Аналитическая статья
УДК 620.9; DOI: 10.61260/2218-13X-2024-4-103-119

РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО ПРИМЕНЕНИЮ НАУЧНО-ТЕХНИЧЕСКОГО ИНСТРУМЕНТАРИЯ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТОВ ЭНЕРГЕТИЧЕСКОГО СЕКТОРА

✉**Израилов Константин Евгеньевич;**
Левшун Диана Альбертовна;
Зеличенок Игорь Юрьевич.
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, Россия
✉***konstantin.izrailov@mail.ru***

Аннотация. Работа посвящена разработке научно-технических предложений по применению научно-технического инструментария для аналитической обработки данных о событиях кибербезопасности объектов энергетического сектора. Задача была поделена на элементы (части-множества), состоящие из различных видов научно-технического инструментария, целей его применения, специфики энергетического сектора и компонентов системы безопасности. Также произведен обзор релевантных работ, позволивший выделить следующую специфику области: кластерность, статичность инфраструктуры, стандартизованность объектов и детерминированность процессов, пониженная стохастичность процессов, непрерывность функционирования и критичность для страны. Произведено полное комбинирование элементов с получением максимально возможного множества групп предложений. Предложена формулировка предложений, получаемая формальным образом из каждой группы. Проанализирована каждая такая группа с выделением применимых для энергетического сектора предложений, а также дана их интерпретация.

Ключевые слова: энергетика, предложения, инструментарий, кибербезопасность, метод

Для цитирования: Израилов К.Е., Левшун Д.А., Зеличенок И.Ю. Разработка предложений по применению научно-технического инструментария для обеспечения кибербезопасности объектов энергетического сектора // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 4. С. 103–119. DOI: 10.61260/2218-13X-2024-4-103-119.

Analytical article

DEVELOPMENT OF PROPOSALS FOR THE APPLICATION OF SCIENTIFIC AND TECHNICAL TOOLS TO ENSURE CYBERSECURITY OF ENERGY SECTOR FACILITIES

✉**Izrailov Konstantin E.;**
Levshun Diana A.;
Zelichenok Igor Yu.
Saint-Petersburg federal research center of the Russian academy of sciences,
Saint-Petersburg, Russia
✉***konstantin.izrailov@mail.ru***

Abstract. The work focuses on developing scientific and technical proposals for using scientific and technical tools to analyze data on cybersecurity events. The problem divided into elements (parts-sets) consisting of various types of scientific and technical tools, the purposes of their application, the specifics of the energy sector and previously created components. A review of relevant works also highlighted the following specifics of the field: clustering, static infrastructure, standardization of objects, and determinism of processes, reduced stochasticity of processes, continuity of operation, and criticality for the country. The authors fully combined the elements to obtain the maximum possible set of proposal groups. The formulation of proposals, formally obtained from each group, is suggested. Each such group underwent analysis, identifying proposals applicable to the energy sector, and providing an interpretation.

Keywords: energy, proposals, tools, cybersecurity, method

For citation: Izrailov K.E., Levshun D.A., Zelichenok I.Yu. Development of proposals for the application of scientific and technical tools to ensure cybersecurity of energy sector facilities // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 4. P. 103–119. DOI: 10.61260/2218-13X-2024-4-103-119.

Введение

Энергетический сектор (ЭС) является критически важной областью любого государства, и в особенности Российской Федерации, входящей в пятерку лидеров по количеству выработанной электроэнергии за год и атомным мощностям [1]. С другой стороны, существенный уровень автоматизации данной области требует обеспечения ее кибербезопасности [2], на сложность чего влияет значительное количество и гетерогенность информационных потоков [3]. Также считается, что «стоимость» производства ядерной энергии существенно меньше, чем связанные с этим риски, что переводит обеспечение безопасности в разряд первоочередных задач.

Ранее в результатах проведенного исследования, участниками которого являлись авторы статьи, был разработан теоретико-практический инструментарий, состоящий из различных методов, моделей, методик, алгоритмов, архитектуры и программных приложений; а также предназначенный для аналитической обработки больших массивов гетерогенных данных, содержащих события кибербезопасности [4–6]. Разработанный инструментарий может применяться к объектам ЭС в интересах оценки их состояния, поддержки принятия решений и расследования компьютерных инцидентов. Тем не менее для обеспечения применимости и повышения ее эффективности требуется разработка соответствующих научно-технических предложений, что является задачей текущего этапа исследования и описывается в данной статье.

Статья организована следующим образом: представлен обзор существующих исследований в области энергетики; описан метод формирования научно-технических предложений; определена специфика энергетического сектора; разработан перечень научно-технических предложений.

Обзор работ в ЭС

Для сбора, анализа и систематизации знаний об ЭС был сделан обзор исследовательских работ, в которых в той или иной степени отражена специфика энергетической области в различных аспектах – актуальность и применимость, функционирования и управления, а также безопасность.

Оценка текущего состояния ЭС Российской Федерации, а также его планируемое развитие рассматривается в работе [7]. Указывается значимость Российской Федерации для мирового рынка в части поставляемой первичной энергии (доля которой составляет 10 %), являясь при этом четвертым экспортером энергоресурсов. Одним из путей развития сектора определяется введение цифровизации и интеллектуализации. Также прогнозируется развитие отдельных территориальных проектов в секторе.

Авторы работы [8] рассматривают проблему обеспечения кибербезопасности ЭС, актуализировавшейся с ее переходом на цифровые платформы. Указывается необходимость и неизбежность перехода информационных процессов сектора на работу по единым стандартам, а также сертификация используемого программного обеспечения. Делается ряд основополагающих выводов, таких как совершенствование механизмов обмена информацией о киберугрозах, создание единой правовой базы сертификации программных продуктов, применение подходов на базе моделей рисков и др.

Различные системы безопасности атомных электростанций (АЭС) рассмотрены в работе [9]: проверки и испытания системы контура, барьеры безопасности, система отсечения главных паропроводов, система защиты второго контура от превышения давления и система пассивного отвода тепла. Отмечается существующая специфика АЭС, заключающаяся в применении простых технологических решений и единых механизмов для реализации ряда функций безопасности. При этом в работе [10] актуализируется проблема ядерного терроризма.

Вопросы внедрения геоинформационных технологий в ЭС Российской Федерации в интересах повышения его эффективности затрагиваются в работе [11]. В качестве перспектив применения данного рода технологий указываются такие, как мониторинг объектов сектора и ее служб, планирования развития, обеспечение финансовых и правовых операций и пр. Выделяются такие гео-атрибуты ЭС, как местоположение оборудования и датчиков мониторинга, мест разбалансировки электроэнергии и др.

Непрерывность обеспечения электроэнергией таких критических объектов, как больницы, центры обработки информации, институциональные службы, актуализируется в работе [12]. В интересах этого авторы описывают специальные модули, препятствующие потере подачи электроэнергии как на короткий, так и на длительный период. Также рассматриваются некоторые аспекты создания ЭС с непрерывным предоставлением энергоресурсов.

В работе [13] приводится опыт проектирования электростанций для нефтегазовой отрасли, относящийся к учету возможностей и потребностей от электрогенераторов, топологии распределения электроэнергии, управления нагрузкой и др. Указывается целесообразность использования количества генераторов, превосходящих минимально необходимое, чтобы нейтрализовать его возможную остановку – что, в частности, говорит о важности непрерывной энергоподачи и приоритете при проектировании устойчивой к сбоям статической структуры, а не ее экстренное восстановление, например, путем физической замены генератора. При этом прокладка электрокабелей с учетом специфики нефтегазовой отрасли является достаточно сложной задачей, которая должна решаться в самом начале проектирования.

В работе [14] выделяются такие особенности топливно-энергетического комплекса (ТЭК), как регуляция на законодательном уровне, развитая инфраструктура из разнородных объектов и монополия энергетических компаний, что требует дополнительного контроля со стороны государства. Экономическая безопасность ТЭК включает в себя ряд

мер, направленных на обеспечение стабильности производства и поставок энергоресурсов, а также гарантирование социальной стабильности и защиты прав потребителей.

В работе [15] рассматривается энергетический комплекс мегаполиса с выделением в нем таких черт, как развитие тенденций децентрализации энергоснабжения и необходимость согласования интересов различных хозяйствующих субъектов. К принципам организации управления развитием энергетического комплекса мегаполиса авторы относят следующие: технологическая доступность, экологичность, экономическая обоснованность, энергоэффективность, инновационность, социальная эффективность и ориентация на использование интегрированных решений. Также принципы развития энергетического комплекса мегаполиса рассмотрены в работе [16], где, в том числе выделяется маневренность – то есть способность организовать гибкую управленческую систему, которая позволяет вносить необходимые изменения в деятельность предприятия при возникновении непредвиденных ситуаций.

Авторы в работе [17] рассматривают особенности энергетических киберфизических систем (ЭКФС), включающие иерархичность системы, самоорганизацию и устойчивость. В отличие от традиционной точки зрения на устойчивость энергосистемы, устойчивость ЭКФС нацелена на интегрированную систему в виде единого целого. По сравнению с оптимизацией и планированием физических объектов для устойчивости энергосистемы, устойчивость ЭКФС должна учитывать всевозможные связи между кибернетическим и физическим уровнями.

В работе [18] особое внимание уделено тому, что с точки зрения безопасности основным защищаемым объектом в энергетике является не столько информация, сколько технологический процесс. Выделяются такие проблемы, как наличие уязвимостей многолетней архитектуры энергетических сетей, устаревшее программное обеспечение и т.д. В работе [19] подчеркивается, что для энергетических предприятий защита от атак должна быть направлена в первую очередь на предотвращение вторжений, а не их предупреждение. Необходимость реагирования на произошедшие инциденты в энергетических комплексах приводит к серьезным последствиям, таким как простои и дорогостоящие перезапуски производства.

В работе [20] авторы проводят обзор использования методик искусственного интеллекта (ИИ) в сфере безопасности энергетической инфраструктуры. Авторы оценивают эффективность машинного обучения в задачах автоматизации и реагирования на инциденты, а также обсуждают необходимость применения ИИ в энергосетях. В качестве основной специфики они указывают то, что энергетическая инфраструктура представляет собой сложную взаимосвязанную сеть, включающую производство, передачу и распределение энергии; такая сеть характеризуется широкой географической распределенностью, интеграцией информационных и операционных технологий для оптимизации управления и мониторинга, а также зависимостью от различных узлов, каждый из которых играет критическую роль. Одним из важнейших факторов является зависимость от третьих лиц поддержания и обеспечения компонентов сети, что увеличивает риск атак через цепочки поставок, а также усиливает эффект каскадных сбоев из-за взаимосвязанности узлов в энергетической сети.

Специфика применения цифровых двойников в ЭС обсуждается в работе [21]. Для этого авторы осуществляют обзор текущих решений и моделей двойников, применяемых в различных отраслях, включая энергетику. В ходе анализа выделяются ключевые параметры, которые определяют эффективность моделей цифровых двойников, такие, как архитектура, механизмы интеграции и функциональность и др. Также выделяются основные характеристики цифровых двойников, которые играют ключевую роль при их интеграции в ЭС. Эти параметры включают гибкость, масштабируемость, точность данных, скорость реакции на изменения и использование протоколов связи, таких как DNP3 и IEC 61850. Главной проблемой, как и в работе [20], устанавливается географическая распределенность узлов энергетической сети, а также их глубокая взаимозависимость.

Авторы работы [22] описывают инструмент SecuriDN, поддерживающий раннее обнаружение кибератак в умных ЭС. Инструмент предназначен для моделирования информационных и организационных технологий подсистем энергосетей, а также для анализа возможных киберугроз, которые могут их затронуть. Также выявлены проблемы географической распределенности и глубокой интеграции различных элементов энергетической сети друг с другом, что было рассмотрено со стороны требований к сертификации, законодательства и рисков. Указывается, что из-за критической важности рассматриваемой инфраструктуры и высоких требований к безопасности, например, согласно стандартам IEC 61850 и IEC 62351, предложенные решения должны, в том числе, иметь низкий порог ложноположительных и ложноотрицательных срабатываний, возможность предсказывать потенциальные атаки и малое временное окно для своевременного обнаружения угрозы и внедрения контрмер.

Более глобальная задача по анализу датчиков в умных домах упомянута в работе [23]. Авторы разрабатывают интеллектуальную систему управления энергией для умных городов с использованием методов машинного обучения. Основная цель исследования заключается в оптимизации потребления энергии и снижении нагрузки на энергетические сети, особенно во время пиковых нагрузок. Выделена такая специфика ЭС, как предсказуемость нагрузки, а также ее интервальность, что позволяет моделям машинного обучения корректировать применяемые контрмеры с учетом временных меток и промежутков.

Российские ученые в работе [24] проводят обзор, касающийся использования моделей ИИ в сфере управления энергосистемами и обнаружения в них аномалий. Предлагается несколько важнейших направлений, таких, как прогнозирование нагрузки, обнаружение аномалий, управление системами и оптимизация возобновляемых источников энергии. Также, авторы выделяют такие отличительные моменты ЭС, как предсказуемая интервальная нагрузка, а также влияние погодных условий, которые вносят эффект случайности в нормальный режим функционирования.

В интересах выявления специфики в ЭС в работе [25] исследование посвящено различным областям применения ИИ. Выделены ключевые направления его использования, такие как кибербезопасность, прогнозирование и повышение энергоэффективности. При этом актуализирована такая специфика ЭС, как уязвимость к кибератакам за счет устаревшего оборудования и необходимость прогнозирования спроса на энергию.

Метод формирования предложений

В интересах решения задачи по разработке научно-технических предложений применительно к заданной области была разработана обобщенная схема проведения исследования, позволяющая выделить группы предложений научно-обоснованным способом в противовес эмпирическому, основанному на точке зрения экспертов. В результате анализа постановки задачи удалось выделить четыре ее основополагающие части-множества.

Во-первых, в предложениях должен использоваться разработанный инструментарий (множество X), состоящий из следующих элементов: теоретических (X_1) – методы, модели, методики, алгоритмы; практических (X_2) – архитектуры, программные приложения; технологических (X_3) – как совокупность теоретического и практического.

В формальном виде это может быть записано следующим образом:

$$\mathrm{X} \equiv \{\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3\}.$$

Во-вторых, разработанный инструментарий должен быть применен для одной из следующих целей (множество Y): оценка состояния (Y_1), поддержка принятия решений (Y_2), расследование компьютерных инцидентов (Y_3).

В формальном виде это может быть записано следующим образом:

$$Y \equiv \{Y_1, Y_2, Y_3\}.$$

В-третьих, предложения должны касаться применения инструментария в области ЭС, которая определяется собственной спецификой (множество Z).

В-четвертых, разработанный инструментарий должен быть включен в определенные компоненты системы безопасности в рамках одной архитектуры (множество K). В каждом из компонентов может содержаться инструментарий (X_i), применимый для множества целей (Y_j) с учетом специфики (Z_l) области. Компоненты в рамках одной архитектуры (K_m) имеют следующие назначения: K_1 – обнаружение в реальном времени атак на основе имитационного и графо-ориентированного моделирования; K_2 – обнаружение в реальном времени аномальной активности и нарушений критериев и политик безопасности на основе аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности; K_3 – оперативная оценка защищенности информационных, телекоммуникационных и других критически важных ресурсов на основе аналитической обработки больших массивов гетерогенных данных; K_4 – оперативный анализ и управление рисками информационной безопасности на основе аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности; K_5 – оперативная визуализация больших массивов гетерогенных данных о событиях кибербезопасности в интересах оценки состояния, поддержки принятия решений и расследования инцидентов; K_6 – проведение расследований компьютерных инцидентов.

Следовательно, множество всех возможных групп предложений (R) как полное комбинирование частей всей задачи имеет следующую формальную запись:

$$\begin{cases} R \equiv \bigcup\limits_{i,j,l,m} R_{i,j,l,m} \\ R_{i,j,l,m} \equiv Essence(X_i, Y_j, Z_l, K_m) \end{cases},$$

где $R_{i,j,l,m}$ – группа предложений по применению инструментария для достижения цели с учетом специфики области ЭС с помощью компонентов на базе единой архитектуры (согласно индексам *I, j, l* и *m*); $Essence(\dots)$ – оператор продуцирования сути предложений из группы согласно заданным параметрам (то есть индексам предложений) по следующему шаблону:

«Группа предложений i.j.l.m. Применение инструментария {X_i} из компонентов на базе единой архитектуры {K_m} для {Y_j}, исходя из специфики {Z_l} области ЭС».

С учетом текущего состояния области и предыдущих полученных результатов, не все группы могут иметь предложения по применению на практике, то есть:

$$\exists A \subset \emptyset : \langle i, j, l, m \rangle \in A \Rightarrow R_{i,j,l,m} \in \emptyset,$$

где A – некоторое непустое множество индексов, для которых не существует подходящих предложений; $\langle \dots \rangle$ – кортеж, как упорядоченный набор индексов для элементов множества R.

Часть предложений может быть объединена в единую группу (из множества G), а их строгая формулировка приведена к более человеко-ориентированному виду:

$$G_{i,k,l,m} = \bigcup_{t} R^{t}_{i,k,l,m},$$

где $G_{i,k,l,m}$ – группа объединенных предложений согласно их индексам *I, j, l* и *m*; t – индекс разновидности предложения с одинаковыми индексами.

В следующем разделе будут более подробно рассмотрены знания о специфике ЭС и выделены элементы множества Z_i.

Определение специфики ЭС

Анализ результатов проведенного обзора работ в двух аспектах – внешнего и внутреннего, позволил выделить следующие отличительные моменты ЭС:

а) с внешней точки рассмотрения:

– выработка и передача выделенного ресурса, которым является электроэнергия (с помощью электрогенераторов, линий электропередач и пр.);

– наличие функции сохранения энергоресурсов (то есть применение аккумуляторов, работающих на различных принципах, включая гравитационные [26]);

– необходимость непрерывного обеспечения электроэнергией (поскольку временное прерывание ее подачи, в отличие, например, от транспортных перевозок, фактически остановит работу целых комплексов, на перезапуск которых потребуются существенные ресурсозатраты);

– большая распределенность систем с локализацией в отдельных точках (АЭС, распределительные комплексы, крупные потребители, соединенные линии электросвязи);

– необходимость для функционирования практически всех отраслей страны (транспорт, производства, города, дома и пр.);

– сверхкритичность от реализации угроз (коллапс на уровне производств, городов, областей и пр.);

– поддержка функционирования информационных систем в части аппаратной части (то есть обеспечение существования нефизических областей жизнедеятельности);

– существование в области ядерного терроризма, отражающегося в виде захвата АЭС, их минирования и взрыва;

– высокие сроки и стоимость сооружения энергообъектов (например, АЭС).

б) с внутренней точки рассмотрения:

– наличие установленного режима нормального функционирования (поскольку имеется четкое описание стандартного поведения системы и отдельных датчиков при нормальных условиях);

– наличие четких диапазонов для ряда параметров ЭС (например, нормальные диапазоны напряжения, температуры, давления и т.д.);

– возможность существования сверхпиковых нагрузок (например, резкое увеличение потребления энергии в определенные часы или при чрезвычайных ситуациях);

– достаточность информации для предиктивного обслуживания (например, предсказание отказов оборудования, что может использоваться при профилактике систем);

– использование специальных и узконаправленных технологий (например, SCADA-систем);

– высокие требования к автоматизации отрасли (из-за количества информационных и технологических процессов, их частоты);

– относительная качественная однородность компонентов, «завязанных» на работу с энергоресурсами (в отличие, например, от авто и железных дорог или крупных городов).

Важно отметить, что угрозы безопасности энергетических объектов влияют не столько на утечку информации, сколько на нарушение технологического процесса и работу всей энергосистемы. Также системы энергетического комплекса обладают достаточно большим количеством контрольных точек для регистрации информативных параметров; поэтому особое внимание, как правило, уделяется выбору приоритетных зон мониторинга.

Систематизация и обобщение указанных аспектов позволили синтезировать шесть следующих специфик ЭС:

– кластерность (Z_1), состоящая в локализации ЭС в отдельных территориальных областях, при этом соединенных в единую электросеть, что требует

высокопроизводительной обработки средних и больших объемов информации, но с учетом особенностей отдельных подсистем;

– статичность инфраструктуры (Z_2), что качественно отличает ЭС от авто и железных дорог или крупных городов, элементами которых часто являются подвижные физические объекты; как результат, в интересах обеспечения кибербезопасности ЭС возможно использовать модели и методы, предварительно созданные и оптимизированные для решения требуемых задач;

– стандартизованность объектов и детерминированность процессов (Z_3), заключающиеся в наличии строго заданных границ различных параметров и характеристик, правил перехода между заранее предопределенными состояниями и пр. [27, 28], что обосновывает эффективность применения графовых представлений, имитационного моделирования и строгих правил, а также методов выявления аномалий и событий кибербезопасности с последующим расследованием компьютерных инцидентов;

– пониженная стохастичность процессов (Z_4), означающая не столь высокое влияние человеческого фактора (сложно прогнозируемого и связанного с психоэмоциональным состоянием субъектов) по причине использования в ЭС отлаженных механизмов, программного обеспечения и прочих достаточно детерминированных исполнительных устройств; например, при нынешнем уровне автоматизации прямые угрозы зачастую происходят из-за превышения датчиками разрешенных параметров (впрочем, источником угрозы могут быть человеческие действия по саботажу на энергетических объектах или следствия некачественных интерфейсов взаимодействия с информационными системами [29–32]);

– непрерывность функционирования (Z_5), означающая риск существенного ущерба (человеческие жертвы, финансовые потери, снижение репутации, тактическое и стратегическое поражение в военной сфере), даже от кратковременного прекращения обеспечения потребителей энергоресурсами, что требует более жесткого категорирования событий и рисков кибербезопасности (то есть важным становиться не степень ущерба, а сам его факт свершения);

– критичность для страны (Z_6), заключающаяся не только в применении ЭС во всех сфер Российской Федерации, но и обеспечение ее стратегической безопасности из-за существования ядерного терроризма (на АЭС), что требует в ряде случаев создания превентивных мер (как мониторинга, так и противодействия), обладающих сверх высокой результативностью и оперативностью из-за потенциальных последствий, связанных, например, с распространением радиоактивных материалов, потенциально огромным уроном и сложностью нейтрализации последствий.

Согласно выделенной специфике ЭС максимальное количество всех групп предложений составит следующее значение (как перемножение мощностей множеств X, Y, Z и K): $3 \times 3 \times 6 \times 6 = 324$; еще раз подчеркнем, что не все группы могут содержать предложения, применимые в ЭС на практике.

Перечень научно-технических предложений

Исходя из предложенной обобщенной схемы проведения исследования в интересах выработки предложений, а также с учетом полученной специфики (Z_k) области, выполнена систематизация указанных частей-множеств задачи исследования с позиции разработки предложений, представленная в таблице. В ячейках таблицы указан группы предложений ($G_{i,j,k,l}$) по применению компонентов из одной архитектуры (строки K_m) для заданных ранее целей (столбцы Y_j).

Поскольку в том или ином виде практически любая модель или метод может учитывать любые специфику ЭС и цель применения инструментария (хотя обоснованность и эффективность может оказаться крайне низкой), в таблице указаны именно основные предложения. Компоненты при этом рекомендуется применять следующим образом:

K_1, K_2 и K_3 – для оценки состояния; K_4 – для оценки состояния и поддержки принятия решений; K_5 – для оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов; K_6 – для расследования компьютерных инцидентов. Расшифровка групп предложений приведена далее.

Таблица

Систематизация предложений для энергетического сектора

		Цели применения инструментария		
		Y_1	Y_2	Y_3
Компоненты одной архитектуры	K_1	$G_{\{1,2,3\},1,\{1,2,6\},1}$		
	K_2	$G_{\{1,2,3\},1,\{1,2,6\},2}$		
	K_3	$G_{\{1,2,3\},1,\{1,2,6\},3}$		
	K_4	$G_{\{1,2,3\},1,\{1,2,6\},4}$	$G_{\{1,2,3\},2,\{3,4,6\},4}$	
	K_5	$G_{\{1,2,3\},1,\{1,2,6\},5}$	$G_{\{1,2,3\},2,\{3,4,6\},5}$	$G_{\{1,2,3\},3,\{3,4,5,6\},5}$
	K_6			$G_{\{1,2,3\},3,\{3,4,5,6\},6}$

Стоит отметить, что свойство Z_6 актуализирует применение в рамках обеспечения кибербезопасности ЭС всего множества инструментария, реализованного во всех компонентах, что указано с помощью множества индексов группы предложений – $G_{\{1,2,3\},\ldots}$; аналогичным образом указывается и множество индексов, соответствующих используемым спецификам ЭС.

Группа предложения $G_{\{1,2,3\},1,\{1,2,6\},1}$. Применение всего инструментария из компонентов на базе единой архитектуры K_1 для Y_1 исходя из специфик области Z_1, Z_2 и Z_6.

Компоненты K_1 для Y_1 могут применяться путем кластеризации и классификацией состояний [33] с последующим выделением нештатного поведения (с помощью имитационного моделирования) как отдельных элементов на объектах ЭС (например, генераторов электроэнергии различного принципа действия), так и всей энергетической системы (например, при полномасштабном внедрении сверхпроводящих кабельных линий [34]). Применимость компонента для оценки состояний была продемонстрирована для датасета, собранного по промышленной системе управления выработкой электроэнергии паровыми турбинами и гидроаккумулирующими электростанциями HAI (HIL-based Augmented ICS) [4]. Данная возможность обусловлена свойством кластерности Z_1, а за счет свойств Z_2 повысится возможность применения заранее построенных имитационных моделей и обученных классификаторов.

Группа предложения $G_{\{1,2,3\},1,\{1,2,6\},2}$. Применение всего инструментария из компонентов на базе единой архитектуры K_2 для Y_1 исходя из специфик области Z_1, Z_2 и Z_6.

Компоненты K_1 для Y_1 могут применяться путем обоснованного выбора или комбинирования алгоритмов выявления аномалий в показаниях датчиков на объектах ЭС

(например, в температурно-темпоральных показателях подвижных механизмов энергетического оборудования [35]). Также, выявление нарушений критериев и политик безопасности с помощью K_1 может применяться для глобальных информационных систем, используемых в ЭС. Данные возможности обусловлены свойством кластерности Z_1, а за счет свойств Z_2 повысится возможность применения заранее определенных критериев и параметров настройки алгоритмов.

Группа предложения $G_{\{1,2,3\},1,\{1,2,6\},3}$. Применение всего инструментария из компонентов на базе единой архитектуры K_3 для Y_1 исходя из специфик области Z_1, Z_2 и Z_6.

Компоненты K_3 для Y_1 могут применяться путем оценки защищенности информационных и телекоммуникационных ресурсов объектов ЭС (например, защищенность от тяжёлых аварий на АЭС, готовность к их управлению при потере конечного поглотителя тепла и пр. [36]), а также оценки защищенности крупных сетей ЭС (например, от масштабных перегрузок). Данная возможность обусловлена свойством кластерности Z_1, а за счет свойств Z_2 повысится возможность применения типовых метрик и методик оценки защищенности.

Группа предложения $G_{\{1,2,3\},1,\{1,2,6\},4}$. Применение всего инструментария из компонентов на базе единой архитектуры K_4 для Y_1 исходя из специфик области Z_1, Z_2 и Z_6.

Компоненты K_4 для Y_1 могут применяться путем формирования интегральных оценок текущего состояния элементов ЭС с позиции существующих рисков кибербезопасности как для отдельных объектов сектора (например, аварии энергоблоков АЭС [37]), так и для всей системы в целом (например, с позиции экономики, окружающей среды, безопасности и нераспространения) [38]. Данная возможность обусловлена свойством кластерности Z_1, а за счет свойств Z_2 повысится возможность применения типовых метрик и методик оценки состояния.

Группа предложения $G_{\{1,2,3\},2,\{3,4,6\},4}$. Применение всего инструментария из компонентов на базе единой архитектуры K_4 для Y_2 исходя из специфик области Z_3, Z_4 и Z_6.

Компоненты K_4 для Y_2 могут применяться путем постановки задачи (например, достижение заданного уровня надежности электроснабжения, доведение средней интенсивности отказов и времени обслуживания электрогенераторов до заданных значений и пр. [39]) компонентам поддержки принятия решений, полученной по результатам оценки рисков ЭС. Данная возможность обусловлена применением предложения $G_{\{1,2,3\},1,\{1,2,6\},4}$, обеспечивающего оценку рисков ЭС и формирование путей их недопущения (в виде соответствующих задач для выполнения); также наличие свойств Z_3 и Z_4 повысит точность формирования задач для последующих компонентов за счет стандартности (то есть известности) условий их возникновения.

Группа предложения $G_{\{1,2,3\},1,\{1,2,6\},5}$. Применение всего инструментария из компонентов на базе единой архитектуры K_5 для Y_1 исходя из специфик области Z_1, Z_2 и Z_6.

Компоненты K_5 для Y_1 могут применяться путем визуального отображения большого количества данных касательно состояния объектов ЭС (например, графики распределения электронагрузки, средняя мощность генераторов, точечные значения напряжения, температура и давление различных узлов и пр.) как экспертам отделов безопасности на отдельных территориальных объектах ЭС, так и в единых центрах обеспечения безопасности всей системы электропередач. Данная возможность обусловлена свойством кластерности Z_1, а за счет свойств Z_2 повысится адаптированность визуализации компонентами для эксперта.

Группа предложения $G_{\{1,2,3\},2,\{3,4,6\},5}$. Применение всего инструментария из компонентов на базе единой архитектуры K_5 для Y_2 исходя из специфик области Z_3, Z_4 и Z_6.

Компоненты K_5 для Y_2 могут применяться путем оперативного распознавать аномалии и событий кибербезопасности (например, превышение скорости вращения турбин и нагрева котла, выход качества водно-химического режима на АЭС за допустимые пределы и пр. [40]), полученных из визуального отображения данных касательно состояния объектов ЭС. Данная возможность обусловлена применением предложения $G_{\{1,2,3\},1,\{1,2,6\},5}$, обеспечивающего предоставление таких данных эксперту; также наличие свойств Z_3 и Z_4 повысит эффективность выявления событий кибербезопасности экспертом из-за адаптированности визуальных представлений для ручного анализа.

Группа предложения $G_{\{1,2,3\},3,\{3,4,5,6\},5}$. Применение всего инструментария из компонентов на базе единой архитектуры K_5 для Y_3 исходя из специфик области Z_3, Z_4, Z_5 и Z_6.

Компоненты K_5 для Y_3 могут применяться путем анализа экспертом всех визуально отображаемых данных (например, графики провалов и пропаданий напряжения, роста показателя несинусоидальности напряжения и пр. [41]), предшествующих и связанных с инцидентом кибербезопасности для восстановления доказательств нарушения. Качественное повышение процесса обеспечивается наличием свойств ЭС – Z_3, Z_4 и Z_5, которые позволяют применять единые методики расследования киберпреступлений.

Группа предложения $G_{\{1,2,3\},3,\{3,4,5,6\},6}$. Применение всего инструментария из компонентов на базе единой архитектуры K_6 для Y_3 исходя из специфик области Z_3, Z_4, Z_5 и Z_6.

Компоненты K_6 для Y_3 могут применяться путем проведения расследования кибератак согласно методу (реализованному компонентами), в рамках которого должны производиться следующие основные этапы: сбор и анализ данных (например, от датчиков напряжения, текущих характеристик жидкометаллических теплоносителей и пр.); определение источника атаки – наиболее критичными для ЭС являются технологические процессы, нарушающие подачу электроэнергии или приводящие к ядерным катастрофам; технический анализ показателей и состояний объектов ЭС, сбор которых в данной области является практически обязательным; оценка ущерба, которая в данном случае с большой вероятностью будет высокой и др. Качественное повышение процесса обеспечивается наличием свойств ЭС – Z_3, Z_4 и Z_5, которые позволяют применять единую методику расследования киберпреступлений.

Заключение

В работе представлены предложения по применению научно-технического инструментария в интересах обеспечения кибербезопасности ЭС. Основным результатом исследования является методологический подход формирования предложений, а частными – набор специфик ЭС и полученные группы предложений. Новизна результата заключается в строгой формализации подхода за счет применения теории множеств. Теоретическая значимость состоит в развитии более строгого теоретического подхода для достаточно эвристической задачи по разработке предложений, а практическая значимость – в его непосредственном применении к объектам сферы энергетики.

В дальнейший план работ включены: улучшение детализации полученных групп предложений, применение подхода для других областей, таких как транспортные системы, Умный город [42] и т.д.

Работа выполнена при частичной финансовой поддержке гранта РНФ 21-71-20078.

Список источников

1. Котова О.Ю. Анализ текущего состояния атомной энергетики Российской Федерации и перспективы развития отрасли до 2030 года // Вестник образовательного консорциума Среднерусский университет. Сер.: Экономика и управление. 2023. № 21. С. 88–91.

2. Натальсон А.В. Формирование цифровых компетенций в области кибербезопасности объектов цифровой энергетики // Вестник НЦБЖД. 2023. № 3 (57). С. 54–60.

3. Кибербезопасность систем, реализующих интенсивное использование данных. Часть 1. Место кибербезопасности в защите информации / В.И. Будзко [и др.] // Системы высокой доступности. 2024. Т. 20. № 1. С. 16–29. DOI: 10.18127/j20729472-202401-02.

4. Levshun D., Kotenko I. Application of Intelligent Methods of Correlation of System Events in Predictive Analysis of Security States of Objects of Critical Infrastructure // Pattern Recognition and Image Analysis. 2023. Vol. 33. № 3. P. 389–397. DOI: 10.1134/S1054661823030264.

5. Kotenko I., Izrailov K., Buinevich M. Analytical modeling for identification of the machine code architecture of cyberphysical devices in Smart Homes // Sensors. 2022. Vol. 22. № 3. P. 1–28. DOI: 10.3390/s22031017.

6. Kotenko I., Gaifulina D., Zelichenok I. Systematic Literature Review of Security Event Correlation Methods // IEEE Access. 2022. Vol. 10. P. 43387–43420. DOI: 10.1109/ACCESS.2022.3168976.

7. Сосюра Б.Е. Современное состояние энергетического сектора, последние изменения и энергетическая политика // Вопросы устойчивого развития общества. 2021. № 1. С. 231–237. DOI: 10.34755/IROK.2021.51.39.004.

8. Вашечкина А.В. Правовые проблемы обеспечения информационной (кибер-) безопасности энергетического сектора в условиях цифровизации // Правовой энергетический форум. 2023. № 4. С. 90–97. DOI: 10.61525/S231243500029322-2.

9. Каракаш Н.С., Скляров К.А., Тульская С.Г. Системы безопасности атомных электростанций // Градостроительство. Инфраструктура. Коммуникации. 2023. № 4 (33). С. 41–45.

10. Нуцалханов Г.Н. Современные глобальные угрозы и вызовы ядерного терроризма // International Law Journal. 2019. Т. 2. № 4. С. 121–125.

11. Ястребов А.Е., Ручкин В.Н. Применение геоинформационных технологий в электрических сетях единой энергетической системы России // Информатика и прикладная математика. 2014. № 20. С. 159–166.

12. Parise G., Allegri M., Parise L. Topology of Integrity Resilience for Service Continuity of Critical Loads // In proceedings of IEEE Industry Applications Society Annual Meeting (Baltimore, MD, USA, 29 September 2019 – 3 October 2019). 2019. P. 1–6. DOI: 10.1109/IAS.2019.8912028.

13. Angays P., Tastet J. Design of large power plant in oil and gas facilities // In proceedings of 5th Petroleum and Chemical Industry Conference Europe – Electrical and Instrumentation Applications (Weimar, Germany, 10–12 June 2008). 2008. P. 1–9. DOI: 10.1109/PCICEUROPE.2008.4563526.

14. Скрипник О.Б. Особенности обеспечения экономической безопасности предприятий топливно-энергетического комплекса России // Экономическая безопасность социально-экономических систем: вызовы и возможности: сб. трудов V Междунар. науч.-практ. конф. Белгород. 2023. С. 76–80.

15. Бугаева Т.М., Викторова Н.Г. Особенности управления развитием энергетического комплекса мегаполиса // Экономические науки. 2020. № 190. С. 14–19.

16. Чекалин В.С., Любарская М.А., Ермакова М.Ю. Энергетический комплекс крупного города: проблемы и пути развития // Известия Санкт-Петербургского государственного экономического университета. 2020. № 4 (124). С. 56–62.

17. On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective / L. Xu [et al.] // Renewable and Sustainable Energy Reviews. 2021. Vol. 152. P. 111642.

18. Голиков С.Е. Проблемы внедрения новых подходов к информационной безопасности в энергетической отрасли // Моделирование, оптимизация и информационные технологии. 2020. Т. 8. № 1. С. 42–43.

19. Разработка моделей и методов раннего обнаружения кибератак на объекты энергетики металлургического предприятия / А.Н. Соколов [и др.] // Вестник УрФО. Безопасность в информационной сфере. 2021. № 3 (41). С. 65–87.

20. Govea J., Gaibor-Naranjo W., Villegas-Ch W. Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence // Systems. 2024. Vol. 12. № 5. P. 165.

21. Bohačík A., Fujdiak R. The Problem of Integrating Digital Twins into Electro-Energetic Control Systems // Smart Cities. 2024. Vol. 7. № 5. P. 2702–2740.

22. SecuriDN: A Modeling Tool Supporting the Early Detection of Cyberattacks to Smart Energy Systems / D. Cerotti [et al.] // Energies. 2024. Vol. 17. № 16. P. 3882.

23. Smart Energy Management System Using Machine Learning / A. Akram [et al.] // Computers, Materials & Continua. 2024. Vol. 78. № 1. P. 959–973.

24. Корченко М.Д. Способы применения нейросетей в энергетике // Вестник науки. 2024. Т. 1. № 6 (75). С. 1444–1448.

25. Новоселов Н.Д. Интеграция искусственного интеллекта для энергетической компании // Научный Лидер. 2024. № 3 (153). С. 15–17.

26. Сорокин В.А., Кубриков М.В. Рекуперационное устройство с гравитационным аккумулятором // Актуальные проблемы авиации и космонавтики. 2012. Т. 1. № 8. С. 72–73.

27. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 1. Предпосылки и схема // Вопросы кибербезопасности. 2023. № 3 (55). С. 90–100. DOI: 10.21681/2311-3456-2023-3-90-100.

28. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 2. Алгоритм, модель и эксперимент // Вопросы кибербезопасности. 2023. № 4 (56). С. 80–93. DOI: 10.21681/2311-3456-2023-4-80-93.

29. Курта П.А., Буйневич М.В. Онтологическая модель взаимодействия пользователя с информационной системой в рамках получения услуги информационного сервиса // Вестник кибернетики. 2021. № 2 (42). С. 17–23. DOI: 10.34822/1999-7604-2021-2-17-23.

30. Курта П.А. Взаимодействие пользователя с информационной системой. Часть 1. Схема взаимодействия и классификация недостатков // Известия СПбГЭТУ ЛЭТИ. 2020. № 8–9. С. 35–45.

31. Курта П.А. Взаимодействие пользователя с информационной системой. Часть 2. Алгоритмы обнаружения недостатков // Известия СПбГЭТУ ЛЭТИ. 2020. № 10. С. 34–44.

32. Курта П.А. Взаимодействие пользователя с информационной системой. Часть 3. Оценка эффективности // Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 58–72.

33. Оценивание и прогнозирование состояния сложных объектов: применение для информационной безопасности / К.Е. Израилов [и др.] // Вопросы кибербезопасности. 2022. № 6 (52). С. 2–21. DOI: 10.21681/2311-3456-2022-6-2-21.

34. Рябин Т.В., Сорокин Д.В. Тенденции развития технологии глобальных электрических сетей // Энергия единой сети. 2019. № 2 (44). С. 64–73.

35. Шевченко М.Е. Сравнительный анализ критериев обнаружения аномалий в работе энергетического оборудования // Известия Кыргызского государственного технического университета им. И. Раззакова. 2024. № 2 (70). С. 765–772. DOI: 10.56634/16948335.2024.2.765-772.

36. Краткий отчет о результатах дополнительных анализов защищенности действующих российских АЭС от внешних экстремальных воздействий // Ядерная и радиационная безопасность. 2012. № 1 (63). С. 3–8.

37. Комаров Ю.А. Возможности риск-ориентированного подхода к проблеме повышения надежности и безопасности АЭС // Теплоэнергетика. 2014. № 10. С. 12. DOI: 10.1134/S0040363614090082.

38. Субботин С.А. Актуализация проблем безопасности и стратегия управления жизненным циклом АЭС и атомной энергетикой // Энергия: экономика, техника, экология. 2013. № 4. С. 27–31.

39. Ракутько С.А., Иванникова Н.Ю., Закирова В.Р. Оптимизационные задачи обеспечения надежности энергетических систем методами математического моделирования // Международный технико-экономический журнал. 2019. № 3. С. 7–15. DOI: 10.34286/1995-4646-2019-66-3-7-15.

40. Вилков Н.Я., Крюков Ю.В. Математическое обеспечение ранней идентификации аномалий водно-химического режима на АЭС по данным оперативного химического контроля // Теплоэнергетика. 2000. № 5. С. 25–28.

41. Асосков С., Крупович В., Цапенко А. Решение задач предупреждения и снижения нарушений в работе энергооборудования ООО «Газпром энерго» // Электроэнергия. Передача и распределение. 2013. № 6 (21). С. 142–147.

42. Курта П.А., Коломеец М.В. Обобщенная классификация интерфейсов транспортной инфраструктуры «Умного Города» // Вестник кибернетики. 2020. № 4 (40). С. 6–13. DOI: 10.34822/1999-7604-2020-4-6-13.

References

1. Kotova O.Yu. Analiz tekushchego sostoyaniya atomnoj ehnergetiki Rossijskoj Federacii i perspektivy razvitiya otrasli do 2030 goda // Vestnik obrazovatel'nogo konsorciuma Srednerusskij universitet. Ser.: Ehkonomika i upravlenie. 2023. № 21. S. 88–91.

2. Natal'son A.V. Formirovanie cifrovykh kompetencij v oblasti kiberbezopasnosti ob"ektov cifrovoj ehnergetiki // Vestnik NCBZHD. 2023. № 3 (57). S. 54–60.

3. Kiberbezopasnost' sistem, realizuyushchikh intensivnoe ispol'zovanie dannykh. Chast' 1. Mesto kiberbezopasnosti v zashchite informacii / V.I. Budzko [i dr.] // Sistemy vysokoj dostupnosti. 2024. T. 20. № 1. S. 16–29. DOI: 10.18127/j20729472-202401-02.

4. Levshun D., Kotenko I. Application of Intelligent Methods of Correlation of System Events in Predictive Analysis of Security States of Objects of Critical Infrastructure // Pattern Recognition and Image Analysis. 2023. Vol. 33. № 3. P. 389–397. DOI: 10.1134/S1054661823030264.

5. Kotenko I., Izrailov K., Buinevich M. Analytical modeling for identification of the machine code architecture of cyberphysical devices in Smart Homes // Sensors. 2022. Vol. 22. № 3. P. 1–28. DOI: 10.3390/s22031017.

6. Kotenko I., Gaifulina D., Zelichenok I. Systematic Literature Review of Security Event Correlation Methods // IEEE Access. 2022. Vol. 10. P. 43387–43420. DOI: 10.1109/ACCESS.2022.3168976.

7. Sosyura B.E. Sovremennoe sostoyanie ehnergeticheskogo sektora, poslednie izmeneniya i ehnergeticheskaya politika // Voprosy ustojchivogo razvitiya obshchestva. 2021. № 1. S. 231–237. DOI: 10.34755/IROK.2021.51.39.004.

8. Vashechkina A.V. Pravovye problemy obespecheniya informacionnoj (kiber-) bezopasnosti ehnergeticheskogo sektora v usloviyakh cifrovizacii // Pravovoj ehnergeticheskij forum. 2023. № 4. S. 90–97. DOI: 10.61525/S231243500029322-2.

9. Karakash N.S., Sklyarov K.A., Tul'skaya S.G. Sistemy bezopasnosti atomnykh ehlektrostancij // Gradostroitel'stvo. Infrastruktura. Kommunikacii. 2023. № 4 (33). S. 41–45.

10. Nucalkhanov G.N. Sovremennye global'nye ugrozy i vyzovy yadernogo terrorizma // International Law Journal. 2019. T. 2. № 4. S. 121–125.

11. Yastrebov A.E., Ruchkin V.N. Primenenie geoinformacionnykh tekhnologij v ehlektricheskikh setyakh edinoj ehnergeticheskoj sistemy Rossii // Informatika i prikladnaya matematika. 2014. № 20. S. 159–166.

12. Parise G., Allegri M., Parise L. Topology of Integrity Resilience for Service Continuity of Critical Loads // In proceedings of IEEE Industry Applications Society Annual Meeting (Baltimore, MD, USA, 29 September 2019 – 3 October 2019). 2019. P. 1–6. DOI: 10.1109/IAS.2019.8912028.

13. Angays P., Tastet J. Design of large power plant in oil and gas facilities // In proceedings of 5th Petroleum and Chemical Industry Conference Europe – Electrical and Instrumentation Applications (Weimar, Germany, 10–12 June 2008). 2008. P. 1–9. DOI: 10.1109/PCICEUROPE.2008.4563526.

14. Skripnik O.B. Osobennosti obespecheniya ehkonomicheskoj bezopasnosti predpriyatij toplivno-ehnergeticheskogo kompleksa Rossii // Ehkonomicheskaya bezopasnost' social'no-ehkonomicheskikh sistem: vyzovy i vozmozhnosti: cb. trudov V Mezhdunar. nauch.-prakt. konf. Belgorod. 2023. S. 76–80.

15. Bugaeva T.M., Viktorova N.G. Osobennosti upravleniya razvitiem ehnergeticheskogo kompleksa megapolisa // Ehkonomicheskie nauki. 2020. № 190. S. 14–19.

16. Chekalin V.S., Lyubarskaya M.A., Ermakova M.Yu. Ehnergeticheskij kompleks krupnogo goroda: problemy i puti razvitiya // Izvestiya Sankt-Peterburgskogo gosudarstvennogo ehkonomicheskogo universiteta. 2020. № 4 (124). S. 56–62.

17. On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective / L. Xu [et al.] // Renewable and Sustainable Energy Reviews. 2021. Vol. 152. P. 111642.

18. Golikov S.E. Problemy vnedreniya novykh podkhodov k informacionnoj bezopasnosti v ehnergeticheskoj otrasli // Modelirovanie, optimizaciya i informacionnye tekhnologii. 2020. T. 8. № 1. S. 42–43.

19. Razrabotka modelej i metodov rannego obnaruzheniya kiberatak na ob"ekty ehnergetiki metallurgicheskogo predpriyatiya / A.N. Sokolov [i dr.] // Vestnik URFO. Bezopasnost' v informacionnoj sfere. 2021. № 3 (41). S. 65–87.

20. Govea J., Gaibor-Naranjo W., Villegas-Ch W. Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence // Systems. 2024. Vol. 12. № 5. P. 165.

21. Bohačík A., Fujdiak R. The Problem of Integrating Digital Twins into Electro-Energetic Control Systems // Smart Cities. 2024. Vol. 7. № 5. P. 2702–2740.

22. SecuriDN: A Modeling Tool Supporting the Early Detection of Cyberattacks to Smart Energy Systems / D. Cerotti [et al.] // Energies. 2024. Vol. 17. № 16. P. 3882.

23. Smart Energy Management System Using Machine Learning / A. Akram [et al.] // Computers, Materials & Continua. 2024. Vol. 78. № 1. P. 959–973.

24. Korchenko M.D. Sposoby primeneniya nejrosetej v ehnergetike // Vestnik nauki. 2024. T. 1. № 6 (75). S. 1444–1448.

25. Novoselov N.D. Integraciya iskusstvennogo intellekta dlya ehnergeticheskoj kompanii // Nauchnyj Lider. 2024. № 3 (153). S. 15–17.

26. Sorokin V.A., Kubrikov M.V. Rekuperacionnoe ustrojstvo s gravitacionnym akkumulyatorom // Aktual'nye problemy aviacii i kosmonavtiki. 2012. T. 1. № 8. S. 72–73.

27. Izrailov K.E., Bujnevich M.V. Metod obnaruzheniya atak razlichnogo geneza na slozhnye ob"ekty na osnove informacii sostoyaniya. Chast' 1. Predposylki i skhema // Voprosy kiberbezopasnosti. 2023. № 3 (55). S. 90–100. DOI: 10.21681/2311-3456-2023-3-90-100.

28. Izrailov K.E., Bujnevich M.V. Metod obnaruzheniya atak razlichnogo geneza na slozhnye ob"ekty na osnove informacii sostoyaniya. Chast' 2. Algoritm, model' i ehksperiment // Voprosy kiberbezopasnosti. 2023. № 4 (56). S. 80–93. DOI: 10.21681/2311-3456-2023-4-80-93.

29. Kurta P.A., Bujnevich M.V. Ontologicheskaya model' vzaimodejstviya pol'zovatelya s informacionnoj sistemoj v ramkakh polucheniya uslugi informacionnogo servisa // Vestnik kibernetiki. 2021. № 2 (42). S. 17–23. DOI: 10.34822/1999-7604-2021-2-17-23.

30. Kurta P.A. Vzaimodejstvie pol'zovatelya s informacionnoj sistemoj. Chast' 1. Skhema vzaimodejstviya i klassifikaciya nedostatkov // Izvestiya SPBGEHTU LEHTI. 2020. № 8–9. S. 35–45.

31. Kurta P.A. Vzaimodejstvie pol'zovatelya s informacionnoj sistemoj. Chast' 2. Algoritmy obnaruzheniya nedostatkov // Izvestiya SPBGEHTU LEHTI. 2020. № 10. S. 34–44.

32. Kurta P.A. Vzaimodejstvie pol'zovatelya s informacionnoj sistemoj. Chast' 3. Ocenka ehffektivnosti // Izvestiya SPBGEHTU LEHTI. 2021. № 4. S. 58–72.

33. Ocenivanie i prognozirovanie sostoyaniya slozhnykh ob"ektov: primenenie dlya informacionnoj bezopasnosti / K.E. Izrailov [i dr.] // Voprosy kiberbezopasnosti. 2022. № 6 (52). S. 2–21. DOI: 10.21681/2311-3456-2022-6-2-21.

34. Ryabin T.V., Sorokin D.V. Tendencii razvitiya tekhnologii global'nykh ehlektricheskikh setej // Ehnergiya edinoj seti. 2019. № 2 (44). S. 64–73.

35. Shevchenko M.E. Sravnitel'nyj analiz kriteriev obnaruzheniya anomalij v rabote ehnergeticheskogo oborudovaniya // Izvestiya Kyrgyzskogo gosudarstvennogo tekhnicheskogo universiteta im. I. Razzakova. 2024. № 2 (70). S. 765–772. DOI: 10.56634/16948335.2024.2.765-772.

36. Kratkij otchet o rezul'tatakh dopolnitel'nykh analizov zashchishchennosti dejstvuyushchikh rossijskikh AEHS ot vneshnikh ehkstremal'nykh vozdejstvij // Yadernaya i radiacionnaya bezopasnost'. 2012. № 1 (63). S. 3–8.

37. Komarov Yu.A. Vozmozhnosti risk-orientirovannogo podkhoda k probleme povysheniya nadezhnosti i bezopasnosti AEHS // Teploehnergetika. 2014. № 10. S. 12. DOI: 10.1134/S0040363614090082.

38. Subbotin S.A. Aktualizaciya problem bezopasnosti i strategiya upravleniya zhiznennym ciklom AEHS i atomnoj ehnergetikoj // Ehnergiya: ehkonomika, tekhnika, ehkologiya. 2013. № 4. S. 27–31.

39. Rakut'ko S.A., Ivannikova N.Yu., Zakirova V.R. Optimizacionnye zadachi obespecheniya nadezhnosti ehnergeticheskikh sistem metodami matematicheskogo modelirovaniya // Mezhdunarodnyj tekhniko-ehkonomicheskij zhurnal. 2019. № 3. S. 7–15. DOI: 10.34286/1995-4646-2019-66-3-7-15.

40. Vilkov N.Ya., Kryukov Yu.V. Matematicheskoe obespechenie rannej identifikacii anomalij vodno-khimicheskogo rezhima na AEHS po dannym operativnogo khimicheskogo kontrolya // Teploehnergetika. 2000. № 5. S. 25–28.

41. Asoskov S., Krupovich V., Capenko A. Reshenie zadach preduprezhdeniya i snizheniya narushenij v rabote ehnergooborudovaniya OOO «Gazprom ehnergO» // Ehlektroehnergiya. Peredacha i raspredelenie. 2013. № 6 (21). S. 142–147.

42. Kurta P.A., Kolomeec M.V. Obobshchennaya klassifikaciya interfejsov transportnoj infrastruktury «Umnogo GorodA» // Vestnik kibernetiki. 2020. № 4 (40). S. 6–13. DOI: 10.34822/1999-7604-2020-4-6-13.

Информация о статье:
Статья поступила в редакцию: 13.11.2024; одобрена после рецензирования: 26.11.2024;
принята к публикации: 28.11.2024

The information about article:
The article was submitted to the editorial office: 13.11.2024; approved after review: 26.11.2024;
accepted for publication: 28.11.2024

Информация об авторах:
Израилов Константин Евгеньевич, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (199178, Санкт-Петербург, В.О., 14-я линия, д. 39), кандидат технических наук, доцент, e-mail: konstantin.izrailov@mail.ru, https://orcid.org/0000-0002-9412-5693
Левшун Диана Альбертовна, младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (199178, Санкт-Петербург, В.О., 14-я линия, д. 39), e-mail: gaifulina@comsec.spb.ru, https://orcid.org/0000-0002-5266-8649
Зеличенок Игорь Юрьевич, младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (199178, Россия, Санкт-Петербург, В.О., 14-я линия, д. 39), e-mail: zelichenok@comsec.spb.ru, https://orcid.org/0000-0002-5211-9025

Information about authors:
Israilov Konstantin E., senior researcher at the laboratory of computer security problems of the Saint-Petersburg Federal research center of the Russian academy of sciences (199178, Saint-Petersburg, V.O., 14th line, 39), candidate of technical sciences, associate professor, e-mail: konstantin.izrailov@mail.ru, https://orcid.org/0000-0002-9412-5693
Levshun Diana A., junior researcher at the laboratory of computer security problems of the Saint-Petersburg Federal research center of the Russian academy of sciences (199178, Saint-Petersburg, V.O., 14th line, 39), e-mail: gaifulina@comsec.spb.ru, https://orcid.org/0000-0002-5266-8649
Zelichenok Igor Yu., junior researcher at the laboratory of computer security problems of the Saint-Petersburg Federal research center of the Russian academy of sciences (199178, Russia, Saint-Petersburg, V.O., 14th line, 39), e-mail: zelichenok@comsec.spb.ru, https://orcid.org/0000-0002-5211-9025