26. *Khar'kovskaya T.A., Kremlev A.S., Sabirova D.M., Efimov D.V., Raissi T.* Interval′nyy nablyudatel′ dlya modeli biologicheskogo reaktora [Interval observer for a biological reactor model], *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki.* [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2014, No 3 (91), pp. 39-45.
27. *P'yavchenko T.A., Finayev V.I. Avtomatizirovannyye informatsionno-upravlyayushchiye sistemy* [Automated information and control systems]. Taganrog: Izd-vo TRTU, 2007, 271 p.

**Лужевский Никита Олегович** – Кубанский государственный технологический университет; e-mail: nikitaluzhev97@gmail.com; г. Краснодар, Россия; тел.: 89288833458; ассистент кафедры автоматизации производственных процессов.

**Лубенцов Валерий Федорович** – Кубанский государственный технологический университет; e-mail: vf.lubentsov@yandex.ru; г. Краснодар, Россия; тел.: 89614440061; д.т.н.; доцент; профессор кафедры автоматизации производственных процессов.

**Лубенцова Елена Валерьевна** – Кубанский государственный технологический университет; e-mail: lubentsovaev@mail.ru; г. Краснодар, Россия; тел.: 89034182575; д.т.н.; доцент; профессор кафедры автоматизации производственных процессов.

**Luzhevsky Nikita Olegovich** – Kuban State Technological University; e-mail: nikitaluzhev97@gmail.com; Krasnodar, Russia; phone: +79288833458; assistant professor, Department of Automation of Industrial Processes.

**Lubentsov Valery Fedorovich** – Kuban State Technological University; e-mail: vf.lubentsov@yandex.ru; Krasnodar, Russia; phone: +79614440061; dr. of eng. sc.; associate professor; professor, Department of Automation of Industrial Processes.

**Lubentsova Elena Valeryevna** – Kuban State Technological University; e-mail: lubentsovaev@mail.ru; Krasnodar, Russia; phone: +79034182575; dr. of eng. sc.; associate professor; professor, Department of Automation of Industrial Processes.

УДК 004.81 + 681.5.015 DOI 10.18522/2311-3103-2026-1-164-179

**Д.Н. Богачева, О.В. Лукинова, А.А. Саломатин**

## СЕМАНТИЧЕСКАЯ МОДЕЛЬ ВЛИЯНИЯ ФАКТОРОВ БЕЗОПАСНОСТИ ДЛЯ ОЦЕНКИ КИБЕРУСТОЙЧИВОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

*В современных условиях обеспечение киберустойчивости информационно-телекоммуникационных систем предприятий становится приоритетной задачей, требующей учета сложного взаимодействия множества факторов. Данная работа посвящена исследованию устойчивости информационно-телекоммуникационных систем с точки зрения процессно-ориентированного подхода, который фокусируется на сохранении непрерывного и безопасного функционирования предприятия при возникновении киберинцидентов. При этом одна из существующих сегодня проблем заключается в отсутствии средств системного анализа факторов безопасности, их влияния на общую защищенность бизнес-процессов. Цель исследования заключается в разработке формализованного инструмента, позволяющего прогнозировать уровень устойчивости с учетом функциональных зависимостей между факторами. В качестве основного метода исследования выступает концептуальное семантическое моделирование, позволяющее формализовать причинно-следственные связи между элементами системы. Научная новизна заключается в разработке модели, фиксирующей взаимное влияние угроз и мер противодействия, что позволяет прогнозировать уровень устойчивости информационно-телекоммуникационных систем уже на этапе проектирования. На примере метода оценки корректности параметров оконечных устройств автоматизированной системы управления технологическим процессом продемонстрировано влияние различных факторов на эффективность механизмов защиты нижнего уровня системы. Результаты, представленные в работе, позволяют сократить противоречие между научным и практическим применением процессно-ориентированного подхода, а также могут быть использованы как теоретическая основа для разработки программных инструментов в контексте принятия решений по выбору мер защиты бизнеса на основе баланса между возможным ущербом, ожидаемыми уровнями киберустойчивости, рисков и безопасности в течение всего жизненного цикла информационной системы.*

*Процессно-ориентированный поход; информационная система; киберустойчивость; семантическая модель факторов безопасности; датчик.*

**D.N. Bogacheva, O.V. Lukinova, A.A. Salomatin**

## SEMANTIC MODEL OF SECURITY FACTORS INFLUENCE FOR EVALUATING CYBER RESILIENCE OF INFORMATION SYSTEMS

*In modern conditions, ensuring the cyber resilience of enterprise information and telecommunication systems is becoming a priority task that requires accounting for the complex interaction of numerous factors. This paper investigates resilience of information and telecommunication systems through the lens of a process-oriented approach, which focuses on maintaining continuous and secure enterprise operations in the event of cyber incidents. However, one of the current problems lies in the lack of tools for systematic analysis of security factors and their impact on the overall protection of business processes. The aim of the study is to develop a formalized tool for predicting resilience levels, taking into account functional dependencies between factors. The primary research method is conceptual semantic modeling, which enables the formalization of cause-and-effect relationships between system elements. The scientific novelty consists in the development of a model that captures the mutual influence of threats and countermeasures, allowing for the prediction of information and telecommunication system resilience levels as early as the design stage. Using the method for evaluating the correctness of Industrial Control Systems endpoint parameters as an example, the influence of various factors on the effectiveness of the system's lower-level protection mechanisms is demonstrated. The results presented in the paper help reduce the gap between the theoretical and practical application of the process-oriented approach. They can also serve as a theoretical foundation for developing software tools to support decision-making in selecting business protection measures, based on a balance between potential damage, expected levels of cyber resilience, risks, and security throughout the entire lifecycle.*

*Process-oriented approach; information system; cyber resilience; semantic model of security factors; sensor.*

**Введение.** Одной из наиболее важных особенностей развития современных информационных систем (ИС) следует считать тенденцию к интеграции. Речь идет о функциональной интеграции, интеграции неоднородных информационных ресурсов, интеграции разных способов представления информации для пользователей информационных систем, интеграции информационных и/или вычислительных систем с телекоммуникационными системами, т.е. возникновению класса интегрированных информационно-телекоммуникационных систем (ИТКС), в которых объединяются функции ИС и систем передачи данных.

К классу ИТКС относятся различные распределенные корпоративные информационные системы (КИС):

- системы, обслуживающие предприятия различных отраслей экономики, финансово-кредитной сферы, системы военного назначения и др.;
- государственные ИС, созданные для нужд правоохранительных органов, электронного правительства, осуществления государственных услуг и т.п.;
- глобальные информационные сети, в которых традиционные услуги связи и передачи данных дополняются услугами информационного обслуживания массовых пользователей.

Применение *Web*-технологий в ИТКС обеспечивает развитие таких областей, как электронный бизнес (оптовая, вплоть до виртуальных бирж, и розничная торговля – Интернет-супермаркеты; взаимодействие промышленных предприятий с потребителями и поставщиками – *business-to-business*), электронные библиотеки, дистанционное обучение (вплоть до виртуальных университетов).

ИТКС представляют собой наиболее сложный класс современных ИС с точки зрения методов и средств их создания, сопровождения и развития, инструментов проектирования и программирования приложений, средств представления информационных ресурсов и доступа к ним.

Очевидно, что к ИТКС предъявляются повышенные требования, в том числе и к вопросам устойчивого функционирования по отношению к внешним негативным воздействиям нарушителя, например, несанкционированному доступу к данным при их

хранении, обработке и передаче по каналам связи или организации распределенных *DOS*-атак. Анализ источников позволяет сделать вывод о том, что устойчивость ИС рассматривается в следующих взаимосвязанных аспектах.

1. Структурно-топологическая устойчивость сетевого слоя ИТКС. В работе [1] приведено определение инфраструктурной устойчивости: «способность инфраструктуры при возмущении системы оставаться на заданном качественном уровне на фоне высокого уровня инфраструктурного деструктивизма». Под инфраструктурным деструктивизмом здесь понимается неспособность какого-либо компонента ИТКС выполнять свои функции в полном объеме.

2. Функциональная устойчивость. В руководстве по оценке мер безопасности в федеральных информационных системах [2], опубликованном Национальным институтом стандартов и технологий США (*NIST*), в исследованиях [3–7] вводится понятие функциональной устойчивости как способность сохранения и/или восстановления возможности выполнения возложенных на систему функций при различных условиях существования, в том числе и при деструктивных воздействиях на ее элементы.

3. Киберустойчивость. В работе [2] киберустойчивость определяется как способность предвидеть, выдерживать, восстанавливаться и адаптироваться к неблагоприятным условиям, атакам или компрометациям ИТ-систем. Всемирный экономический форум (*WEF*) определяет киберустойчивость как способность организации минимизировать влияние существенных киберинцидентов на ее основные бизнес-цели и задачи. Здесь прослеживается связь с методологией, описанной в [8–10], где речь идет о том, что систему защиты ИС необходимо планировать, проектировать и эксплуатировать исходя из обеспечения безопасности бизнес-процессов организации. Среди стратегий обеспечения основ киберустойчивости эксперты *WEF* называют управление рисками. Риск – это потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов. Определяется как функция от вероятности реализации угрозы, использующей уязвимости, и оценки величины ущерба, как последствия реализации угрозы [11, 12]. Управление рисками включает: определение профиля рисков; назначение явных владельцев конкретных рисков и определение ответственности в случае их наступления; планирование и внедрение мер снижения и смягчения рисков; соблюдение регуляторных требований [13]. В работе [14] также рассматривается связь между устойчивостью и рисками негативных воздействий на компоненты ИТКС. Для каждого компонента экспертами задаются критерии – свойства безопасности (конфиденциальность, целостность и доступность), а также коэффициенты важности, степень уязвимости актива и степень реализации угрозы по каждому критерию. Эти параметры авторы используют для расчета рисков нарушения свойств безопасности, посредством которых, в свою очередь, оценивается совокупная мера риска всей ИТКС. В работе [15] авторы подчеркивают, что наиболее важной составляющей в обеспечении киберустойчивости и, как следствие, общей устойчивости, является именно оценка рисков, т.к. именно регулярный анализ рисков помогает разработать эффективные стратегии защиты, а также минимизировать вероятность различных кибератак.

Кроме того, повсеместное развитие цифровой экономики требует от бизнес-структур непрерывного функционирования, что, в свою очередь, реализуемо только при внедрении в жизненный цикл ИТКС принципов процессно-ориентированного подхода [16], которые переводят фокус внимания защиты с информационной системы на бизнес-организацию предприятия.

Тогда очевидно, что возникает проблема в разработке таких инструментов, которые позволили бы еще при создании ИС прогнозировать уровень ее устойчивости к воздействиям различных инцидентов, инициируемых злоумышленниками.

Для решения указанной задачи в данной работе предлагается семантическая модель, предназначенная для оценки влияния факторов безопасности на риски и киберустойчивость при проектировании или эксплуатации ИТКС. При этом модель учитывает расширенный (по сравнению с классическим) набор параметров безопасности, отражает принципы процессно-ориентированного подхода, включает концепт целевой функции, содер-

жит контуры принятия решений в разных парадигмах управления безопасностью и может служить формализованной основой для создания программных инструментов указанного подхода.

**Постановка задачи.** На сегодняшний день существует два основных подхода к проектированию систем обеспечения безопасности ИС. Первый – традиционный, классический, основан на удовлетворении требований нормативно-правовых документов [17–19], которые в качестве объекта защиты определяют саму целевую ИС, а также фокусируются на барьерных мерах по защите периметра ИС за счет встроенных и наложенных средств защиты (СЗ). Основная направленность этого подхода – противодействие предполагаемым угрозам в целях предотвращения несанкционированного доступа, сохранения целостности, обеспечения доступности данных, хранящихся и обрабатываемых в системе. Поэтому главным требованием регуляторов информационной безопасности (ИБ) является наличие для защищаемой системы модели угроз, т.е. моделей нарушителя, уязвимостей, а также потенциально возможных атак, противовесом которых являются механизмы и средства защиты.

Однако в современных условиях глобального интернета, когда размывается само понятие «защищаемый периметр» вследствие использования облачных сервисов; когда резко возросло количество кибератак и технических возможностей нарушителей для их осуществления; когда усложнились архитектуры систем; когда многократно возросла потребность в оценке влияния киберрисков на бизнес-цели, возникла новая парадигма – процессно-ориентированный подход. Первыми публикациями в этой области, в которых изложены базовые принципы новой методологии, можно считать [9, 10]. Эти принципы апеллируют к бизнес-процессному подходу, стандартам *ITIL* [20] и заключаются в том, что, в отличие от традиционной парадигмы, требования к безопасности информационной инфраструктуры предприятия необходимо выстраивать исходя из безопасного функционирования бизнес-процессов организации, их информационных потоков и функций. Следовательно, объектом защиты становятся бизнес-процессы компании, а не информационная система, которая в соответствии с *ITIL*, является лишь способом реализации бизнес-процесса, его ресурсом.

Таким образом, процессно-ориентированный подход представляет собой методологию, ориентированную на обеспечение безопасной и непрерывной деятельности бизнеса, методически основываясь на том, что свойства безопасности (конфиденциальность (*K*), целостность (*C*), доступность (*D*)) становятся атрибутами бизнес-процесса и, одновременно, требованиями безопасности, предъявляемыми к защите приложений и платформы информационной системы. Другими словами, вектор $\overline{KS} = \{K, C, D\}$ будет являться целевым при проектировании системы безопасности ИТКС. Тогда очевидно, что риски ИБ – это лишь один из подчиненных аспектов управления бизнес-рисками предприятия и, если они становятся для предприятия актуальными, то ИБ-защита выступает способом минимизации общих рисков. Международные и отечественные стандарты и методологии по управлению рисками [16, 21], начиная с десятых годов 21 века, также фиксируют основные положения процессно-ориентированного подхода. Так, стандарт NIST SP 800-39 «Managing Information Security Risk» [16] прямо описывает трехуровневую модель управления рисками: организация, бизнес-процессы, информационные системы, которая предписывает на уровне ИС реализовать все требования по управлению рисками ИБ, которые были приняты на бизнес-уровне. Кроме того, вводится понятие устойчивости ИС как показатель жизнеспособности бизнес-функций компании. Отечественный ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска» [21] апеллирует к 607-П ЦБ РФ «О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков». Методология *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)* используется для моделирования и оценки рисков как информационных систем, так и критических бизнес-активов компании. В стандарте ISO/IEC 27005:2018 [22] декларируется тот факт, что оценка рисков должна осуществляться с учетом последствий рисков для бизнеса.

Однако следует заметить, что, несмотря на наличие документов и публикаций, декларирующих положения прогрессивного подхода, в области практического использования указанных стандартов существуют следующие проблемы. Во-первых, нормативные документы носят исключительно рекомендательный характер. Во-вторых, несмотря на достаточно развитые теоретические и нормативные основания процессной методологии, наличие средств по моделированию угроз, анализу уязвимостей программного обеспечения ИС и пр., на практике существует потребность в таких моделях, методах и инструментах, которые воплощали бы процессно-ориентированную идеологию.

Таким образом, целью данного исследования является разработка модели, позволяющей оценивать взаимовлияние различных факторов ИБ при выборе механизмов и средств защиты от воздействия киберинцидентов, минимизирующих риски и повышающих устойчивое функционирование как ИТКС, так бизнес-процессов.

Для достижения указанной цели в ходе исследования необходимо выполнить следующие задачи:

1. Расширить, систематизировать и формализовать перечень ключевых факторов ИБ, влияющих на киберустойчивость и позволяющих проводить более детализированный анализ;
2. Разработать концептуальную семантическую модель, устанавливающую причинно-следственные связи между факторами безопасности. На основе модели выделить и проанализировать управленческие контуры, соответствующие различным парадигмам обеспечения безопасности (классической, ориентированной на риски, процессной и комплексной).
3. Показать, как экземпляр концепта механизмов защиты, реализованный на основе метода оценки корректности параметров оконечных устройств (датчиков) [23, 24], и расширяющий номенклатуру существующих средств, может быть использован при оценке анализа защищенности автоматизированных систем управления технологическим процессом (АСУ ТП).

Решение этих задач позволит создать формализованный аппарат для комплексного анализа факторов киберустойчивости, связывающий технические средства защиты с бизнес-требованиями и управлением рисками, который может быть реализован в качестве ядра системы поддержки принятия решений для выбора рационального набора защитных мер вдоль всего жизненного цикла системы.

**Семантическая модель влияния факторов информационной безопасности.** Для решения поставленной задачи в работе был выбран аппарат семантического моделирования, который широко применяется в области информационной безопасности. Наиболее распространенными среди них являются следующие средства.

1. Онтологические модели.

Онтологические модели применяются для систематизации основных понятий предметной области, позволяя связать виды угроз, их взаимовлияния друг на друга и на остальные концепты кибербезопасности [25].

Примеры онтологий в области кибербезопасности приведены в работах [26, 27].

Онтологические модели обычно описывают с использованием формальных языков разметки *Web Ontology Language (OWL)* и *Resource Description Framework (RDF)* [28].

*OWL* позволяет создавать чёткие и однозначные структуры данных, удобные для автоматической обработки и анализа. Основываясь на логике первого порядка, *OWL* способен представлять сложные связи и ограничения между классами и свойствами, что делает его незаменимым инструментом для задач, требующих строгой формализации данных. Его ключевые преимущества включают высокую выразительную мощность, возможность логического вывода и поддержку семантического анализа данных. Однако сложность создания больших онтологий и высокие требования к производительности остаются основными препятствиями для массового внедрения.

*RDF* организует данные в виде триплетов «субъект-предикат-объект», что позволяет описывать любые сущности и их свойства в унифицированном формате. *RDF* подходит для описания разнообразной информации, совмещается с другими стандартами, способен легко внедряться в существующее программное обеспечение за счет подключае-

мых модулей и библиотек для различных языков программирования. Однако у *RDF* есть и ограничения, связанные с относительно низкой производительностью при работе с большими объёмами данных и недостатком встроенных средств проверки целостности.

2. Когнитивные карты.

Когнитивные карты, как показывает анализ, в ИБ зачастую применяются для моделирования угроз и оценки рисков. Они показывают потенциальные направления угроз, включая зоны наибольшего риска, пути движения злоумышленников и потенциальные последствия успешных атак. Они помогают организациям наглядно оценить свои слабые места и спланировать эффективные меры защиты.

Среди карт угроз распространены нечеткие когнитивные карты (НКК). Они являются удобными в использовании, имеют возможность учитывать неопределённость и нечеткость в процессе оценки рисков, способны изменяться и адаптироваться в соответствии с новыми данными и требованиями [29]. НКК используется для решения задач, связанных с определением и оценкой влияния факторов ситуации, а также для получения прогнозов развития ситуации на основе вычисленных влияний. Основные элементы, необходимые при создании НКК: узлы, связи, матрица весов связей, функция активации, обучение и обновление, распространение активации.

Другими известными примерами когнитивных карт выступают *Spoofing, Tampering, Repudiation, Infromation Disclosure, Denial of Service, Elevation of Privilege (STRIDE)* и *Process for Attack Simulation and Threat Analysis (PASTA)* [30–33].

*STRIDE* направлен на идентификацию, классификацию и последующую нейтрализацию потенциальных угроз. Рассматривается шесть основных типов угроз, учитываемых в *STRIDE*.

1. *Spoofing* (Подделывание идентичности). Атака, при которой злоумышленники пытаются выдавать себя за доверенного пользователя или систему.
2. *Tampering* (Манипулирование данными). Угроза нарушения целостности данных путём несанкционированного изменения их содержания.
3. *Repudiation* (Отказ от обязательств). Угроза, направленная на уязвимость, позволяющую пользователям отрицать совершение определенных действий.
4. *Information Disclosure* (Раскрытие конфиденциальной информации). Угроза утечки конфиденциальной информации вследствие неправильного конфигурирования систем или наличия уязвимых точек входа.
5. *Denial of Service* (Отказ в обслуживании). Угроза снижения доступности ресурса для легитимных пользователей, приводящая к перегрузке или выходу системы из строя.
6. *Elevation of Privilege* (Повышение привилегий). Угроза получения злоумышленником большего набора прав и возможностей в системе, чем предусмотрено правилами безопасности.

Анализ угроз с использованием *STRIDE* включает несколько ключевых шагов.

1. Идентификация компонентов системы, подлежащих защите.
2. Классификация угроз по одной из шести категорий, приведенных выше.
3. Оценка вероятности возникновения угроз и потенциального ущерба.
4. Выбор мер противодействия каждому типу угроз.
5. Реализация мер защиты.

*PASTA* позволяет проводить всестороннюю оценку и минимизацию рисков безопасности путем моделирования атак и анализа угроз. Основные этапы процесса *PASTA* следующие.

*Этап 1.* Сбор и анализ информации. Всестороннее исследование системы с оценкой важнейших активов и потенциальных уязвимых точек.

*Этап 2.* Имитация атаки. Моделирование реального хода атаки и подбор средств, которые могли бы использовать злоумышленники.

*Этап 3.* Анализ последствий. Оценка ущерба, который мог бы быть нанесён системой в результате успешной атаки.

*Этап 4.* Выбор мер защиты. Определение и реализация необходимых защитных мер для минимизации рисков и повышения устойчивости системы.

3. Базы знаний угроз.

Базы знаний угроз содержат информацию о существующих угрозах, уязвимостях и методах атак, делая выявление и устранение рисков более оперативным. Наиболее известными примерами баз знаний угроз являются: *MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)* и *Common Vulnerability Scoring System (CVSS)* [34, 35].

*MITRE ATT&CK* служит для описания поведения злоумышленников и их тактик, техник и процедур при проведении кибератак. Она состоит из трех основных матриц, каждая из которых ориентирована на определенный тип целевого окружения.

1. *Enterprise Matrix*. Охватывает техники атак на рабочие станции и серверы, функционирующие под управлением операционных систем *Windows, macOS, Linux* и других платформ.
2. *Mobile Matrix*. Фокусируется на методах атак на мобильные устройства *Android* и *iOS*.
3. *PRE-ATT&CK Matrix*. Описывает подготовительный этап перед осуществлением атаки, включая разведку угроз и подготовку инфраструктуры.

*CVSS* позволяет измерить и сравнить уязвимости, присваивая каждой из них единую оценку, варьирующаяся от нуля до десяти, со следующими соответствиями:

- 0–3,9 – низкий уровень риска;
- 4,0–6,9 – средний уровень риска;
- 7,0–8,9 – высокий уровень риска;
- 9,0–10 – чрезвычайно высокий уровень риска.

Сначала рассчитывается базовая оценка, включающая доступность, воздействие, степень потенциального ущерба атаки и прочие факторы. Затем применяются поправки временной оценки, такие как наличие работающего средства исправлений уязвимости, их доступность и уровень осведомленности о проблеме. Наконец, дополнительно уточняют значение экологическими показателями: важностью системы, критичностью данных, значимостью возможного нарушения функционирования системы.

Несмотря на преимущества описанных моделей, они обладают рядом значимых недостатков. Онтологические модели хоть и основаны на принципах формальной строгости и предопределенные правила, но характеризуются низкой адаптивностью и масштабируемостью. Когнитивные карты угроз хорошо подходят для визуализации и первичного анализа направлений атак, но ограничены в возможностях по формированию сложных логических конструкций и выполнению автоматизированного анализа. Базы знаний угроз, такие как *MITRE ATT&CK* и *CVSS*, собирают обширную информацию о текущих угрозах и уровнях риска, но не предоставляют инструментов для оперативной аналитики и моделирования сценариев угроз.

Использование предлагаемой семантической является, в данном случае, более предпочтительным, поскольку она:

- расширяет таксономию концептов, необходимых для оценки устойчивости и управления рисками с учетом функциональных зависимостей между ними;
- обеспечивает полноту учета факторов безопасности, позволяющих получать более детализированную оценку средств защиты при проектировании ИТКС;
- реализует адаптивное управление рисками, создавая условия для комплексного мониторинга киберустойчивости и бизнес-процессов в ходе эксплуатации ИТКС;
- включает в себя формализованную целевую функцию системы защиты ИТКС, отражающую основные свойства безопасности, предъявляемые к информационным потокам и функциям бизнес-процессов.

Рассмотрим концептуальную модель (КМ), представленную на рис. 1 и разработанную с использованием аппарата семантических сетей. Первоначально она была представлена в работе [36]. В данном исследовании модель была переосмыслена и модифицирована с точки зрения оценки киберустойчивости.

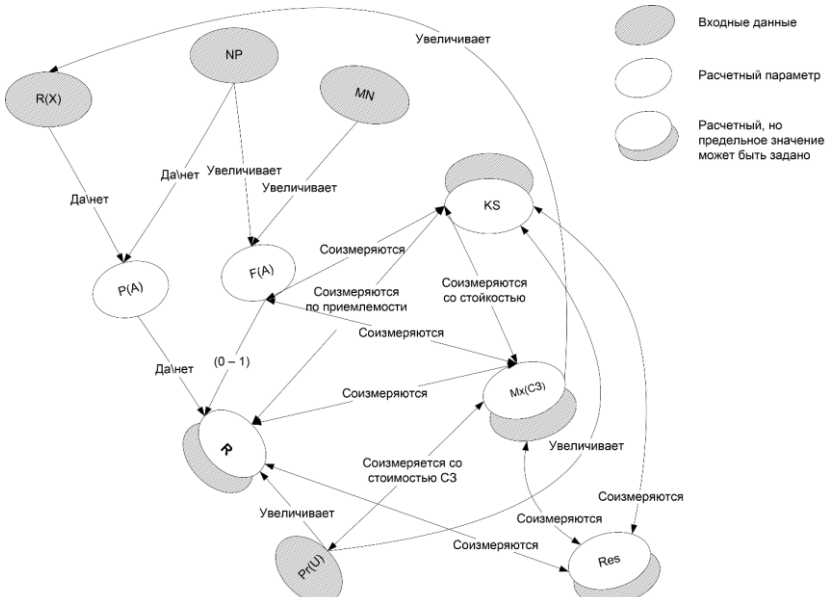


*Рис. 1. Концептуальная модель влияния факторов безопасности ИТКС*

Здесь вершины графа интерпретируются следующим образом:

1. *NP* – потенциал нарушителя, оцениваемый на основании его возможностей;
2. *R(X)* – рейтинг уязвимости компонентов системы, составленный на основе оценок частоты использования уязвимости нарушителем и трудности ее обнаружения;
3. *MN* – мотивация нарушителя, оцениваемая экспертами;
4. *P(A)* – возможность осуществления угрозы (атаки) нарушителем, который обладает потенциалом *NP* и сможет воспользоваться уязвимостью с рейтингом *R(X)*;
5. *F(A)* – сила (мощность) атаки, ассоциируемая с ресурсами (усилиями), необходимыми для преодоления стойкости защитных механизмов;
6. $\overline{KS}$={*K, C, D*} – целевая функция безопасности, которую должна обеспечивать система защиты ИТКС на заданном уровне, представляет собой вектор основных свойств безопасности, предъявляемых к информационным потокам и функциям бизнес-процессов предприятия. Для измерения компонентов вектора $\overline{KS}$ вводятся оценочные шкалы «Уровень конфиденциальности» (*K*), «Уровень целостности» (*C*) и «Уровень доступности» (*D*) в пространстве лингвистических переменных;
7. *Pr(U)* – ценность информационных ресурсов, используемых при выполнении функций бизнес-процесса. Ценность ресурсов определяет и ущерб, наносимый атакой;
8. *R* – риск получения ущерба *Pr(U)* в случае нарушения критериев $\overline{KS}$ и осуществления атаки; риск выступает интегральным фактором-посредником, связывающим угрозы, ценность актива (Pr(U)) и требования безопасности.
9. *Mx(C3)* – защитные механизмы, реализуемые программно-аппаратными средствами;
10. *Res* – устойчивость информационной системы к нарушению вектора $\overline{KS}$.

Если потенциал нарушителя, оцениваемый его возможностями, превосходит рейтинг уязвимостей *NP* > *R(X)*, то атака *A*, в принципе, возможна. Но данные отношения могут принимать значения «да\нет», т.е. возможна\невозможна. Чтобы оценить степень возможности, надо рассмотреть и другие факторы. В частности, потенциал нарушителя, т.е. его степень профессионализма, знания о системе, используемые средства и т.п. напрямую влияют на силу атаки (<*NP*, «увеличивает», *F(A)*>) (здесь и далее влияние измеряется экспертной нормированной шкалой от нуля до единицы). На силу атаки огромное влияние имеет также мотивация нарушителя *MN*. Если она велика, то, и, не имея собственных возможностей, он может нанять профессионала, поэтому имеет место связь <*MN*, «увеличивает», *F(A)*>.

Влияние концепта *Pr(U)* (ценность/ущерб) на систему представленных в КК понятий сказывается следующим образом:

а) ценностью определяется требуемый уровень безопасности информационной системы *(<Pr(U)*, «увеличивает», $\overline{KS}$ *>);*

б) от величины оценки ущерба зависит показатель риска *R* (<*Pr(U)*, «увеличивает», R>);

в) потенциальный ущерб следует соизмерять со стоимостью системы защиты, по крайней мере, для коммерческих предприятий *(<Pr(U)*, «соизмеряется», *Mx(C3)>*).

Механизмы защиты *Mx*, с одной стороны, обеспечивают безопасность и выбираются в соответствии с уровнем критериев *(<Mx(C3)*, «соизмеряется», $\overline{KS}$>), а с другой – противостоят силе атаки *F(A)*. А это значит, что силу атаки, в силу транзитивности, можно структурировать измерительными шкалами критериев безопасности и имеет место отношение <*F(A)*, «соизмеряется», >.

Величина рисков предприятия *R* при нарушении уровня зависит от трех причин:

а) возможности осуществимости атаки *P(A)* (<*P(A)*, «да/нет»), *R*>);

б) величины оценки ущерба *(<Pr(U)*, «увеличивает», *R*>);

в) силы атаки (<*F(A)*, «(0 – 1)», *R*>).

В свою очередь, показатель риска *R* оказывает влияние на выбор СЗ: чем выше величина риска, тем более стойкие механизмы и СЗ надо выбирать и наоборот (<*R*, «соизмеряется», *Mx(C3)>*).

Управление рисками реализуется двусторонней связью <$\overline{KS}$ , «соизмеряются», *R*>. Семантика связи заключается в том, чтобы после выбора *Mx*, обеспечивающих требуемый уровень $\overline{KS}$, произвести оценку будущего риска при данном наборе защитных средств (это можно сделать благодаря связи *<Mx(C3)*, «увеличивает», *R(X)>*, которая говорит о том, что средства защиты выбранного набора изменяют величину исходного риска) и сделать вывод о его приемлемости. Если риск неприемлем, берется другой набор *Mx(C3)* и производится сближение оценок и по рискам *R*, и по уровню безопасности.

Устойчивость *Res* напрямую зависит от используемых в системе защиты ИТКС защитных механизмов *Mx(C3)* (<*Res*, «соизмеряется», *Mx(C3)>*). При этом требования к уровню устойчивости предъявляются исходя из установленного $\overline{KS}$.

Вывод об уровне устойчивости ИТКС строится на основании оценивания риска (приемлем/неприемлем). Для этого после выбора *Mx(C3)*, обеспечивающих требуемый уровень $\overline{KS}$, необходимо произвести оценку будущего риска при данном наборе защитных средств (это можно сделать благодаря связи *<Mx(C3)*, «соизмеряется», *R(X)>*, которая говорит о том, что средства защиты выбранного набора изменяют величину исходного риска) и сделать вывод о его приемлемости. Если риск неприемлем, берется другой набор *Mx(C3)* и производится сближение оценок и по рискам *R*, и по уровню безопасности $\overline{KS}$.

На КМ можно выделить несколько контуров, которые отражают различные парадигмы управления безопасностью при организации защиты ИТКС. Каждый контур образован двунаправленными отношениями. Это означает, что происходит взаимовлияние факторов и, стало быть, выбор той или иной вершины в качестве цели при принятии решения по выбору вариантов определит направление стрелок и выбор генеральной стратегии политики безопасности предприятия. Ниже описаны некоторые из них:

*Контур 1.* Образован вершинами *F(A),* $\overline{KS}$*, Mx(C3)*. Отражает идею управления безопасностью с двух точек зрения: классической (на основании модели нарушителя) и процессной.

*Контур 2*. Вершины *F(A), R, Mx(C3)*. Отражает политику, требующую разработки повышенных требований к безопасности, основанную на управлении рисками [37].

*Контур 3*. Вершины $\overline{KS}$*, R, Mx(C3)*. Отражает идею управления безопасностью ИТКС, исходя из оптимального баланса остаточных рисков и уровня безопасности.

*Контур 4.* Вершины $\overline{KS}$*, R, Mx(C3), Res*. Отражает комплексный подход к управлению безопасностью ИТКС с учетом требуемого уровня безопасности, а также оценок устойчивости и рисков.

Вершина *Res* наглядно показывает взаимосвязи устойчивости с остальными концептами предметной области (как прямые, так и косвенные). Она представляет собой эмерджентное свойство всей системы, возникающее из взаимодействия перечисленных факторов. Это позволяет выбрать оптимальную политику управления при некотором требуемом уровне устойчивости, что особенно важно при обеспечении безопасности ИТКС предприятия.

**Применение метода оценки параметров оконечных устройств.** Механизмы защиты от информационных угроз, представленные в КМ концептом *Mx(СЗ),* напрямую влияют на устойчивость как ИТКС в целом, так и отдельных ее компонентов. В работе [38] представлена следующая классификация защитных средств и механизмов на группы.

*Группа 1: основные (или целевые).* Механизмы, обеспечивающие основные свойства безопасности *K, C, D*. Используют дискреционный метод доступа, мандатный метод доступа, ролевое управление доступом и т.д.

*Группа 2: обеспечивающие.* Механизмы, осуществляющие дополнительные действия, необходимые для функционирования целевых *Mx* на том или ином уровне безопасности (например, идентификация, аутентификация, криптографическая поддержка, межсетевые экраны и т.д.)

*Группа 3: Управляющие.* Механизмы, которые обеспечивают согласованное функционирование *Mx* первой и второй групп:

- мониторинг и аудит событий, происходящих в системе;
- анализ защищенности, т.е. выявление и анализ уязвимостей;
- оценка рисков, сопровождающих функционирование системы;
- администрирование системы безопасности:

В работах [23, 24] авторами был разработан метод оценки корректности параметров оконечных устройств (устройств нижнего уровня) АСУ ТП, являющийся, по сути, компонентом средства мониторинга и анализа защищенности (САЗ) и принадлежащий к группе 3 вышеуказанной классификации (управляющий механизм защиты). Нижний уровень автоматизированных систем управления технологическими процессами, как правило, представлен датчиками, счетчиками, исполнительными механизмами, а также контроллерами, передающими данные от указанных оконечных устройств далее, в верхние уровни системы. Алгоритм предполагает создание комплексных отпечатков (КО) датчиков и их последующее сравнение. Комплексный отпечаток состоит из цифрового отпечатка, основанного на динамической модели сигнала датчика, и аналогового отпечатка, который строится на основе параметров сигнала датчика на технологической шине. Посредством сравнения эталонного КО устройства с текущим КО (с определенной периодичностью или по запросу оператора) можно сделать вывод о подмене или неисправности устройства, т.е. оценить корректность данных, им передаваемых. Предполагается, что при неудовлетворительной оценке осуществляется необходимое управляющее воздействие (как правило, физическая проверка датчика, работы по его ремонту или замене и т.д.).

Рассмотрим использование описанного метода в управленческом контуре 4.

Алгоритм метода, будучи экземпляром *Mx(СЗ)* группы 3, осуществляет анализ уровня защищенности и его влияние на уровень киберустойчивости системы (*Res*), поскольку направлен на своевременное обнаружение некорректного сигнала от датчика. Такой сигнал может быть свидетельством как воздействия внутреннего нарушителя, так и выхода устройства из нормального режима работы в результате повреждения, устаревания и т.д.

Использование рассматриваемого алгоритма снижает риски (*R*) возникновения следующих событий:

- подмена сигнала устройства внутренним нарушителем;
- подмена самого устройства внутренним нарушителем;
- выход устройства из строя вследствие неисправности или устаревания.

Величина, на которую снижаются эти риски, определяется исходя из «жесткости» требований, задаваемых $\overline{KS}$. Можно настроить систему поддержки принятия решений с данным САЗ так, что она будет требовать проверку датчика при даже самом малом отклонении от эталонного отпечатка: это значительно понизит риски, но при этом может быть экономически нецелесообразно. Поэтому так важно верно определить $\overline{KS}$ исходя из необходимого уровня защиты системы.

Значение вектора $\overline{KS}$ опосредованно определяет следующее.

1. Диапазоны значений шкалы оценки отклонения от эталонного отпечатка. В зависимости от требуемого уровня безопасности могут быть заданы разные интервалы для значений «норма», «рекомендуется проверка», «требуется проверка». Например, при высоких требованиях $\overline{KS}$ в системах, относящимся к критическим информационным инфраструктурам, шкала оценки отклонения может принимать вид, представленный в табл. 1.

Таблица 1

**Шкала оценки отклонения от эталонного отпечатка (пример)**

| Величина отклонения, % | Оценка |
|---|---|
| 0-1 | норма |
| 1-5 | рекомендуется проверка |
| 5-100 | требуется проверка |

2. Частота обновления эталонных отпечатков. Чем выше требования по безопасности, тем чаще необходимо актуализировать эталонные отпечатки, чтобы величина отклонения при штатном функционировании датчика не превышала установленное пороговое значение для «нормы» (к примеру, вследствие сезонности).

3. Частота сравнения отпечатков. Здесь высокие требования по безопасности могут означать, что устройства нужно опознавать по их текущим комплексным отпечаткам как можно чаще.

Из рис. 1 видно, что все вышеупомянутые концепты КМ оказывают прямое влияние на работу алгоритма; в зависимости от требований и условий работы его параметры могут быть изменены.

**Заключение.** Из всего многообразия видов устойчивости систем (структурная-топологическая, организационная, функциональная, процессная и т.п.) для исследования в рамках данной работы была выбрана устойчивость информационной системы к различным видам компрометаций и факторам неблагоприятных условий и инцидентов с точки зрения информационной безопасности.

Результаты, представленные в статье, позволяют осуществлять оценку влияния различных факторов информационной безопасности на уровень риска и киберустойчивости ИТКС. Для этого была создана семантическая концептуальная модель влияния факторов информационной безопасности, таких как рейтинг уязвимостей программного обеспечения, возможности нарушителя и его мотивы, свойства безопасности в составе целевого вектора $\overline{KS}$, механизмы и средства защиты, уровень киберустойчивости и т.д. На основе данной модели появляется возможность прогнозировать уровень риска/киберустойчивости при воздействиях различных факторов безопасности систем защиты ИТКС. Для этого выделены несколько контуров управления. Следует отметить, что разработанная модель отражает принципы процессно-ориентированного подхода к защите информационных систем.

Показано, что метод оценки корректности параметров оконечных устройств систем управления технологическими процессами в данной модели реализуется как экземпляр управляющих механизмов концепта модели «*Мх(СЗ)*» во множестве средств защиты, для чего приведена классификация механизмов защиты. Кроме того, представлена процедура, демонстрирующая встраивание данного метода в контекст модели.

В перспективе авторы планируют продолжение исследований в области теоретической проработки управленческого аспекта модели, а также ее программной реализации как средства поддержки принятия решений при проектировании и эксплуатации систем обеспечения безопасности ИТКС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. *Максимова Е.А., Садовникова Н.П.* Оценка инфраструктурной устойчивости субъекта критической информационной инфраструктуры при деструктивных воздействиях // Известия ЮФУ. Технические науки. – 2021. – № 4 (221). – С. 155-165. – DOI: 10.18522/2311-3103-2021-4-155-165.
2. *Ross R., Johnson L.* Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, Special Publication (NIST SP). – Gaithersburg MD: National Institute of Standards and Technology. 2010. – 399 p.
3. *Воеводин В.А.* Модель оценки функциональной устойчивости элементов информационной инфраструктуры для условий воздействия множества компьютерных атак // Информатика и автоматизация. – СПб.: ФИЦ РАН, 2023. – Т. 22, № 3. – С. 691-715. – DOI: 10.15622/ia.22.3.8.
4. *Тарасов А.А.* Функциональная устойчивость компьютерных систем как фактор обеспечения их информационной безопасности // Информационная безопасность России в условиях глобального информационного общества: Сб. материалов 3-й Всерос. конф. – М., 2002. – С. 193-200.
5. *Бородакий Ю.В., Лободинский Ю.Г.* Информационные технологии. Методы, процессы, системы. – М.: Радио и связь, 2002. – 451 с. – ISBN 5-256-01566-4.
6. *Королев А.Н.* Функциональная устойчивость навигационно-информационных систем // Известия вузов. Приборостроение. – 2018. – Т. 61, № 7. – С. 559-565. – DOI: 10.17586/0021-3454-2018-61-7-559-565.
7. *Бородакий Ю.В., Тарасов А.А.* О функциональной устойчивости информационно-вычислительных систем // Известия ЮФУ. Технические науки. – 2006. – № 7. – С. 5-12.
8. *Лукинова О.В.* Компьютерные методы и алгоритмы управления безопасностью информационных систем. – М.: ИПУ РАН, 2014. – 248 с.
9. *Лукинова О.В.* Формализация задачи планирования защиты распределенной компьютерной сети на основе бизнес-процессного подхода // Надежность. – 2009. – № 1. – С. 72-80.
10. *Лукинова О.В.* Формирование модели угроз безопасности компьютерной сети при бизнес-процессном подходе // Реинжиниринг бизнес-процессов на основе современных информационных технологий: Тр. XII науч.-практ. конф. – М., 2009. – С. 170-176.
11. ГОСТ Р 51897–2011/Руководство ИСО 73:2009. Менеджмент риска. Термины и определения. – М.: Стандартинформ, 2012. – 16 с.
12. ГОСТ Р ИСО/МЭК 13335-1–2006. Информационная технология. Методы и средства обеспечения безопасности. Ч. 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – М.: Стандартинформ, 2007. – 23 с.
13. Азбука киберустойчивости. – 2025. – URL: https://www.kaspersky.ru/blog/cyber-resilience-101/39564/ (дата обращения: 03.11.2025).
14. *Краснов А.Е., Мосолов А.С., Феоктистова Н.А.* Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности // Безопасность информационных технологий. – 2021. – Т. 28, № 1. – С. 106-120. – DOI: 10.26583/bit.2021.1.09.
15. *Солянов Д.А., Тимирянова Д.Р.* Стратегии повышения уровня киберустойчивости в корпоративной инфраструктуре // Международный студенческий научный вестник. – 2025. – № 1. – URL: https://eduherald.ru/ru/article/view?id=21744 (дата обращения: 03.11.2025).
16. NIST SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View / National Institute of Standards and Technology. – Gaithersburg: NIST, 2011. – 82 p. – URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf (дата обращения: 03.11.2025).
17. Российская Федерация. Законы. О персональных данных : Федер. закон № 152-ФЗ: принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 г. – М., 2006. – Доступ из справ.-правовой системы «КонсультантПлюс».
18. Российская Федерация. Законы. О безопасности : Федер. закон № 390-ФЗ: принят Гос. Думой 7 декабря 2010 г. : одобр. Советом Федерации 15 декабря 2010 г. – М., [2010. – Доступ из справ.-правовой системы «КонсультантПлюс».
19. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: Федер. закон № 149-ФЗ: принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 г. – М., 2006. – Доступ из справ.-правовой системы «КонсультантПлюс».
20. ITIL Essentials for IT Service Management: Матер. учебного курса. – Версия В.00. – Hewlett-Packard Education, 1998. – 178 с.
21. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска. – Введ. 2012–12–01. – М.: Стандартинформ, 2012. – 74 с.
22. ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management. – 3rd ed. – Geneva: ISO/IEC, 2018. – 61 p.

23. *Богачева Д.Н., Лукинова О.В.* Вопросы оценки корректности данных устройств нижнего уровня автоматизированных систем // Матер. 32-й Международной научно-технической конференции «Системы безопасности – 2023». – М.: Академия ГПС МЧС России, 2023. – С. 349-355.
24. *Bogacheva D.N., Lukinova O.V., Pavlova E.S.* The Approach to Assessing the Correctness of Automated System Endpoint Devices' Parameters Using their Reference Models // Proceedings of the 2024 International Russian Smart Industry Conference (SmartIndustryCon). – Sochi: IEEE, 2024. – P. 850-854.
25. *Массель А.Г., Гаськова Д.А.* Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов // Онтология проектирования. – 2019. – Т. 9, № 2 (32). – С. 225-238.
26. *Бурый А.С., Усцелемов В.Н.* Онтологический подход к формированию когнитивных моделей оценки кибербезопасности // Информационно-экономические аспекты стандартизации и технического регулирования. – 2020. – № 3 (55). – С. 77-84.
27. Ученые МГУ разработали новую онтологию информационной безопасности. – 2025. – URL: https://cs.msu.ru/news/3933 (дата обращения: 03.11.2025).
28. *Колесникова Д.С., Верещагина Е.А.* Применение онтологий в обучающих системах // Инженерный вестник Дона. – № 6 (102). – С. 247-257.
29. *Гузайров М.Б., Вульфин А.М., Картак В.М., Кириллова А.Д., Миронов К.В.* Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности// Тр. ИСА РАН. – 2019. – Т. 69, № 4. – URL: http://www.isa.ru/proceedings/images/documents/2019-69-4/62-69.pdf (дата обращения: 03.11.2025.)
30. *Яцук К.В., Свиридов О.И., Иванов Д.А., Скоробогатов С.Ю.* Методика моделирования угроз STRIDE на технологию SDN-контроллеров // Известия Тульского государственного университета. Технические науки. – 2022. – № 3. – С. 347-352.
31. *Khan R., McLaughlin K., Laverty D., Sezer S.* STRIDE-based Threat Modeling for Cyber-Physical Systems // Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe. – 2017. – P. 1-6.
32. *Shevchenko N., Chick T.A., O'Riordan P., Scanlon T.P., Woody C.* Threat modelling: A summary of available methods. – Carnegie Mellon University Software Engineering Institute. – 2018. – С. 1-24.
33. *Миняев А.А.* Моделирование угроз безопасности информации в территориально-распределенных информационных системах // Наукоемкие технологии в космических исследованиях Земли. – 2021. – № 13 (2). – С. 52-65.
34. *Зуфарова А.С., Кошелева А.Д.* Что такое MITRE ATT&CK: разбор популярной тактической модели. Информатика. Экономика. Управление // Informatics. Economics. Management. – 2025. – № 4 (1). – С. 2027-2037. – DOI: 10.47813/2782-5280-2025-4-1-2027-2037.
35. *Дойникова Е.В., Чечулин А.А., Котенко И.В.* Оценка защищенности компьютерных сетей на основе метрик CVSS // Информационно-управляющие системы. – 2017. – №. 6 (91). – С. 76-87.
36. *Бойченко А.В., Лукинова О.В.* Когнитивный подход к анализу влияния факторов информационной безопасности // Тр. 7-й Международной научно-практической конференции «Интегрированные модели и мягкие вычисления в искусственном интеллекте». – М.: Физматлит, 2013. – С. 583-586.
37. *Афонцев Э.В., Поршнев С.В.* Опыт построения методик обнаружения вирусной сетевой активности // Вестник УГТУ-УПИ. – 2004. – № 20 (50). – С. 215-217.
38. *Лукинова О.В., Пугачев А.В.* Особенности построения профилей систем безопасности ИС // Открытое образование. – 2015. – № 4. – С. 80-87. – DOI: 10.21686/1818-4243-2015-4(111-38-44).

REFERENCES

1. *Maksimova E.A., Sadovnikova N.P.* Otsenka infrastrukturnoy ustoychivosti sub"yekta kriticheskoy informatsionnoy infrastruktury pri destruktivnykh vozdeystviyakh [Assessment of the infrastructure resilience of a critical information infrastructure subject under destructive impacts], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2021, No. 4, pp. 155-165, DOI: 10.18522/2311-3103-2021-4-155-165.
2. *Ross R., Johnson L.* Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, Special Publication (NIST SP), Gaithersburg MD, National Institute of Standards and Technology, 2010, 399 p.
3. *Voevodin V.A.* Model' otsenki funktsional'noy ustoychivosti elementov informatsionnoy infrastruktury dlya usloviy vozdeystviya mnozhestva komp'yuternykh atak [Model for assessing the functional stability of information infrastructure elements under multiple computer attacks], *Informatika i avtomatizatsiya* [Informatics and Automation], Saint Petersburg, FITs RAN, 2023, Vol. 22, No. 3, pp. 691-715. DOI: 10.15622/ia.22.3.8.

4. *Tarasov A.A.* Funktsional'naya ustoychivost' komp'yuternykh sistem kak faktor obespecheniya ikh informatsionnoy bezopasnosti [Functional stability of computer systems as a factor in ensuring their information security], *Informatsionnaya bezopasnost' Rossii v usloviyakh global'nogo informatsionnogo obshchestva* [Information Security of Russia in the Global Information Society], Moscow, 2002, pp. 193-200.
5. *Borodakiy Yu.V., Lobodinskiy Yu.G.* Informatsionnye tekhnologii. Metody, protsessy, sistemy [Information technologies. Methods, processes, systems], Moscow, Radio i svyaz', 2002, 451 p.
6. *Korolev A.N.* Funktsional'naya ustoychivost' navigatsionno-informatsionnykh sistem [Functional stability of navigation and information systems], *Izvestiya vuzov. Priborostroenie* [Journal of Instrument Engineering], 2018, Vol. 61, No. 7, P. 559–565. DOI: 10.17586/0021-3454-2018-61-7-559-565.
7. *Borodakiy Yu.V., Tarasov A.A.* O funktsional'noy ustoychivosti informatsionno-vychislitel'nykh sistem [On the functional stability of information and computing systems], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2006, No. 7, pp. 5-12.
8. *Lukinova O.V.* Komp'yuternye metody i algoritmy upravleniya bezopasnost'yu informatsionnykh sistem [Computer methods and algorithms for information systems security management], Moscow, IPU RAN [ICS RAS], 2014, 248 p.
9. *Lukinova O.V.* Formalizatsiya zadachi planirovaniya zashchity raspredelennoy komp'yuternoy seti na osnove biznes-protsessnogo podkhoda [Formalization of the task of planning the protection of a distributed computer network based on a business process approach], *Nadezhnost'* [Dependability], 2009, No. 1, pp. 72-80.
10. *Lukinova O.V.* Formirovanie modeli ugroz bezopasnosti komp'yuternoy seti pri biznes-protsessnom podkhode [Formation of a computer network security threat model using a business process approach], *Reinzhiniring biznes-protsessov na osnove sovremennykh informatsionnykh tekhnologiy* [Business Process Reengineering Based on Modern Information Technologies], Moscow, 2009, pp. 170-176.
11. GOST R 51897-2011/ISO Guide 73:2009. Menedzhment riska. Terminy i opredeleniya [Risk management. Vocabulary. Guidelines for use in standards]. Moscow: Standartinform, 2012, 16 p.
12. GOST R ISO/IEC 13335-1-2006. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Chast' 1. Kontseptsiya i modeli menedzhmenta bezopasnosti informatsionnykh i telekommunikatsionnykh tekhnologiy [Information technology. Security techniques. Part 1. Concepts and models for information and telecommunications technology security management], Moscow, Standartinform, 2007, 23 p.
13. Azbuka kiberustoychivosti [Cyber resilience ABCs], *Kaspersky Blog* [Kaspersky Blog], 2025. Available at: https://www.kaspersky.ru/blog/cyber-resilience-101/39564/ (accessed 03 November 2025).
14. *Krasnov A.E., Mosolov A.S., Feoktistova N.A.* Otsenivanie ustoychivosti kriticheskikh informatsionnykh infrastruktur k ugrozam informatsionnoy bezopasnosti [Evaluating the resilience of critical information infrastructures to information security threats], *Bezopasnost' informatsionnykh tekhnologiy* [IT Security], 2021, Vol. 28, No. 1, pp. 106-120. DOI: 10.26583/bit.2021.1.09.
15. *Solyanov D.A., Timiryanova D.R.* Strategii povysheniya urovnya kiberustoychivosti v korporativnoy infrastrukture [Strategies for increasing the level of cyber resilience in corporate infrastructure], *Mezhdunarodnyy studencheskiy nauchnyy vestnik* [International Student Scientific Bulletin], 2025, No. 1. Available at: https://eduherald.ru/ru/article/view?id=21744 (accessed 03 November 2025).
16. NIST SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View, *National Institute of Standards and Technology*, Gaithersburg, NIST, 2011, 82 p. Available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf (accessed 03 November 2025).
17. Russian Federation. Laws. O personal'nykh dannykh: Feder. zakon No. 152-FZ [On Personal Data: Federal Law No. 152-FZ]. Moscow, 2006, ConsultantPlus.
18. Russian Federation. Laws. O bezopasnosti: Feder. zakon No. 390-FZ [On Security: Federal Law No. 390-FZ]. Moscow, 2010, ConsultantPlus.
19. Russian Federation. Laws. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: Feder. zakon No. 149-FZ [On Information, Information Technologies and Information Protection: Federal Law No. 149-FZ]. Moscow, 2006, ConsultantPlus.
20. ITIL Essentials for IT Service Management: materialy uchebnogo kursa. Versiya B.00 [ITIL Essentials for IT Service Management: Course Materials. Version B.00], *Hewlett-Packard Education*, 1998, 178 p.
21. GOST R ISO/IEC 31010-2011. Menedzhment riska. Metody otsenki riska [Risk management. Risk assessment techniques]. Moscow, Standartinform, 2012, 74 p.
22. ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management, 3rd ed., Geneva, ISO/IEC, 2018, 61 p.
23. *Bogacheva D.N., Lukinova O.V.* Voprosy otsenki korrektnosti dannykh ustroystv nizhnego urovnya avtomatizirovannykh sistem [Issues of assessing the correctness of data from low-level devices of automated systems], *Materialy 32-y Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii "Sistemy bezopasnosti – 2023"* [Proceedings of the 32nd International Scientific and Technical Conference "Security Systems – 2023"]. Moscow, Akademiya GPS MCHS Rossii, 2023, pp. 349-355.

24. *Bogacheva D.N., Lukinova O.V., Pavlova E.S.* The Approach to Assessing the Correctness of Automated System Endpoint Devices' Parameters Using their Reference Models, *Proceedings of the 2024 International Russian Smart Industry Conference (SmartIndustryCon)*, Sochi, IEEE, 2024, pp. 850-854.
25. *Massel' A.G., Gaskova D.A.* Ontologicheskiy inzhiniring dlya razrabotki intellektual'noy sistemy analiza ugroz i otsenki riskov kiberbezopasnosti energeticheskikh ob"yektov [Ontological engineering for the development of an intelligent system for threat analysis and cybersecurity risk assessment of energy facilities], *Ontologiya proektirovaniya* [Ontology of Designing], 2019, Vol. 9, No. 2 (32), pp. 225-238.
26. *Buryy A.S., Ustselemov V.N.* Ontologicheskiy podkhod k formirovaniyu kognitivnykh modeley otsenki kiberbezopasnosti [Ontological approach to the formation of cognitive models for cybersecurity assessment], *Informatsionno-ekonomicheskie aspekty standartizatsii i tekhnicheskogo regulirovaniya* [Information and Economic Aspects of Standardization and Technical Regulation], 2020, No. 3 (55), pp. 77-84.
27. Uchenye MGU razrabotali novuyu ontologiyu informatsionnoy bezopasnosti [MSU scientists have developed a new information security ontology], *VMK MSU* [VMK MSU website], 2025. Available at: https://cs.msu.ru/news/3933 (accessed 03 November 2025).
28. *Kolesnikova D.S., Vereshchagina E.A.* Primenenie ontologiy v obuchayushchikh sistemakh [Application of ontologies in educational systems], *Inzhenernyy vestnik Dona* [Engineering Journal of Don], 2025, No. 6 (102), pp. 247-257.
29. *Guzairov M.B., Vul'fin A.M., Kartak V.M., Kirillova A.D., Mironov K.V.* Sravnitel'nyy analiz algoritmov kognitivnogo modelirovaniya pri otsenke riskov informatsionnoy bezopasnosti [Comparative analysis of cognitive modeling algorithms in information security risk assessment], *Trudy ISA RAN* [Proceedings of ISA RAS], 2019, Vol. 69, No. 4. Available at: http://www.isa.ru/proceedings/images/documents/2019-69-4/62-69.pdf (accessed 03 November 2025).
30. *Yatsuk K.V., Sviridov O.I., Ivanov D.A., Skorobogatov S.Yu.* Metodika modelirovaniya ugroz STRIDE na tekhnologiyu SDN-kontrollerov [STRIDE threat modeling methodology for SDN controller technology], *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki* [News of the Tula State University. Technical Sciences], 2022, No. 3, pp. 347-352.
31. *Khan R., McLaughlin K., Laverty D., Sezer S.* STRIDE-based Threat Modeling for Cyber-Physical Systems, *Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe*, 2017, pp. 1-6.
32. *Shevchenko N., Chick T.A., O'Riordan P., Scanlon T.P., Woody C.* Threat modelling: A summary of available methods, *Carnegie Mellon University Software Engineering Institute*, 2018, pp. 1-24.
33. *Minyaev A.A.* Modelirovanie ugroz bezopasnosti informatsii v territorial'no-raspredelennykh informatsionnykh sistemakh [Information security threat modeling in geographically distributed information systems], *Naukoyemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli* [Hign-tech Technologies in Earth Space Research], 2021, No. 13 (2), pp. 52-65.
34. *Zufarova A.S., Kosheleva A.D.* Chto takoe MITRE ATT&CK: razbor populyarnoy takticheskoy modeli [What is MITRE ATT&CK: Analysis of a Popular Tactical Model], *Informatika. Ekonomika. Upravlenie* [Informatics. Economics. Management], 2025, No. 4 (1), pp. 2027-2037. DOI: 10.47813/2782-5280-2025-4-1-2027-2037.
35. *Doynikova E.V., Chechulin A.A., Kotenko I.V.* Otsenka zashchishchennosti komp'yuternykh setey na osnove metrik CVSS [Security assessment of computer networks based on CVSS metrics], *Informatsionno-upravlyayushchie sistemy* [Information Management Systems], 2017, No. 6 (91), pp. 76-87.
36. *Boychenko A.V., Lukinova O.V.* Kognitivnyy podkhod k analizu vliyaniya faktorov informatsionnoy bezopasnosti [Cognitive approach to the analysis of the influence of information security factors], *Trudy 7-y Mezhdunarodnoy nauchno-prakticheskoy konferentsii "Integrirovannye modeli i myagkie vychisleniya v iskusstvennom intellekte"* [Proceedings of the 7th International Scientific and Practical Conference "Integrated Models and Soft Computing in Artificial Intelligence"], Moscow, Fizmatlit, 2013, pp. 583-586.
37. *Afontsev E.V., Porshnev S.V.* Opyt postroeniya metodik obnaruzheniya virusnoy setevoy aktivnosti [Experience in building methods for detecting viral network activity], *Vestnik UGTU-UPI* [Bulletin of USTU-UPI], 2004, No. 20 (50), pp. 215-217.
38. *Lukinova O.V., Pugachev A.V.* Osobennosti postroeniya profiley sistem bezopasnosti IS [Features of constructing security system profiles for information systems], *Otkrytoe obrazovanie* [Open Education], 2015, No. 4, P. 80-87. DOI: 10.21686/1818-4243-2015-4(111-38-44).

**Богачева Дарья Николаевна** – Институт проблем управления им. В.А. Трапезникова РАН; e-mail: bogacheva@ipu.ru; г. Москва, Россия; тел.: 84953348910; лаборатория Инфраструктурных систем; м.н.с.

**Лукинова Ольга Васильевна** – Институт проблем управления им. В.А. Трапезникова РАН; e-mail: lukinova@ipu.ru; г. Москва, Россия, тел.: 84953348910; лаборатория Инфраструктурных систем; д.т.н.; доцент; в.н.с.

**Саломатин Александр Александрович** – Институт проблем управления им. В.А. Трапезникова РАН; e-mail: sandr@ipu.ru; г. Москва, Россия, тел.: 84953348910; лаборатория Киберфизических систем; к.т.н.; с.н.с.

**Bogacheva Darya Nikolaevna** – V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences; e-mail: bogacheva@ipu.ru; Moscow, Russia; phone: +74953348910; Infrastructure Systems Laboratory; junior researcher.

**Lukinova Olga Vasilievna** – V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences; e-mail: lukinova@ipu.ru; Moscow, Russia; phone: +74953348910; Infrastructure Systems Laboratory; dr. of eng. sc.; associate professor; leading researcher.

**Salomatin Aleksandr Aleksandrovich** – V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences; e-mail: sandr@ipu.ru; Moscow, Russia; phone: +74953348910; Cyber-Physical Systems Laboratory; cand. of eng. sc.; senior researcher.

УДК 004.056.53:004.75 DOI 10.18522/2311-3103-2026-1-179-191

**Д.О. Ларин, Р.И. Захарченко, С.А. Диченко**

## МАНДАТНАЯ АТРИБУТИВНО-РОЛЕВАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ В КРУПНОМАСШТАБНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

*В условиях стремительного развития информационных систем федерального масштаба, их эволюции в цифровые экосистемы, к процессу обеспечения безопасности обрабатываемой в них информации предъявляются новые требования. Такими требованиями, в частности, являются повышение доступности информации при управлении доступом пользователей с сохранением требуемого уровня ее конфиденциальности, принятие решения о доступе к ресурсам на основе множества факторов. Для их удовлетворения ранее было предложено множество композиционных моделей управления доступом на основе ролей и атрибутов, которые решили ряд актуальных проблем, сохранив удобство администрирования и обеспечив при этом гибкость и масштабируемость без «взрыва ролей». Однако известные модели все еще имеют существенный недостаток – невозможность их использования в информационных системах, где обрабатывается информация высокого уровня значимости. Целью исследования является разработка в рамках методологии субъект-сущностного подхода теории информационной безопасности новой мандатной атрибутивно-ролевой модели управления доступом, а также ее формальное описание с помощью математического аппарата теории автоматов. Использование модели позволит предотвращать запрещенные информационные потоки от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности динамически, в процессе ограничения набора разрешений, назначенных роли, с помощью реализации мандатного разграничения доступа через отдельную атрибутивную политику, сохраняя при этом возможность предоставления пользователям доступа высокой степени детализации на основе атрибутов контекста. Применение модели может быть востребовано в крупномасштабных информационных системах, где одновременно обрабатывается информация различных уровней конфиденциальности и, ввиду особенностей функционирования, необходима реализация атрибутивного управления доступом.*

*Атрибутивное управление доступом; ролевое управление доступом, мандатное управление доступом; модель управления доступом; MAP модель; конфиденциальность; доступность.*

**D.O. Larin, R.I. Zaharchenko, S.A. Dichenko**

## MANDATORY ROLE-CENTRIC ATTRIBUTE-BASED ACCESS CONTROL MODEL FOR LARGE-SCALE INFORMATION SYSTEMS

*In the context of the rapid development of national-scale information systems and their evolution into digital ecosystems, new requirements are imposed on the process of ensuring the security of the information processed within them. These requirements include enhancing information availability in user access management while maintaining the required level of confidentiality, and making access decisions to resources based on multiple factors. To meet these requirements, numerous compositional access control models based on roles and attributes have been proposed previously, which have resolved several pressing issues while maintaining administrative convenience and providing flexibility and scalability*