфраструктуры ТЭК от новых средств кибернетического нападения. Опыт борьбы с дистанционным терроризмом // Энергобезопасность и энергосбережение. 2012. № 1. С. 5–10.

14. *Логинов Е.Л., Логинов А.Е.* Интеллектуальная электроэнергетика: новый формат интегрированного управления в Единой энергетической системе России // Национальные интересы: приоритеты и безопасность. 2012. Т. 8, № 29 (170). С. 28–32.

15. *Маликов А.В.* Модель диагностирования нарушений безопасности на основе искусственных нейронных сетей // Математические методы в технике и технологиях – ММТТ. 2019. Т. 6. С. 125–128.

16. *Назаров И.Г., Суслов Д.В., Никандров М.В., Славутский Л.А.* Комплекс обеспечения контролируемой деградации системы управления энергообъекта при киберинцидентах // Вестник Чувашского университета. 2018. № 1. С. 146–152.

17. *Нестерук Ф.Г., Котенко И.В.* Инструментальные средства создания нейросетевых компонент интеллектуальных систем защиты информации // Труды СПИИРАН. 2013. № 3 (26). С. 7–25.

18. *Сухопаров М.Е., Семенов В.В., Лебедев И.С.* Мониторинг информационной безопасности элементов киберфизических систем с использованием искусственных нейронных сетей // Методы и технические средства обеспечения безопасности информации. 2018. № 27. С. 59–60.

19. *Фисун В.В.* Искусственный интеллект управления информационной безопасностью объектов критической информационной инфраструктуры. М.: Русайнс, 2020. 357 с.

20. *Шабуров А.С.* Модели нейронных сетей для решения задач обеспечения безопасности объектов критической информационной инфраструктуры // Нейрокомпьютеры: разработка, применение. 2019. Т. 21, № 3. С. 73–78.

21. *Шелухин О.И., Чернышев А.И.* Исследование и моделирование нейросетевых алгоритмов обнаружения аномальных вторжений в компьютерные сети // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8, № 12. С. 102–106.

References

1. Ageev A.I. (2020) *Smart-kollaps v cifrovoj energetike budushchego: ugrozy global'nogo obrusheniya informacionnyh sistem upravleniya v usloviyah vozmozhnoj samoorganizovannoj informacionnoj blokady* [Smart Collapse in the Digital Energy of the Future: Threats of a Global Collapse of Information Management Systems in the Context of a Possible Self-Organized Information Blockade]. *Energetik*, no. 6, pp. 10–14 (in Russian).
2. Astaulov R.A., ZHukov V.G. (2018) *Zashchita perimetra seti raspredelennoj sistemoj obnaruzheniya vtorzhenij* [Protecting the network perimeter with a distributed intrusion detection system]. *Reshetnevskie chteniya*, vol. 2, pp. 316–318 (in Russian).
3. Balanovskaya A.V., Volkodaeva A.V. (2017) *Informacionnaya bezopasnost' kriticheski vazhnyh ob"ektov v avtomatizirovannyh sistemah upravleniya tekhnologicheskimi processami* [Information security of critical objects in automated process control systems]. *Vestnik Samarskogo municipal'nogo instituta upravleniya*, no. 1, pp. 74–81 (in Russian).
4. Burenin A.N., Legkov K.E. (2015) *Voprosy bezopasnosti infokommunikacionnyh sistem i setej special'nogo naznacheniya: upravlenie bezopasnost'yu setej* [Security issues of infocommunication systems and special-purpose networks: network security management] *Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli*, vol. 7, no. 4, pp. 42–51 (in Russian).
5. Vasil'ev Y.S., Zegzhda P.D., Zegzhda D.P. (2016) *Obespechenie bezopasnosti avtomatizirovannyh sistem upravleniya tekhnologicheskimi processami na ob'ektah gidroenergetiki* [Ensuring the safety of automated control systems for technological processes at hydropower facilities]. *Izvestiya Rossijskoj akademii nauk. Energetika*, no. 3, pp. 49–61 (in Russian).
6. Vorob'ev A.E., Fral'cova T.A., Tomashev M.S. (2017) *O povyshenii urovnya zashchishchennosti potencial'no opasnyh ob"ektov TEK ot terroristicheskih atak* [On increasing the level of protection of potentially dangerous objects of the fuel and energy complex from terrorist attacks]. *Burenie i neft'*, no. 6, pp. 68–73 (in Russian).
7. Grabchak E.P., Grigor'ev V.V., Loginov E.L., Derkach A.K. (2020) *Formirovanie territorial'no raspredelennoj seti katastrofoustojchivyh data-centrov: koncentraciya zashchishchennyh sistem upravleniya v energetike, adaptirovannyh dlya raboty v usloviyah chrezvychajnyh situacij i v osobyj period* [Formation of a geographically distributed network of disaster-resistant data centers: concentration of protected control systems in the energy sector, adapted to work in emergency situations and in a special period]. *Problemy bezopasnosti i chrezvychajnyh situacij*, no. 5, pp. 75–81 (in Russian).
8. Grabchak E.P., Loginov E.L. (2020) *Cifrovaya energetika: povyshenie nadezhnosti upravleniya elektro- i teploenergeticheskimi sistemami na osnove vnedreniya cifrovyh tekhnologij* [Digital energy: improving the reliability of control of electrical and heat power systems through the introduction of digital technologies]. Moscow, MNIIPU, INES, 222 p. (in Russian).
9. Grabchak E.P. (2018) *Cifrovaya transformaciya elektroenergetiki* [Digital transformation of the electricity industry]. Moscow, Knorus Publishing, 340 p. (in Russian).

10. Zhilenkov A.A., CHernyj S.G. (2020) *Sistema bezavarijnogo upravleniya kriticheski vazhnymi ob"ektami v usloviyah kiberneticheskih atak* [A system of trouble-free management of critical objects in the context of cyber attacks]. *Voprosy kiberbezopasnosti*, no. 2 (36), pp. 58–66 (in Russian).
11. Ivanov S.N. (2009) *Energosberezhenie: problemy dostizheniya energoeffektivnosti* [Energy saving: problems of achieving energy efficiency]. Moscow, NIEB Publishing, 329 p. (in Russian).
12. Korneev A.V. (2011) *Bezopasnost' energeticheskih setej SSHA: problemy bor'by s kiberneticheskim terrorizmom* [US Energy Grid Security: Challenges in Combating Cyber Terrorism]. *SSHA i Kanada: ekonomika, politika, kul'tura*, no. 7 (499), pp. 25–46 (in Russian).
13. Korneev A.V. (2012) *Zashchita infrastruktury TEK ot novyh sredstv kiberneticheskogo napadeniya. Opyt bor'by s distancionnym terrorizmom* [Protection of the fuel and energy complex infrastructure from new means of cyber attack. Experience in Combating Remote Terrorism]. *Energobezopasnost' i energosberezhenie*, no. 1, pp. 5–10 (in Russian).
14. Loginov E.L., Loginov A.E. (2012) *Intellektual'naya elektroenergetika: novyj format integrirovannogo upravleniya v Edinoj energeticheskoj sisteme Rossii* [Intelligent Power Industry: A New Format of Integrated Management in the Unified Energy System of Russia]. *Nacional'nye interesy: prioritety i bezopasnost'*, vol. 8, no. 29 (170), pp. 28–32 (in Russian).
15. Malikov A.V. (2019) *Model' diagnostirovaniya narushenij bezopasnosti na osnove iskusstvennyh nejronnyh setej* [A model for diagnosing security violations based on artificial neural networks]. *Matematicheskie metody v tekhnike i tekhnologiyah – MMTT*, vol. 6, pp. 125–128 (in Russian).
16. Nazarov I.G., Suslov D.V., Nikandrov M.V., Slavutskij L.A. (2018) *Kompleks obespecheniya kontroliruemoj degradacii sistemy upravleniya energoob"ekta pri kiberincidentah* [Complex for ensuring controlled degradation of the power facility management system in case of cyber incidents]. Vestnik Chuvashskogo universiteta, no. 1, pp. 146–152 (in Russian).
17. Nesteruk F.G., Kotenko I.V. (2013) I*nstrumental'nye sredstva sozdaniya nejrosetevyh komponent intellektual'nyh sistem zashchity informacii* [Tools for creating neural network components of intelligent information security systems]. *Trudy SPIIRAN*, no. 3 (26), pp. 7–25 (in Russian).
18. Suhoparov M.E., Semenov V.V., Lebedev I.S. (2018) *Monitoring informacionnoj bezopasnosti elementov kiberfizicheskih sistem s ispol'zovaniem iskusstvennyh nejronnyh setej* [Monitoring information security of elements of cyber-physical systems using artificial neural networks]. *Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informacii*, no. 27, pp. 59–60 (in Russian).
19. Fisun V.V. (2020) Iskusstvennyj intellekt upravleniya informacionnoj bezopasnost'yu ob"ektov kriticheskoj informacionnoj infrastruktury [Artificial Intelligence of Information Security Management of Critical Information Infrastructure Objects]. Moscow, Rusayns Publishing, 357 p. (in Russian).
20. Shaburov A.S. (2019) *Modeli nejronnyh setej dlya resheniya zadach obespecheniya bezopasnosti ob"ektov kriticheskoj informacionnoj infrastruktury* [Neural network models for solving security problems of critical information infrastructure objects]. *Nejrokomp'yutery: razrabotka, primenenie*, vol. 21, no. 3, pp. 73–78 (in Russian).

21. Sheluhin O.I., Chernyshev A.I. (2014) *Issledovanie i modelirovanie nejrosetevyh algoritmov obnaruzheniya anomal'nyh vtorzhenij v komp'yuternye seti* [Research and modeling of neural network algorithms for detecting anomalous intrusions into computer networks]. *T-Comm: Telekommunikacii i transport*, vol. 8, no. 12, pp. 102–106 (in Russian).