МИРЭА - Российский технологический университет

МЕТОДОЛОГИЯ АНАЛИЗА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТАМ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ДВОЙНИКОВ

Научная специальность:

2.3.6. Методы и системы защиты информации, информационная безопасность

Соискатель: д.э.н., профессор,

Заведующий кафедрой КБ-9 РТУ МИРЭА

Митяков Евгений Сергеевич

Санкт-Петербург – 2025

Актуальность темы исследования

- В условиях цифровизации критическая информационная инфраструктура (КИИ) приобретает стратегическое значение из-за рисков киберинцидентов с серьёзными последствиями
- Современные информационные угрозы становятся более сложными и целенаправленными, что требует новых подходов к их анализу
- Существующие методы анализа угроз ограничены документарностью, неполным учетом специфики объектов КИИ
- Концепция цифровых двойников (ЦД) представляет перспективный инструмент для анализа и моделирования угроз объектам КИИ
- Для повышения эффективности защиты необходимо разработать научно обоснованную, воспроизводимую и адаптируемую методологию анализа угроз с использованием ЦД.

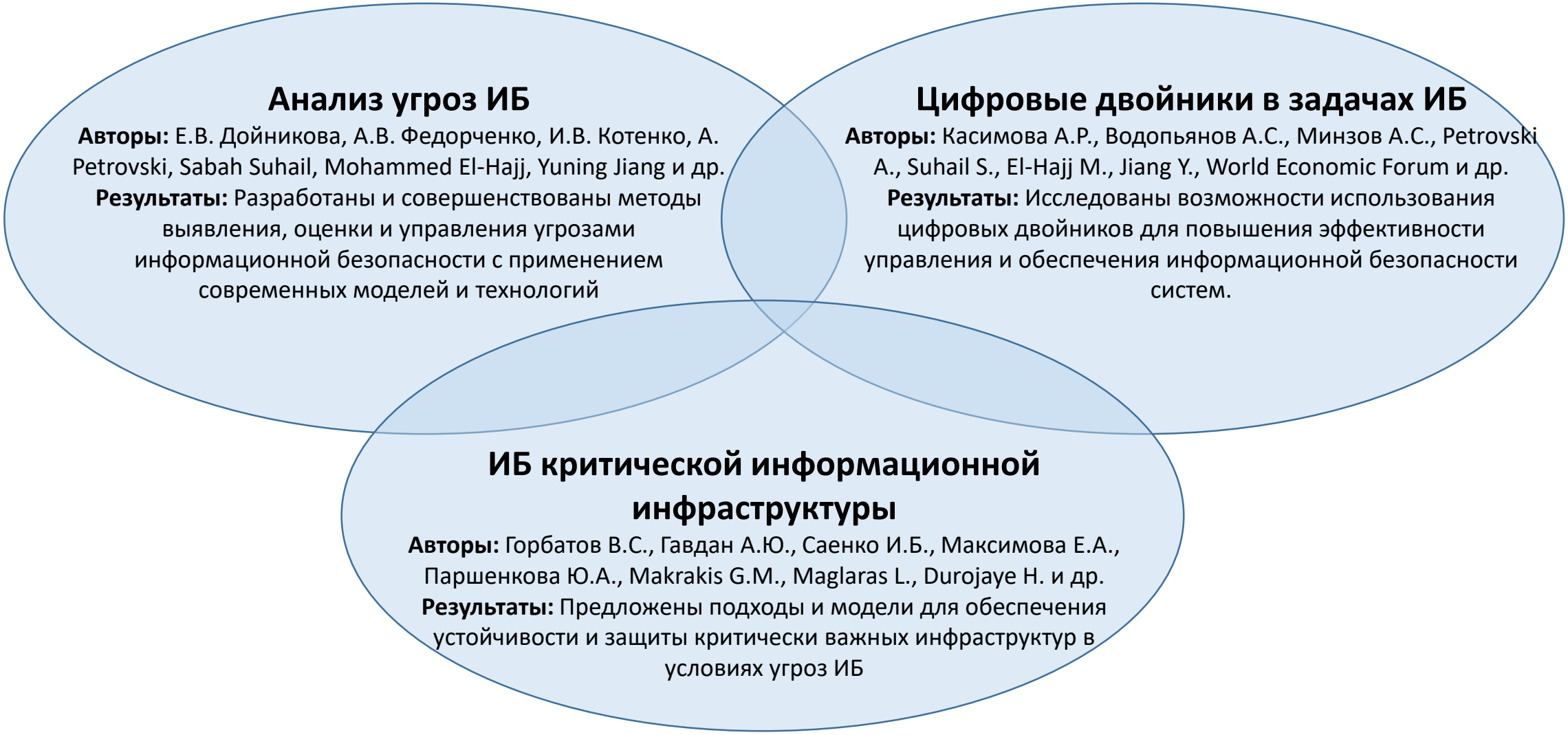
Классификация проблем использования ЦД в ИБ объектов КИИ

Категория проблем	Де-факто	Де-юре
Технические	Ограниченная точность моделирования и высокая ресурсоемкость, задержки синхронизации данных, уязвимости компонентов ЦД, несогласованность временных меток, ошибки в прогнозах, ложные тревоги, неэффективные реакции	Недостаточная защита ЦД как критической системы, отсутствие стандартов эксплуатации, риски внедрения вредоносных компонентов
Организационные	Недостаточная квалификация специалистов, потеря доверия к технологии после инцидентов	Проблемы интеграции с существующими средствами ИБ, отсутствие правового статуса данных, полученных из ЦД

Анализ состояния исследований

Цифровой двойник изделия — это система, состоящая из цифровой модели изделия и двусторонних информационных связей с изделием (при наличии изделия) и (или) его составными частями. (ГОСТ Р 57700.37–2021)

Цифровой двойник объекта критической информационной инфраструктуры — это система, состоящая из цифровой модели объекта КИИ и двусторонних информационных связей с этим объектом и (или) его компонентами.



Научная проблема

Разработка моделей, методов и методик анализа угроз ИБ объектов КИИ с применением ЦД

Цель и задачи исследования

Цель исследования: повышение эффективности анализа угроз ИБ объектам КИИ за счет разработки методологии, основанной на применении цифровых двойников.

Задачи исследования:

- Разработать многоаспектную модель декомпозиции КИИ как объекта цифрового моделирования, обеспечивающую структурированное представление компонентов, их взаимодействий и форм проявления угроз ИБ.
- Построить комплекс моделей, реализующих концепцию ЦД объекта КИИ с возможностью двунаправленной синхронизации с физическим прототипом для анализа угроз ИБ.
- Сформировать расширенную модель угроз ИБ, интегрирующую ЦД для анализа актуальных и потенциальных угроз.
- Разработать метод и алгоритмы обнаружения угроз ИБ на основе ЦД.
- Создать комплекс методик оценки угроз ИБ объектам КИИ на основе ЦД.

Объект и предмет диссертационного исследования

Объект исследования: объекты КИИ, подверженные угрозам ИБ.

Предмет исследования: процесс выявления, моделирования и оценки угроз ИБ объектов КИИ с применением ЦД

Положения, выносимые на защиту (основные научные результаты, ОНР)

1. Многоаспектная модель декомпозиции КИИ как объекта цифрового моделирования, обеспечивающую структурированное представление компонентов, их взаимодействий и форм проявления угроз ИБ
2. Комплекс моделей ЦД объекта КИИ с возможностью двунаправленной синхронизации для анализа угроз ИБ
3. Расширенная модель угроз ИБ объектам КИИ для анализа актуальных и потенциальных угроз
4. Метод и алгоритмы обнаружения угроз ИБ на основе ЦД объекта КИИ
5. Комплекс методик оценки угроз ИБ объектам КИИ на основе ЦД

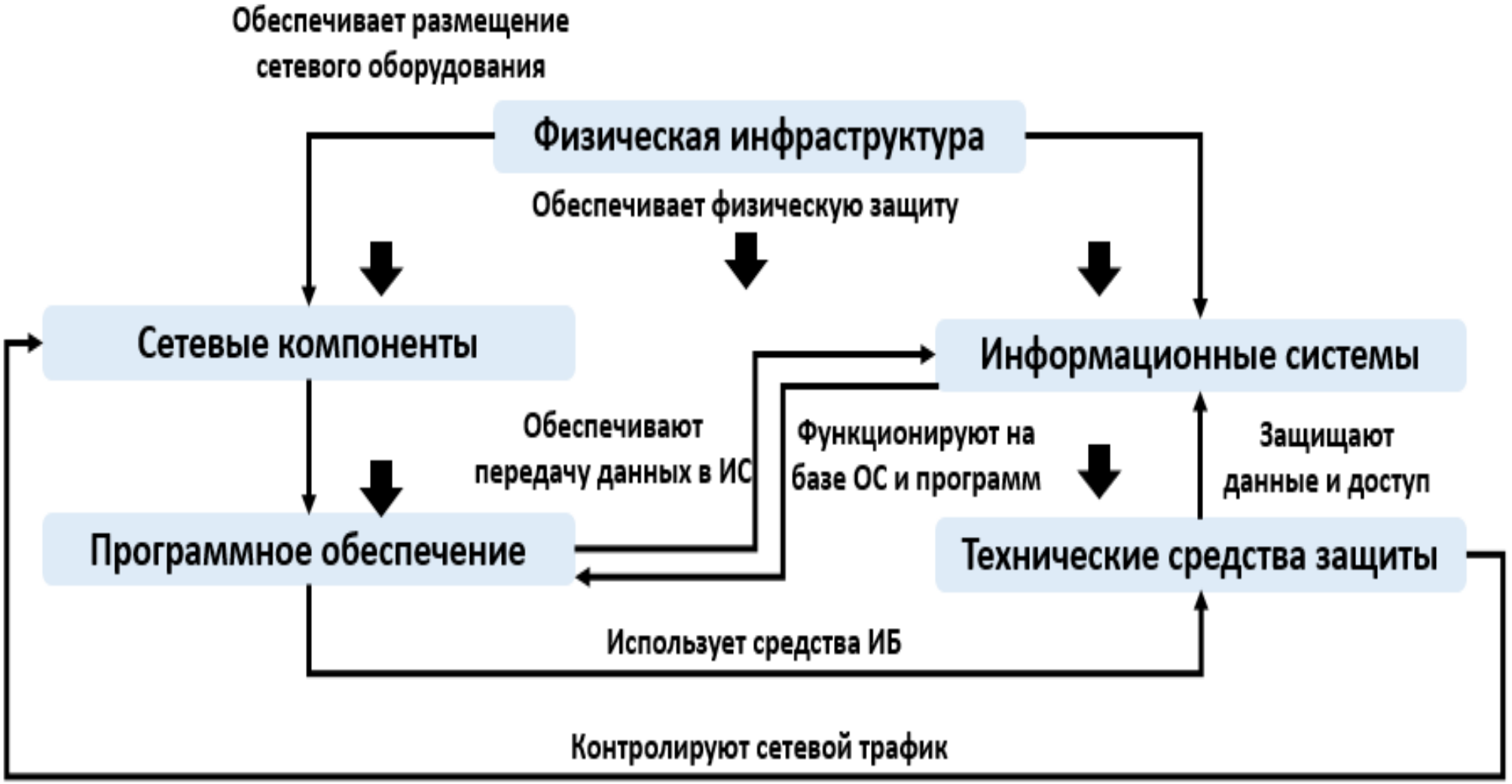
1. Многоаспектная модель декомпозиции КИИ как объекта цифрового моделирования

Диагональная матрица взаимосвязей классификационных признаков компонентов КИИ

Объект влияния / Источник влияния	Технический признак	Процессный признак	Организационный признак	Функциональный признак	Отраслевой признак
Технический признак	—	Технические средства формируют базу для реализации процессов обеспечения ИБ; устойчивость процессов зависит от надёжности инфраструктуры	Организационные решения и регламенты определяют архитектуру, состав и конфигурацию технических средств	Техническая реализация определяет доступность и непрерывность выполнения функций КИИ	Специфика отрасли обусловливает выбор типовых технических решений и допустимые уровни риска
Процессный признак	Реализация процессов обеспечивается функционированием технической инфраструктуры	—	Эффективность процессов определяется уровнем организационной зрелости и наличием структур управления ИБ	Защищённость и устойчивость бизнес-функций обеспечивается реализацией процессов мониторинга, резервирования, восстановления и реагирования	Отраслевые нормативные акты определяют обязательные процессы обеспечения ИБ в специфичных сферах деятельности
Организационный признак	Стратегии управления и организационные регламенты напрямую влияют на эксплуатацию и модернизацию технической базы	Организационная структура обеспечивает управление жизненным циклом процессов и контроль их выполнения	—	Организационная поддержка (наличие службы ИБ, финансирование) критична для реализации функций безопасности	Требования отраслевых регуляторов формируют специфические организационные меры и распределение полномочий
Функциональный признак	Отказ технических компонентов может приводить к недоступности функций КИИ; функции определяют приоритетность технических ресурсов	Функции обеспечиваются соответствующими процессами, реализуемыми на уровне ИБ-сервисов	Выполнение функций возможно при наличии организационной поддержки и ресурсного обеспечения	—	Критичность функций напрямую зависит от отраслевого контекста и уровня допустимого риска
Отраслевой признак	В каждой отрасли применяются уникальные технические решения, стандарты и протоколы	Регламентация процессов безопасности осуществляется отраслевыми органами и регуляторами	Организационная структура подчиняется отраслевым требованиям и стандартам	Отрасль определяет функциональные приоритеты, от которых зависит устойчивость КИИ	—

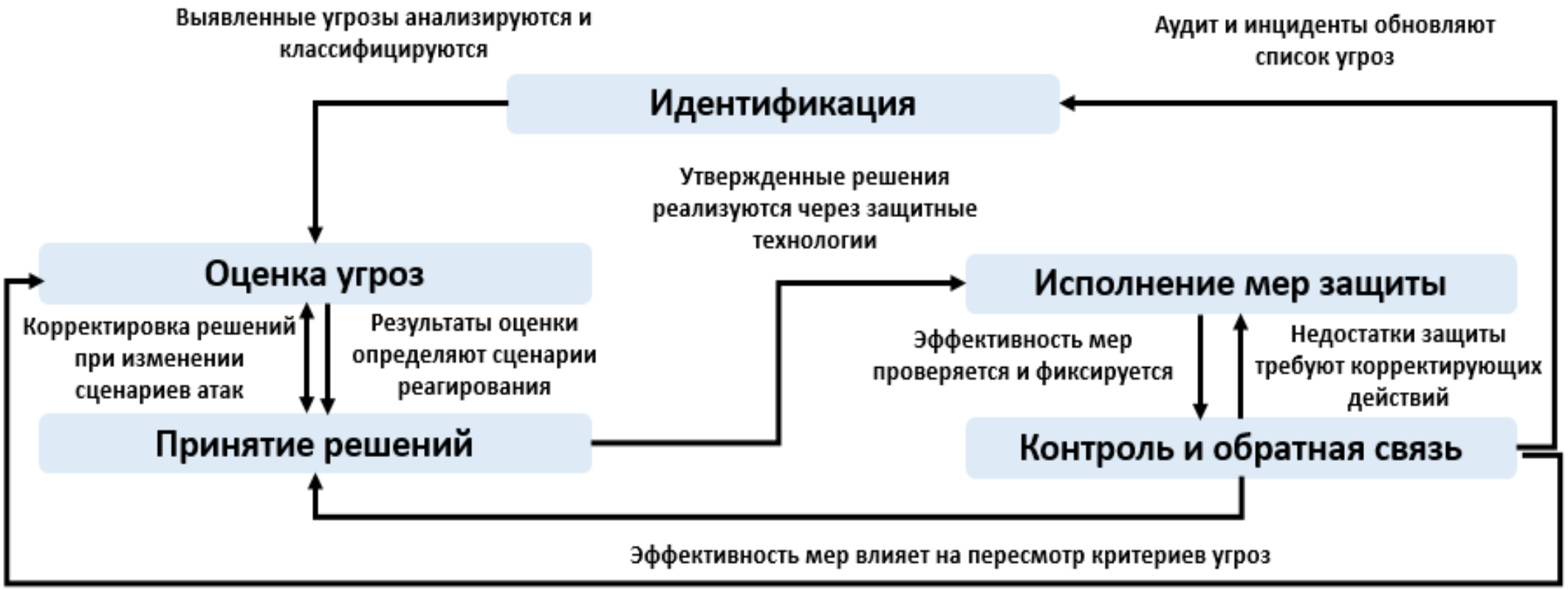
1. Многоаспектная модель декомпозиции КИИ как объекта цифрового моделирования

Взаимодействие в контексте технического признака



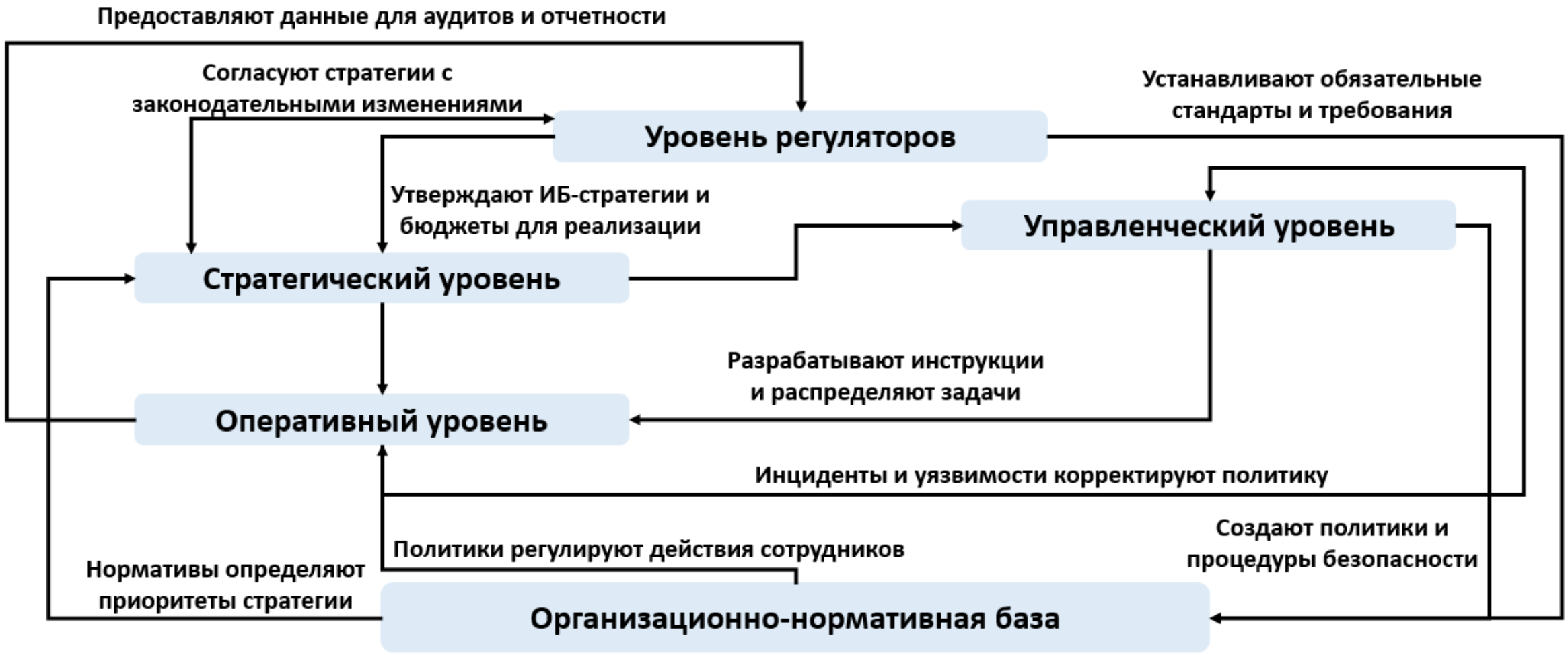
1. Многоаспектная модель декомпозиции КИИ как объекта цифрового моделирования

Взаимодействие в контексте процессного признака



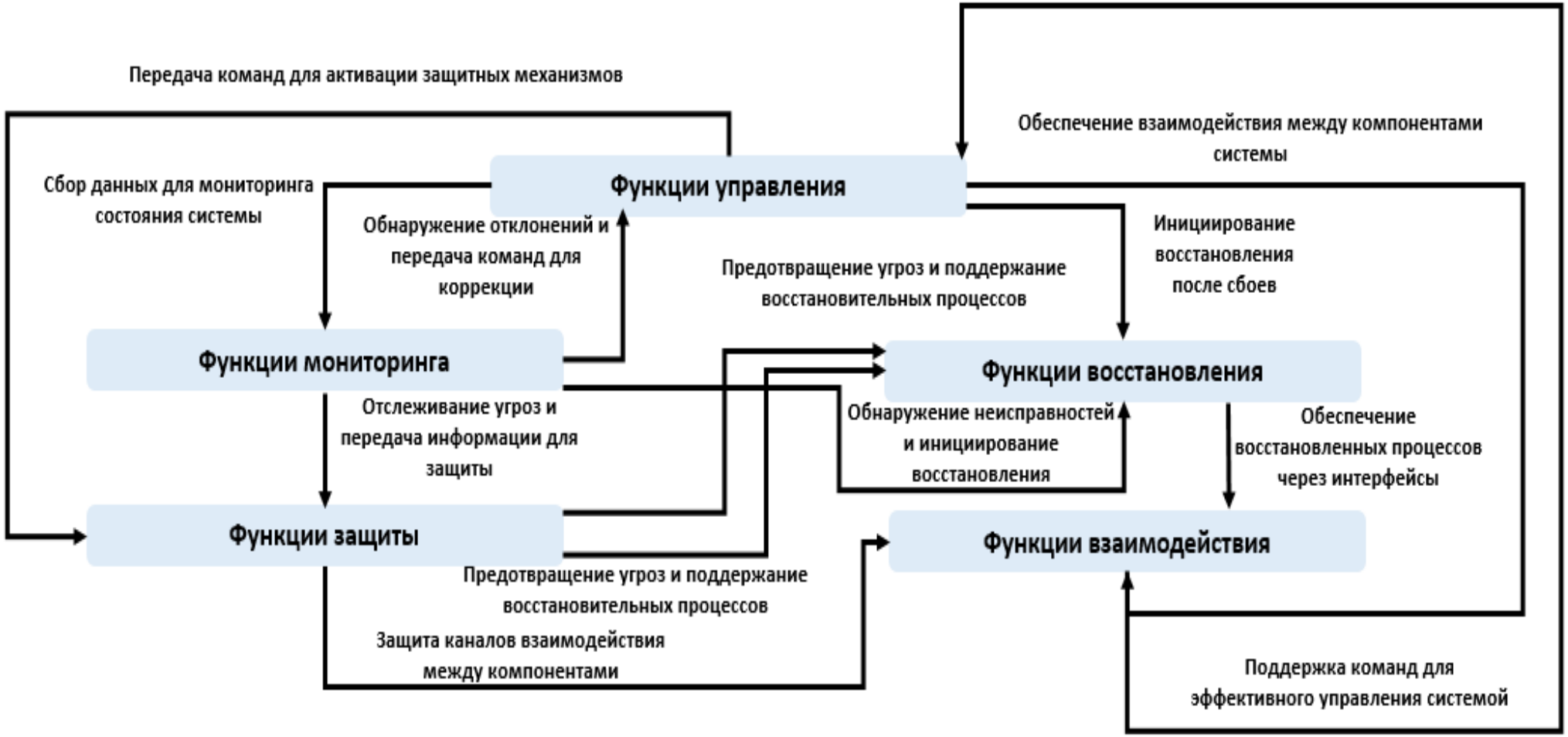
1. Многоаспектная модель декомпозиции КИИ как объекта цифрового моделирования

Взаимодействие в контексте организационного признака



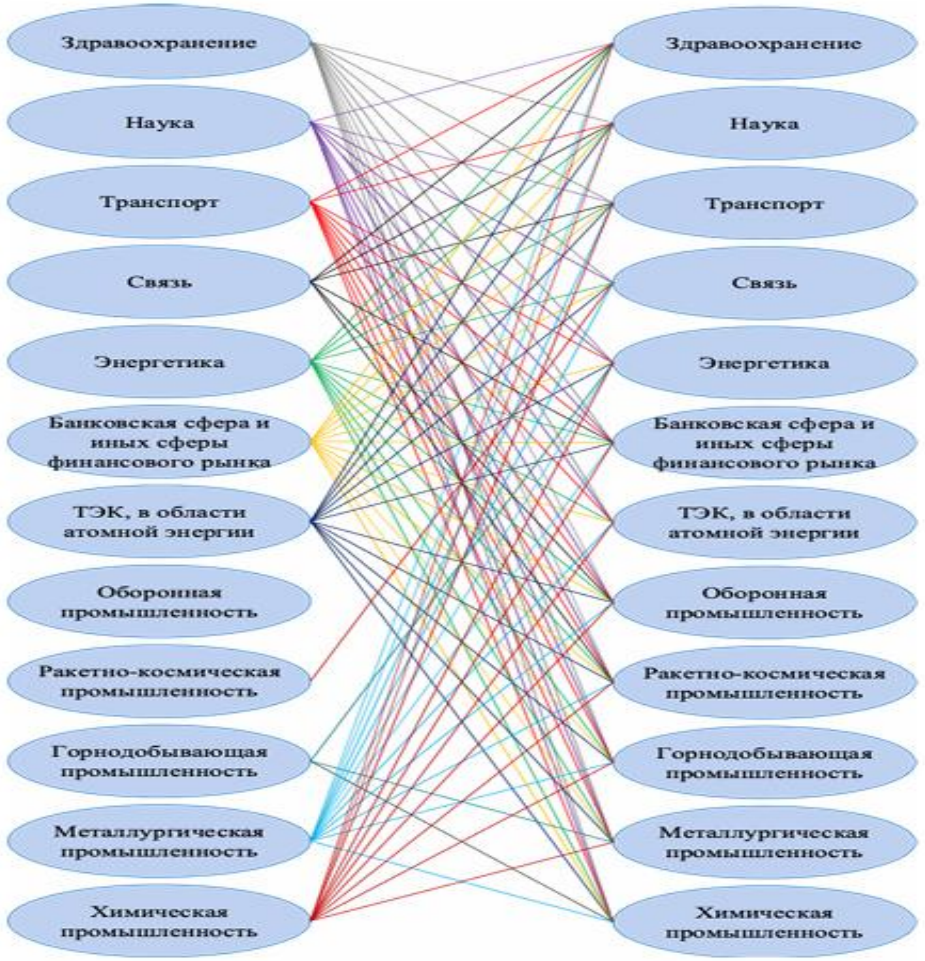
1. Многоаспектная модель декомпозиции КИИ как объекта цифрового моделирования

Взаимодействие в контексте функционального признака



1. Многоаспектная модель декомпозиции КИИ как объекта цифрового моделирования

Взаимодействие в контексте отраслевого признака*



Сфера Сфера	*Z*	*N*	*T*	*S*	*E*	*B*	*Top*	*Ob_Pr*	*Rak_Pr*	*Gor_Pr*	*M_Pr*	*Him_Pr*
Z	1	0	0	0	0	0	0.5	0.5	0.5	0.5	0.5	0.5
N	0.5	1	0	0	0.5	0	0.5	0.5	0.5	0.5	0.5	0.5
T	0	0	1	0.5	0.5	0.5	1	0	0	0.5	0.5	0.5
S	1	1	1	1	1	1	1	1	1	1	1	1
E	1	1	1	1	1	1	1	1	1	1	1	1
B	0.5	0	0.5	1	1	0	0.5	0	0	0	0	0
Top	0.5	0	1	0	1	0	0	1	1	1	1	1
Ob_Pr	0	0	0	0	0	0	0	0	0.5	0	0	0
Rak_Pr	0	0	0	0	0	0	0	0.5	0	0	0	0
Gor_Pr	0	0	0	0	0.5	0	1	0.5	0.5	0.5	1	0.5
M_Pr	0	0	0	0	0	0	1	0.5	0.5	0	0	0
Him_Pr	1	0	0	0	0	0	0.5	0.5	0.5	0	0	1

Z –здравоохранение, N – сфера науки, T – сфера транспорта, S – сфера связи, E – сфера энергетики, B – банковская сфера и иные сферы финансового рынка, Top – топливно-энергетический комплекс, в области атомной энергии, Ob_Pr – сфера оборонной промышленности, Rak_Pr – сфера ракетно-космической промышленности, Gor_Pr – сфера горнодобывающей промышленности, M_Pr – сфера металлургической промышленности, Him_Pr – сфера химической промышленности.

* Составлено по материалам докторской диссертации: Максимова, Е.А. Модели и методы оценки информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях инфраструктурного генеза : диссертация ... доктора технических наук : 2.3.6. / Максимова Елена Александровна; [Место защиты: ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»]. - Санкт-Петербург, 2022. - 448 с.

1. Многоаспектная модель декомпозиции КИИ как объекта цифрового моделирования

Формализация модели декомпозиции

$C = \{c_1, c_2, \dots, c_n\}$ (11.1) – пространство декомпозиции

$\vec{p}(c_i) = \left(p_i^{(T)}, p_i^{(P)}, p_i^{(O)}, p_i^{(F)}, p_i^{(I)}\right)$ (11.2) – вектор признаков

- $p_i^{(T)} \in \mathbf{T}$ — технический признак (отражает уровень материально-технической архитектуры),
- $p_i^{(P)} \in \mathbf{P}$ — процессный признак (жизненный цикл обеспечения ИБ),
- $p_i^{(O)} \in \mathbf{O}$ — организационный признак (уровень управления и ответственности),
- $p_i^{(F)} \in \mathbf{F}$ — функциональный признак (роль в обеспечении устойчивости),
- $p_i^{(I)} \in \mathbf{I}$ — отраслевой признак (сфера деятельности субъекта КИИ).

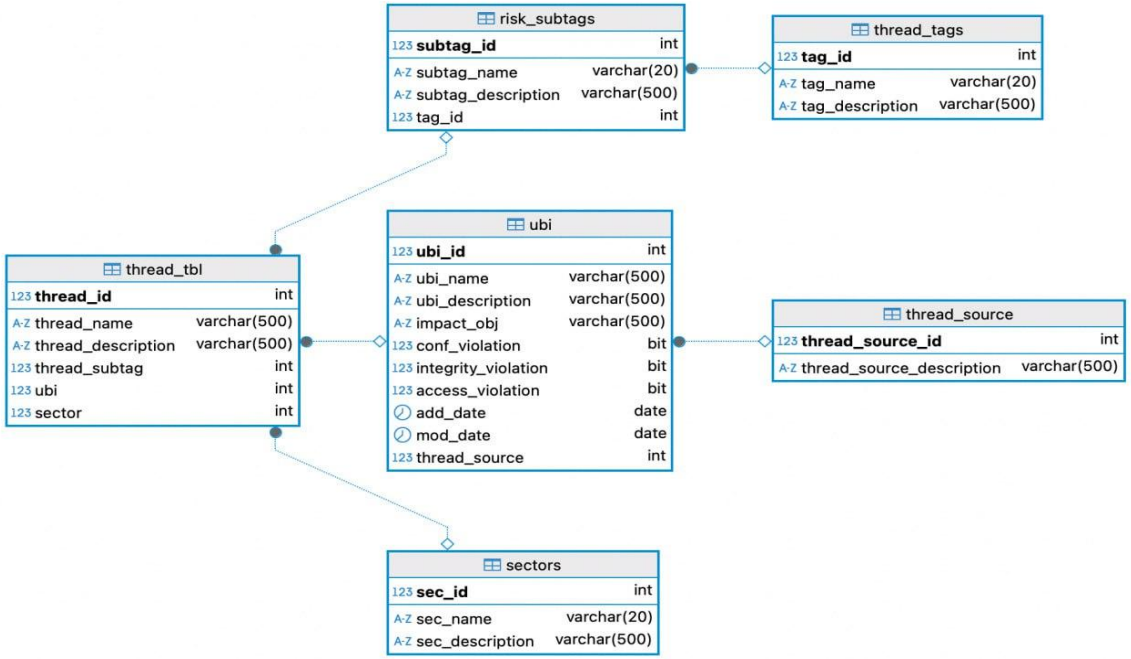
$M_i = (M_{i,\mathbf{T}}, M_{i,\mathbf{P}}, M_{i,\mathbf{O}}, M_{i,\mathrm{F}}, M_{i,\mathrm{I}})$ (10.3) – матрица взаимосвязей

$T_i = f(M_i, \vec{p}(c_i))$ (10.4) – формализация угрозы

$$T = \sum_{i=1}^{n} \alpha_i \cdot U_i$$ (10.5) – общая угроза системе

$$\min_{\text{защитные меры}} T = \min_{\text{защитные меры}} \alpha_i \cdot f(M_i, \vec{p}(c_i))$$ (11.6)

Модель описания угроз ИБ объектам КИИ

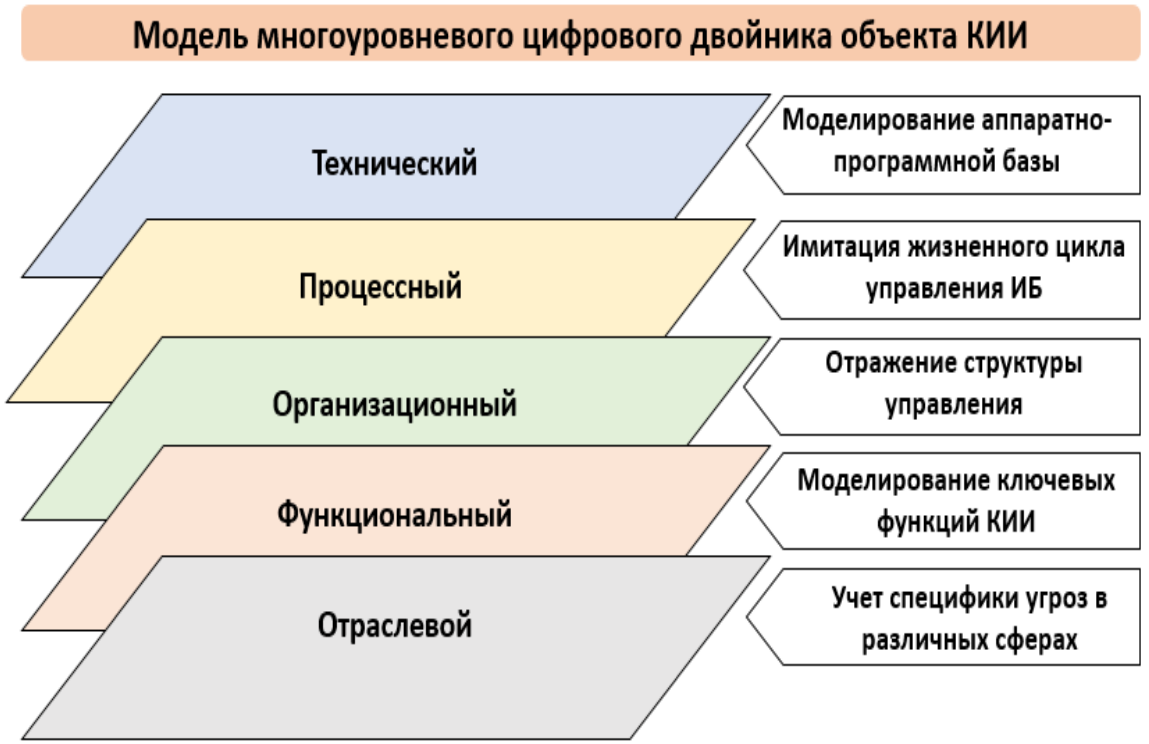


Название таблицы	Назначение
threat_tbl	Основная таблица, содержащая описания комплексных угроз информационной безопасности КИИ.
ubi	Справочник по угрозам безопасности информации, соответствующим классификатору ФСТЭК (УБИ).
threat_source	Справочник источников возникновения угроз
sectors	Справочник сфер функционирования субъектов КИИ
threat_tags	Справочник категорий (признаков) угроз
threat_subtags	Справочник подпризнаков угроз

1. Многоаспектная модель декомпозиции КИИ как объекта цифрового моделирования

Архитектура цифрового двойника объекта КИИ

Компонент ЦД	Описание	Интеграция с аспектами КИИ
Данные	Реальные операционные данные, исторические инциденты, нормативные документы.	Технический слой (логи сетевого оборудования), организационный слой (регламенты).
Аналитика	Алгоритмы ML, симуляторы каскадных отказов, модели угроз.	Процессный слой (прогнозирование времени реакции), функциональный слой (оценка устойчивости).
Визуализация	Интерактивные дашборды, графы взаимосвязей.	Все слои (отображение матрицы взаимозависимостей в реальном времени).
Интеграция	API для подключения к SIEM, SCADA, системам мониторинга.	Технический и отраслевой слои (синхронизация с объектами КИИ).



1. Многоаспектная модель декомпозиции КИИ как объекта цифрового моделирования

Суть: Предложена модель, структурирующая компоненты КИИ по пяти признакам: техническому, процессному, организационному, функциональному и отраслевому. Выполнена их декомпозиция, формализованная через вектор признаков и матрицу взаимосвязей. На основе модели предложена архитектура цифрового двойника КИИ.

Научная новизна:

1. **Впервые** предложена классификация компонентов КИИ по пяти взаимосвязанным признакам с их иерархической декомпозицией и формализацией в виде вектора признаков и матрицы межпризнаковых связей.
2. **Впервые** разработана многоаспектная модель цифрового двойника КИИ, в которой каждому признаку соответствует отдельный слой. Это позволило учитывать каскадные эффекты и межотраслевые зависимости при анализе угроз информационной безопасности.

Теоретическая значимость: расширена методология анализа угроз информационной безопасности КИИ за счет введения многомерной структуры декомпозиции и формализованного представления взаимосвязей между признаками, что обеспечивает основу для математического моделирования угроз и устойчивости.

Практическая значимость: полученные результаты применимы при построении специализированных баз данных угроз ИБ, разработке имитационных моделей оценки угроз ИБ, проектировании адаптивных систем защиты и регламентов управления ИБ субъектов КИИ.

Соответствие паспорту специальности:

П. 3. *Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.*

П. 7. *Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.*

По данному результату опубликовано 4 работы, а также получено 1 свидетельство о регистрации БД.

2. Комплекс моделей ЦД объекта КИИ

Онтологическая модель ЦД объекта КИИ

Классы онтологической модели

Класс	Атрибуты	Описание
Цифровой двойник	Идентификатор объекта КИИ, тип модели, источники данных, уровни декомпозиции	Многослойная модель, имитирующая поведение объекта КИИ на разных уровнях
Объект КИИ	Категория объекта КИИ (ИС, ИТС, АСУ), уровень критичности (высокий, средний, низкий)	Реальный объект КИИ, декомпозированный на технический, процессный и др. уровни
Уровень декомпозиции	Тип уровня, матрица взаимосвязей между уровнями декомпозиции	Слой модели, отражающий специфику аспектов КИИ
Угроза	Наименование, описание, источник, объект воздействия, последствия, целевой уровень атаки, сценарий реализации угрозы	Угроза, направленная на конкретный уровень (например, DDoS на технический уровень)
Уязвимость	Наименование уязвимости, описание уязвимости, уровень опасности уязвимости, уровень декомпозиции	Слабость, привязанная к определенному уровню декомпозиции
Злоумышленник	Тип злоумышленника, методы атаки, целевые уровни декомпозиции	Атакующий, эксплуатирующий уязвимости на выбранных уровнях.
Контрмера	Тип контрмеры, уровень применения контрмеры, соответствие требованиям законодательства	Мера защиты, применяемая к конкретному уровню
Нормативный документ	Название, требования к защите по уровням декомпозиции	Документы, регламентирующие защиту
Риск	Уровень, вероятность реализации угрозы, целевой уровень декомпозиции	Оценка риска для конкретного уровня декомпозиции.

Схема онтологической модели

2. Комплекс моделей ЦД объекта КИИ

Концептуальная модель двустороннего взаимодействия ЦД в системе ИБ

Схема концептуальной модели

Формализация модели

$$\begin{cases} D(t) = \Phi(S(t)) + \epsilon(t) \\ P(T_i|D(t)) = f_{\text{ML}}(D(t), H) \\ A(t) = \Gamma(D(t), T) \\ \Delta(t) = \Psi(D(t), M(t)) \\ R(t) = \Lambda(\Delta(t)) \\ M(t) = \Theta(D(t)) \\ \text{Input}_B(t) = A(t) \\ D(t+1) = D(t) + \Sigma(t) \end{cases} \quad (15.1)$$

$D(t)$ — Состояние цифрового двойника в момент времени t

$S(t)$ — Состояние физической системы в момент времени t

Φ — Синхронизатор данных между физической системой и ЦД

$\epsilon(t)$ — Погрешность синхронизации данных

$P(T_i|D(t))$ — Апостериорная вероятность угрозы T_i, вычисленная на основе данных ЦД

f_{ML} — Функция машинного обучения для прогнозирования угроз

$A(t)$ — Вектор атак в момент времени t, представляющий сценарии угроз

Γ — Оператор симуляции атак

$\Delta(t)$ — Вектор аномалий в поведении ЦД

Ψ — Функция для выявления аномалий

$M(t)$ — Мета-состояние модели (целостность, достоверность и корректность)

$R(t)$ — Реакция системы на аномалии

Λ — Функция принятия решения о защитных мерах

Θ — Процедура верификации модели

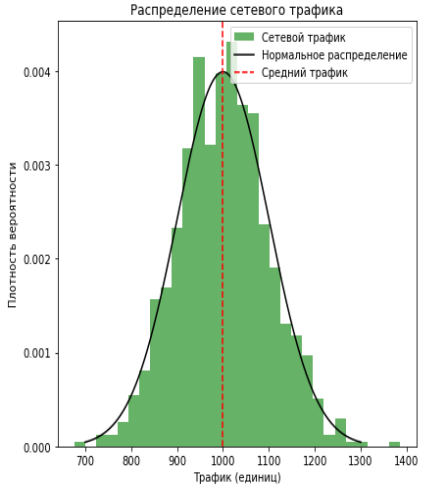
$Input_B(t)$ — Входные данные для подсистемы B из подсистемы A

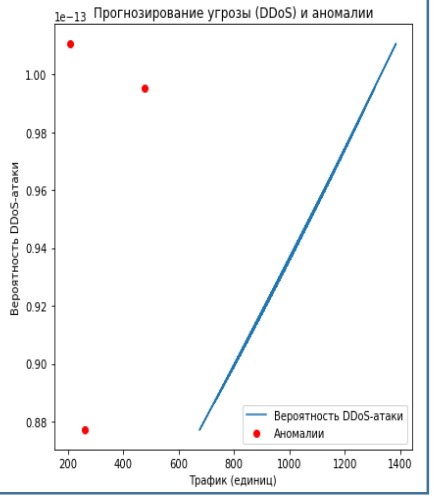
$\Sigma(t)$ — Корректирующие воздействия на модель

Пример моделирования

$$D(t) = \{x_1, x_2, \dots, x_{1000}\}, \quad x_i \sim N(\mu, \sigma^2). \quad (15.2)$$

$$P(T_{DDoS} \mid D(t)) = \frac{1}{1 + e^{-(\alpha \cdot x_{\text{норм}} + \beta)}}, \quad x_{\text{норм}} = (x - \mu)/\sigma \quad (15.3)$$





2. Комплекс моделей ЦД объекта КИИ

Вычислительная модель цифрового двойника объекта КИИ

Алгоритм модели:

1. Декомпозиция объекта: $D(o) \to \{l_1, l_2, \ldots, l_n\}$
2. Уязвимости на уровне l : $V_L = \{v_1, v_2, \ldots, v_k\}$
3. Злоумышленники, эксплуатирующие уязвимости: $A_L = \{a \in A \mid \exists v \in V_L,\ \text{Method}(a) \triangleright v\}$
4. Угрозы: $T_L = \{\tau_i = (v_j, a_k) \mid v_j \in V_L,\ a_k \in A\}$
5. Контрмеры: $\forall \tau_i \in T_L,\ \exists m \in M_L : m \vdash \tau_i$
6. Соответствие нормативам: $m \vDash N_L$
7. Стратегия защиты на уровне l : $\text{Strategy}(l) = \{(\tau_i, m_j) \mid m_j \vdash \tau_i,\ m_j \vDash N_L\}$
8. Общая стратегия защиты объекта: $\text{Strategy}(O) = \bigcup_{l \in L} \text{Strategy}(l)$

Пример — уровень: АСУ ТП (технический)

Элемент	Значение
V_L	v_1: удалённый доступ, v_2: доступ к внутренней сети
A_L	a_1: внешняя группа, a_2: внутренний инсайдер
T_L	$\tau_1 = (v_1, a_1),\ \tau_2 = (v_2, a_2)$
M_L	m_1: межсетевой экран, m_2: сегментация сети, m_3: SIEM
Проверки	$m_1 \vdash \tau_1,\ m_2 \vdash \tau_2,\ m_3 \vdash \tau_2$
Нормативы	$m_1 \vDash N_L,\ m_2 \vDash N_L,\ m_3 \vDash N_L$
$\text{Strategy}(l)$	$\{(\tau_1, m_1),\ (\tau_2, m_2),\ (\tau_2, m_3)\}$

Обозначения:

$D(o)$ — объект КИИ

l_i — уровень декомпозиции

V_L — уязвимости на уровне l

A — множество всех злоумышленников

A_L — злоумышленники, активные на уровне l

$\text{Method}(a)$ — метод атаки злоумышленника

T_L — множество угроз на уровне l

τ_i — угроза как пара (уязвимость, атакующий)

M_L — контрмеры, применимые на уровне l

$m \vdash \tau_i$ — контрмера m нейтрализует угрозу τ_i

N_L — нормативные требования уровня

$m \vDash N_L$ — контрмера m соответствует нормативам

$\text{Strategy}(l)$ — стратегия защиты уровня

$\text{Strategy}(O)$ — совокупная стратегия объекта КИИ

2. Комплекс моделей ЦД объекта КИИ

Суть: предложен комплекс моделей ЦД объекта КИИ, построенный в логике: онтологическая модель → концептуальная модель → вычислительная модель, обеспечивающий формализованное представление объектов и угроз ИБ КИИ, а также механизмов их обнаружения и нейтрализации.

Научная новизна: Впервые предложен комплекс моделей ЦД объекта КИИ, интегрирующий онтологическую формализацию знаний, концептуальную модель с двусторонним взаимодействием, включающую ЦД как инструмент прогнозирования и предотвращения угроз, а также механизмы защиты самого ЦД от кибератак, а также вычислительную модель формирования адаптивных защитных стратегий, что обеспечивает системный подход к прогнозированию и предотвращению киберугроз с учетом уровневой декомпозиции объекта КИИ и нормативных требований регуляторов.

Теоретическая значимость:

1. Онтологическая модель расширяет теорию формализации знаний в области информационной безопасности объектов КИИ, структурируя знания об угрозах, уязвимостях и защитных механизмах с декомпозицией по уровням системы.
2. Концептуальная модель дополняет теорию системного моделирования, описывая динамическое двустороннее взаимодействие цифрового двойника и объекта КИИ с использованием методов машинного обучения для прогнозирования угроз и адаптивного реагирования.
3. Вычислительная модель вносит вклад в методологию построения комплексных защитных стратегий с учетом анализа уязвимостей, характеристик злоумышленников и нормативных требований.

Практическая значимость: На базе разработанного комплекса моделей возможно формирование ЦД объектов КИИ, которые обеспечивают автоматизированное прогнозирование киберугроз, обнаружение отклонений в поведении системы (аномалий), указывающих на потенциальные инциденты безопасности, и синтез адаптивных стратегий защиты.

Соответствие паспорту специальности:

П. 3. *Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.*

П. 7. *Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.*

По данному результату опубликовано 6 работы (из них 5 в Scopus)

3. Расширенная модель угроз ИБ объектам КИИ

Интеграция ЦД в процесс моделирования угроз обеспечивает следующие преимущества:

- Повышение точности анализа за счет учета реальных данных о состоянии объекта.
- Оперативность принятия решений благодаря симуляции сценариев в режиме, близком к реальному времени.
- Адаптивность к изменениям в архитектуре объекта или появлению новых угроз.

3. Расширенная модель угроз ИБ объектам КИИ

Интеграция ЦД в модель угроз ИБ объектов КИИ

Этап моделирования	Действия с использованием ЦД	Преимущества и результаты
1. Описание объекта защиты	Создание виртуальной модели объекта КИИ	Точное моделирование архитектуры, выявление критичных компонентов и каналов распространения угроз
2. Определение источников угроз	Мониторинг данных в реальном времени для выявления аномалий и неавторизованных действий	Идентификация внутренних и внешних нарушителей, анализ их поведения и мотивации
3. Формирование списка уязвимостей	Проведение стресс-тестов и имитационного анализа компонентов для выявления слабых мест	Обнаружение технических и организационных уязвимостей, оценка их критичности
4. Определение перечня угроз безопасности	Симуляция сценариев атак (внедрение вредоносного кода, подмена данных) на виртуальной модели.	Верификация актуальности угроз, адаптация списка под специфику объекта.
5. Определение атрибутов угроз	Анализ интенсивности, продолжительности и последствий угроз на основе данных симуляции.	Качественная оценка вероятности реализации угроз и их потенциального ущерба.
6. Прогнозирование киберфизических последствий	Моделирование воздействия угроз на технологические процессы (например, перегрузка сети).	Оценка реальных физических последствий (аварии, остановка производства, финансовые потери).
7. Верификация защитных мер	Тестирование эффективности существующих мер защиты на цифровой модели.	Оптимизация архитектуры безопасности, снижение затрат на внедрение неэффективных решений.

Формализация базовой и расширенной моделей угроз

Базовая модель

$$T = S \wedge V \wedge O \rightarrow (I \rightarrow C), \quad (19.1)$$

S — источник угрозы,
V — уязвимость,
O — объект воздействия,
I — способ реализации угрозы,
C — последствия.

Расширенная модель

$$T_{ext} = (S \otimes V \otimes O \otimes K \otimes D) \rightarrow (I \otimes C \otimes DT), \quad (19.2)$$

K – контекст системы,
D – динамические факторы,
DT – цифровой двойник системы, включающий четыре компонента:

- Sim(A) — моделирование атак;
- Pred(C) — прогнозирование последствий;
- Resp(M) —внедрение защитных мер в режиме реального времени;
- Test(R) —проведение стресс-тестов.

3. Расширенная модель угроз ИБ объектам КИИ

Суть: Расширенная модель угроз ИБ для объектов КИИ интегрирует ЦД для динамического моделирования угроз, анализа киберфизических последствий и тестирования защитных мер в виртуальной среде.
Научная новизна: Разработана новая расширенная модель угроз информационной безопасности для объектов критической информационной инфраструктуры, интегрирующая цифровой двойник и учитывающая динамические факторы, контекст системы и взаимосвязь компонентов. В модели введен итеративный цикл «анализ — верификация — корректировка» с использованием цифрового двойника, обеспечивающий повышение адаптивности и точности моделирования угроз. Формализация модели позволяет анализировать эволюцию угроз во времени и учитывать их синергетическое взаимодействие.
Теоретическая значимость: Модель расширяет теоретические основы оценки угроз информационной безопасности за счет интеграции цифрового двойника, что позволяет учитывать динамичность и сложность современных киберфизических систем, способствуя развитию адаптивного моделирования и верификации защитных мер.
Практическая значимость: Модель позволяет повысить воспроизводимость и точность оценки угроз за счет снижения субъективности экспертных методов и обеспечивает оперативное тестирование и корректировку защитных мер без воздействия на реальную инфраструктуру с использованием цифрового двойника.

Соответствие паспорту специальности:
П. 3. *Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.*
П. 7. *Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.*
П. 9. *Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.*

По данному результату опубликовано 4 работы (2 ВАК).

4. Метод и алгоритмы обнаружения угроз ИБ объектам КИИ

Метод включает следующие этапы:

1. Предобработка данных с применением частотного анализа и вейвлет-преобразования.

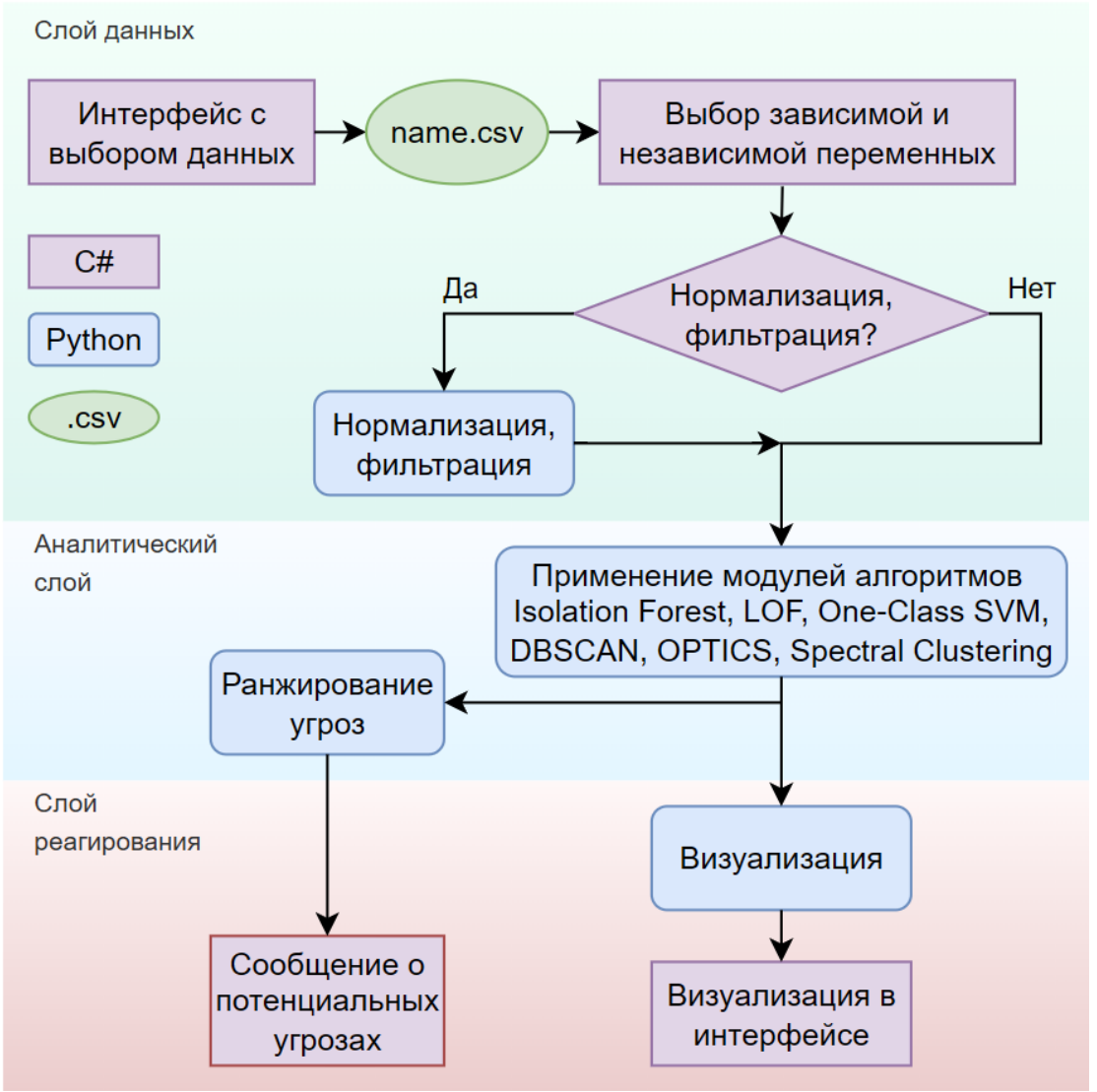
2. Параллельный анализ отклонений от нормального поведения и кластеризация данных:

- Анализ отклонений — сравнение текущих параметров с эталонными характеристиками нормального состояния;
- Кластеризация — объединение данных с похожими признаками в группы, отражающие нормальные состояния. Данные, не попадающие ни в одну группу, считаются аномальными.

Используемые алгоритмы:

- **Обнаружение аномалий:** Isolation Forest, LOF, One-Class SVM
- **Кластеризация:** DBSCAN, Spectral Clustering, OPTICS

Архитектура системы обнаружения угроз

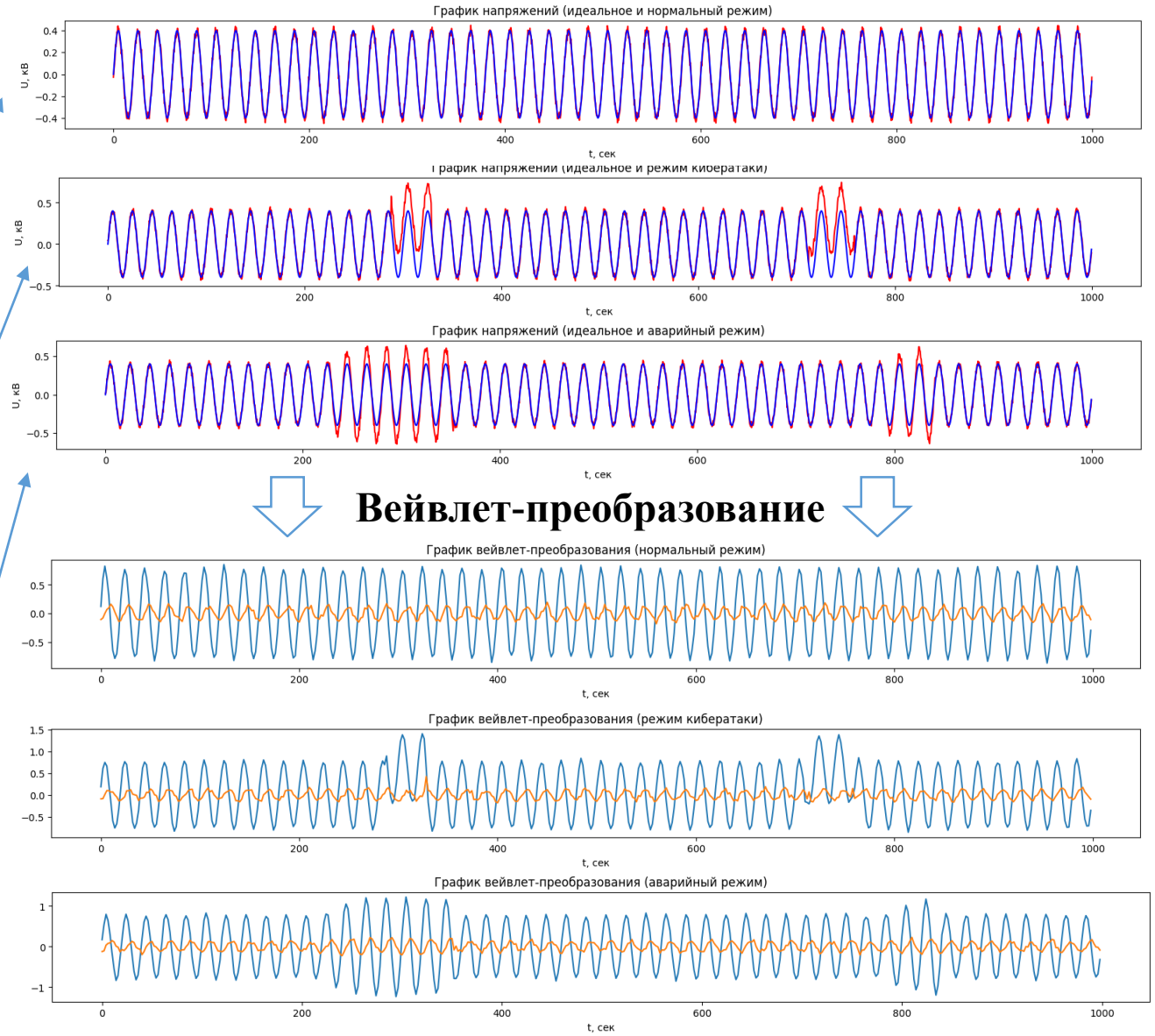


4. Метод и алгоритмы обнаружения угроз ИБ объектам КИИ

Режимы работы сети

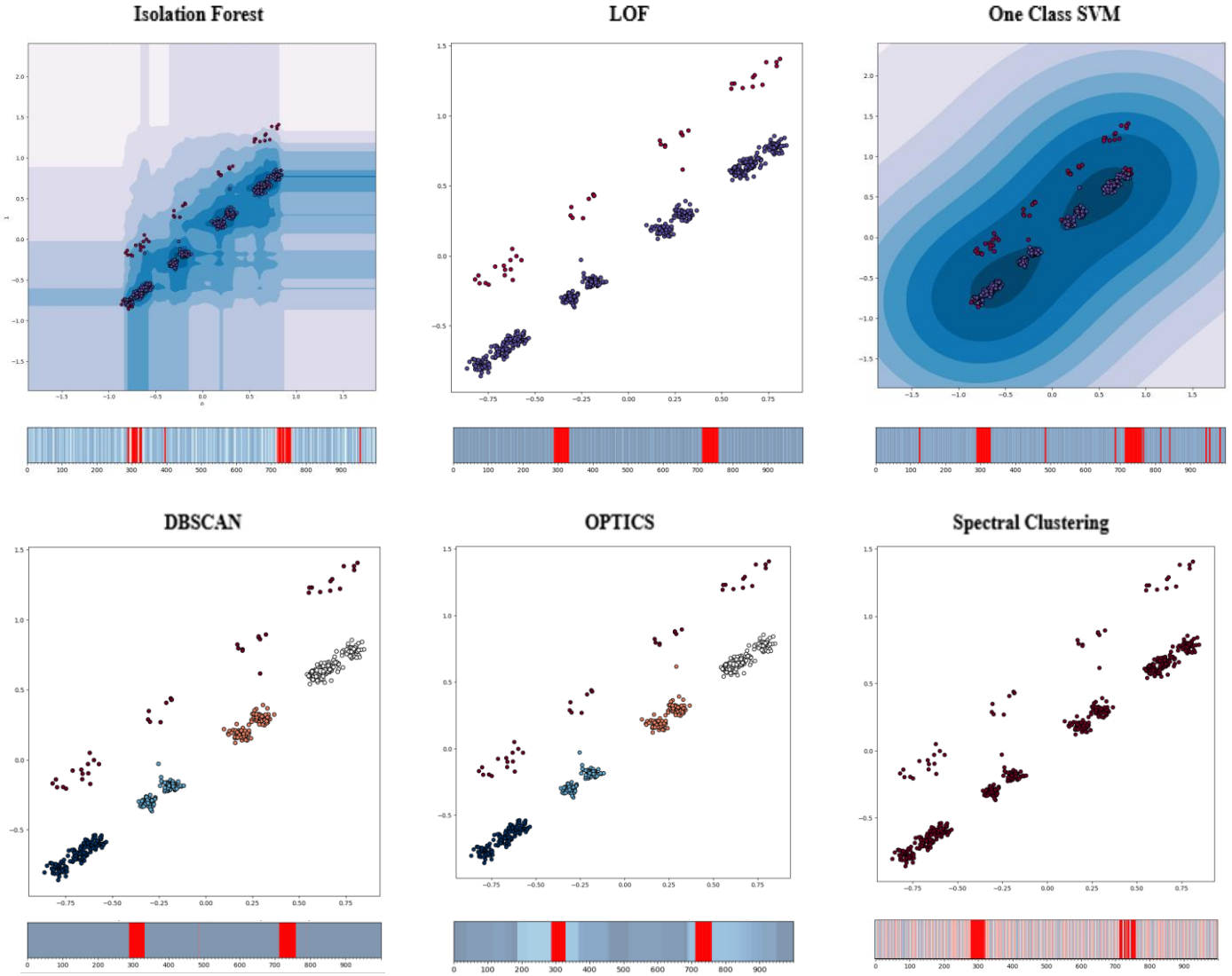
Режим	Формула	Длительность
Нормальный режим	Синусоидальная функция по времени с добавлением случайного шума: $U(t) = U_{\text{ном}} \cdot sin(2\pi ft) \pm N(0,\sigma)$, где $U_{\text{ном}}$ = 0,4 кВ; f = 50 Гц; σ = 0,05 кВ	
Режим кибератаки	Плавное увеличение с $U(t) = U_{\text{ном}} \cdot sin(2\pi ft) + \frac{(t-t_{\text{нач}})^2}{100} \pm N(0,\sigma)$ до $U(t) = U_{\text{ном}} \cdot sin(2\pi ft) + U_{\text{ка}} \pm N(0,\sigma)$, где $U_{\text{ка}} = 0{,}3$ кВ; $t_{\text{нач}}$ – начало кибератаки	50-100 с
Аварийный режим	Плавное увеличение с $U(t) = (0.4 + 0.1 \cdot e^{\frac{t-t_{\text{нач}}}{100}}) \cdot sin(2\pi ft) \pm N(0,\sigma)$ – плавное увеличение амплитуды до $U_{\text{макс}} = 0.6$ кВ	50-400 с

Исходные данные для моделирования



4. Метод и алгоритмы обнаружения угроз ИБ объектам КИИ

Графики выделения аномальных данных и тепловые карты аномалий на временной шкале (режим кибератаки)

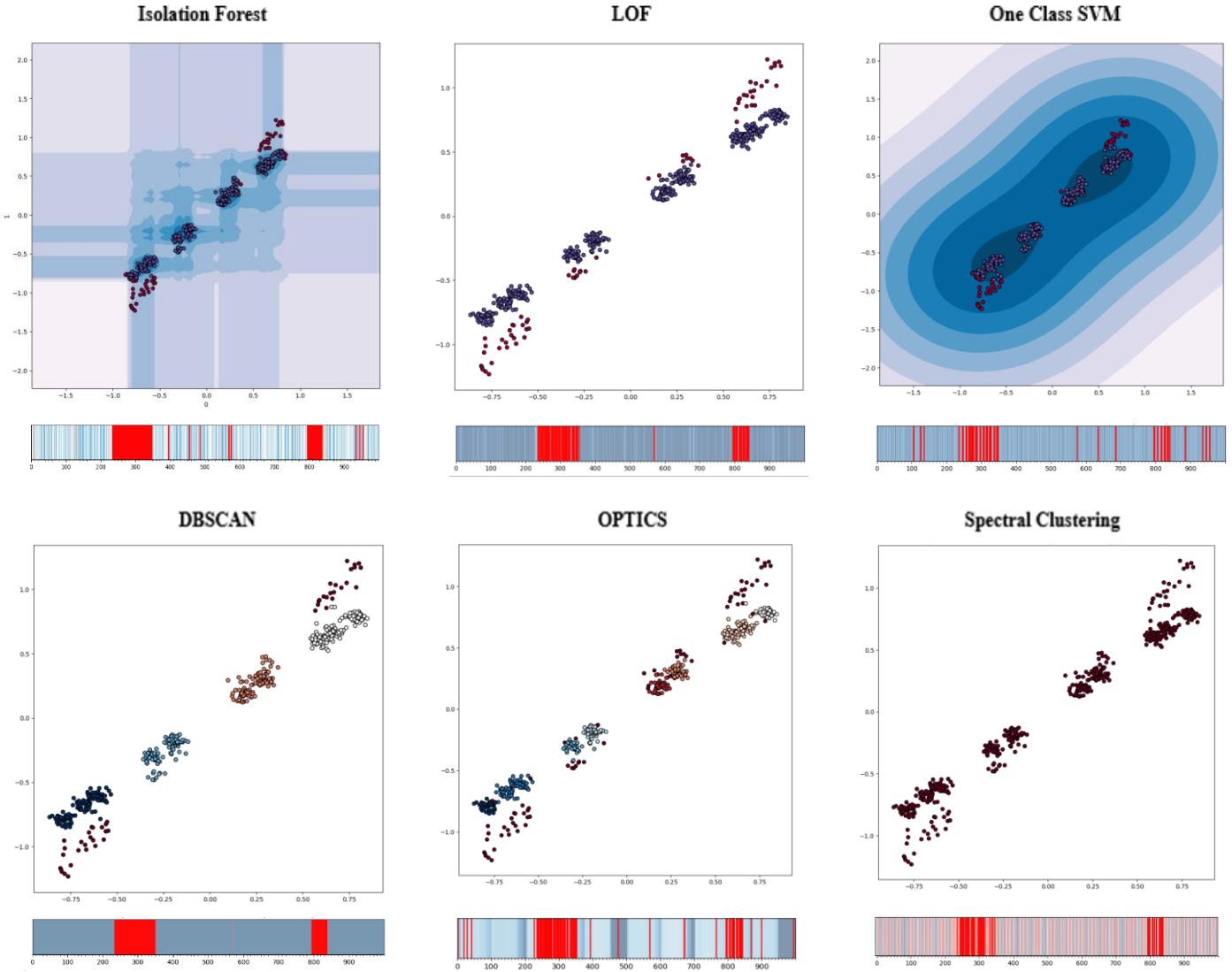


Метрики оценки

Метод	Точность	F1-Score	Время	Ложные срабатывания
Isolation Forest	98%	0.96	20 ms	2%
LOF	89%	0.82	150 ms	15%
One-Class SVM	92%	0.88	80 ms	5%
DBCAN	98%	0.95	130 ms	3%
OPTICS	96%	0.92	160 ms	8%
Spectral Clustering	92%	0.89	180 ms	12%
K-means	85%	0.78	50 ms	10%
GMM	84%	0.82	100 ms	17%

4. Метод и алгоритмы обнаружения угроз ИБ объектам КИИ

Графики выделения аномальных данных и тепловые карты аномалий на временной шкале (аварийный режим)



Метрики оценки

Метод	Точность	F1-Score	Время	Ложные срабатывания
Isolation Forest	93%	0.88	20 ms	5%
LOF	82%	0.80	150 ms	20%
One-Class SVM	83%	0.82	80 ms	10%
DBCAN	95%	0.86	130 ms	8%
OPTICS	90%	0.83	160 ms	11%
Spectral Clustering	86%	0.80	180 ms	18%
K-means	93%	0.88	20 ms	5%
GMM	82%	0.80	150 ms	20%

4. Метод и алгоритмы обнаружения угроз ИБ объектам КИИ

Суть: Разработан метод обнаружения угроз информационной безопасности объектов КИИ с использованием ЦД. Метод включает предобработку данных (вейвлет-преобразование), параллельный анализ отклонений от нормального поведения и кластеризацию векторов признаков, отражающих состояние объекта.

Научная новизна:

Разработан новый метод обнаружения угроз информационной безопасности объектов КИИна основе анализа аномалий в данных, отражающих поведение объекта. Метод отличается интеграцией частотного анализа, анализа отклонений и кластеризации признаков с параллельной обработкой на стороне цифрового двойника. В рамках метода осуществлен обоснованный выбор и применение алгоритмов машинного обучения, адаптированных к задаче детектирования аномалий в данных, представляющих параметры функционирования объектов КИИ.

Теоретическая значимость: Развитие теоретических основ обнаружения угроз информационной безопасности объектам КИИ за счет интеграции алгоритмов определения аномалий и применения ЦД для моделирования поведения систем.

Практическая значимость: Результаты работы будут полезны разработчикам и операторам систем защиты критической информационной инфраструктуры для мониторинга и своевременного выявления угроз информационной безопасности

Соответствие паспорту специальности:

П. 3. *Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.*

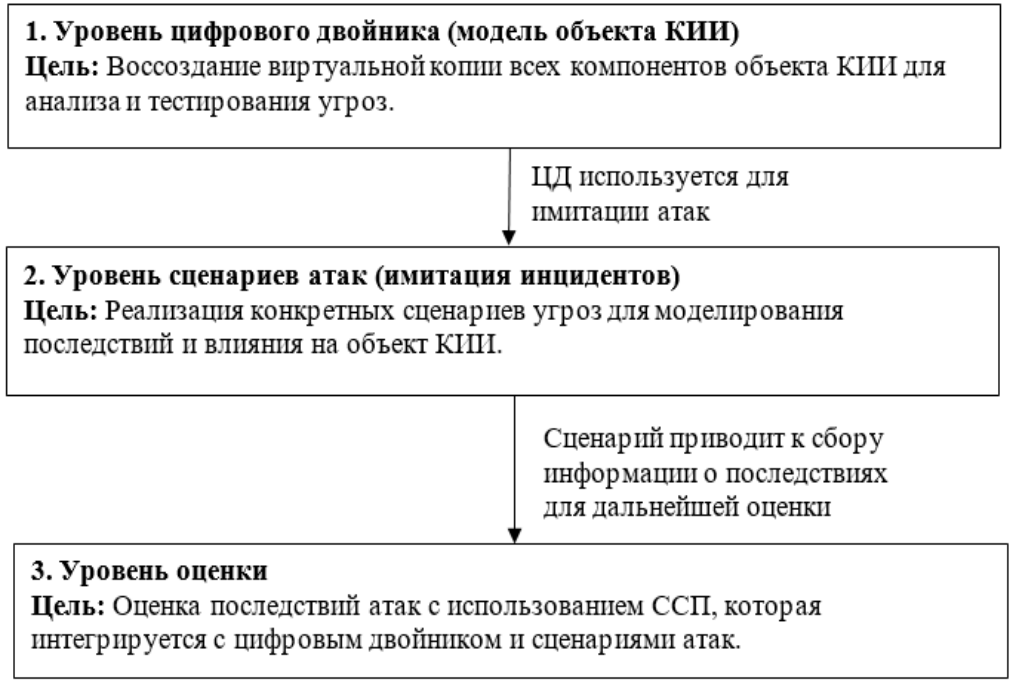
П. 6. *Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.*

По данному результату опубликовано 14 работ (Scopus: 4, ВАК: 3)

5. Комплекс методик оценки угроз ИБ объектам КИИ

Методика количественной оценки угроз для объектов КИИ на основе системы показателей

Архитектура методики



Методика включает:

1.Формирование системы показателей (например, доля уязвимостей, время простоя, потери данных);
2.Сбор данных в реальном времени с помощью ЦД;
3.Предобработку и нормирование данных;
4.Расчет интегральных показателей угроз

Апробация на синтетических данных

№	Показатель	Значение	Пороговые значения	Нормализованное значение
Показатели вероятности реализации угрозы				
1.1	Количество аналогичных инцидентов за год	4	Высокий риск: >5	0.8
1.2	Доля незакрытых уязвимостей (%)	18%	Критично: >20%	0.9
1.3	Частота срабатываний защиты/мес	12	Высокий риск: >15	0.8
Интегральный показатель вероятности реализации угрозы				0.83
Показатели масштаба ущерба				
2.1	Время простоя системы (часы)	10	Критично: >12	0.83
2.2	Процент потери данных (%)	8%	Критично: >10%	0.8
2.3	Финансовые потери (у.е.)	45,000	Критично: >50,000	0.94
Интегральный показатель масштаба ущерба				0.86
Интегральный показатель уровня угрозы = 0,845				

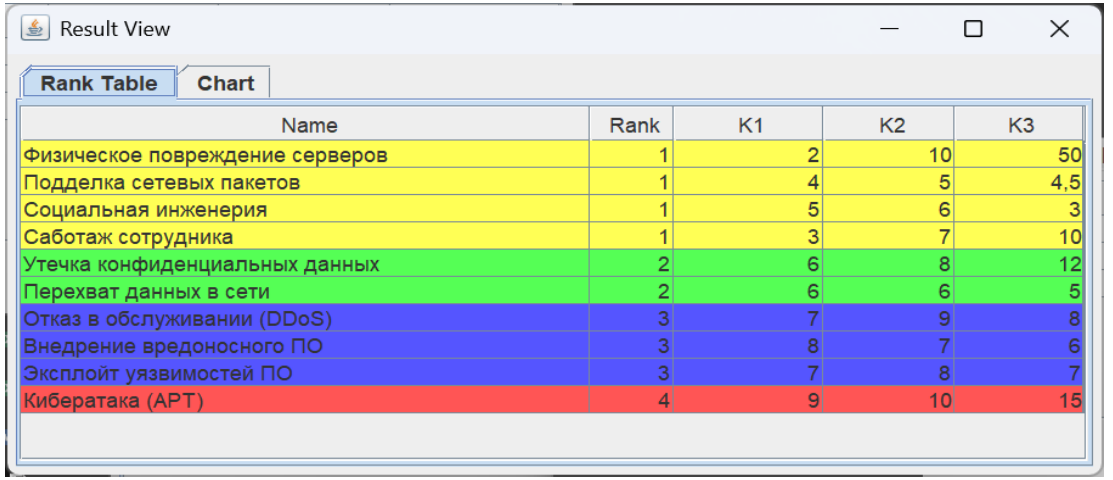
5. Комплекс методик оценки угроз ИБ объектам КИИ

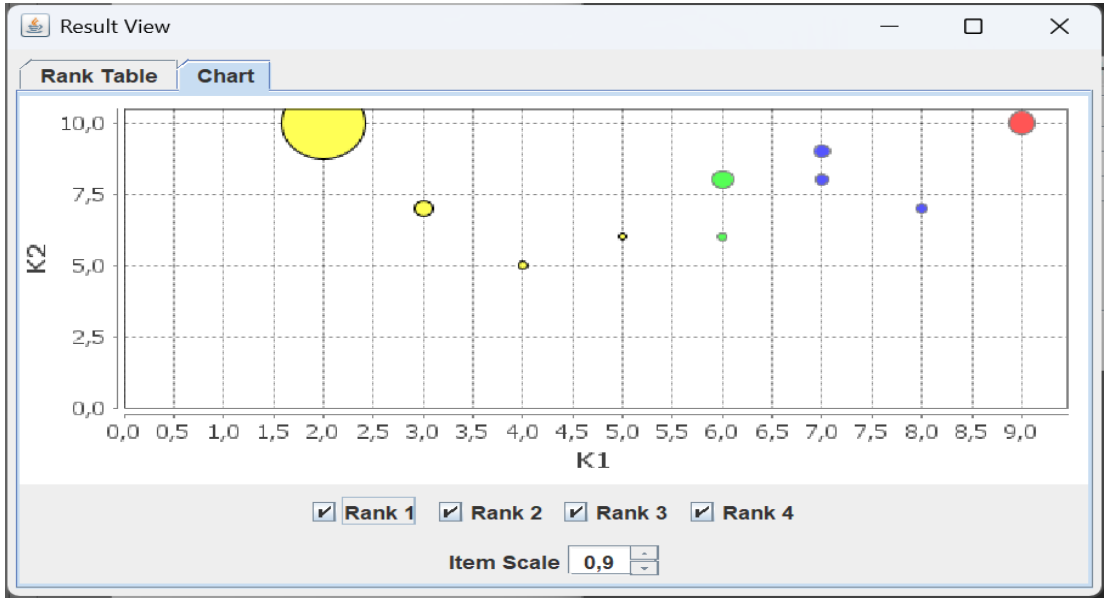
Методика многокритериальной оценки угроз ИБ объектов КИИ

Алгоритм методики

1. **Формирование исходных данных:**
   Определяется множество угроз: $T = \{T_1, T_2, \ldots, T_m\}$;
   задаются критерии оценки: $C = \{C_1, C_2, \ldots, C_k\}$.
2. **Выделение значимых угроз по критериям:**
   Для каждого критерия C_i отбираются угрозы с граничными значениями:
   $T_1^{(1)}, T_2^{(1)}, \ldots, T_k^{(1)}$.
3. **Формирование объединённого множества:**
   Объединяются угрозы, отобранные по всем критериям:
   $T^{(1)} = \bigcup_{i=1}^{k} T_i^{(1)}$.
4. **Исключение доминируемых угроз:**
   Удаляются угрозы, уступающие остальным по всем критериям одновременно.
5. **Итерационный анализ:**
   Шаги 2–4 повторяются для оставшихся угроз, пока на итерации $t = T$ не останется менее двух элементов.
   На каждой итерации формируется:
   $T^{(t)} = \bigcup_{i=1}^{k} T_i^{(t)}$.
6. **Формирование итогового множества:**
   Все полученные в итерациях подмножества объединяются:
   $M_{\text{итог}} = \bigcup_{t=1}^{T} T^{(t)}$.
7. **Сопоставление с требованиями:**
   Проверяется соответствие угроз нормативам и стратегическим приоритетам, при необходимости корректируются показатели.
8. **Финальное ранжирование:**
   Множество $M_{\text{итог}}$ упорядочивается по степени значимости угроз, формируется итоговая классификация.

Пример апробации методики





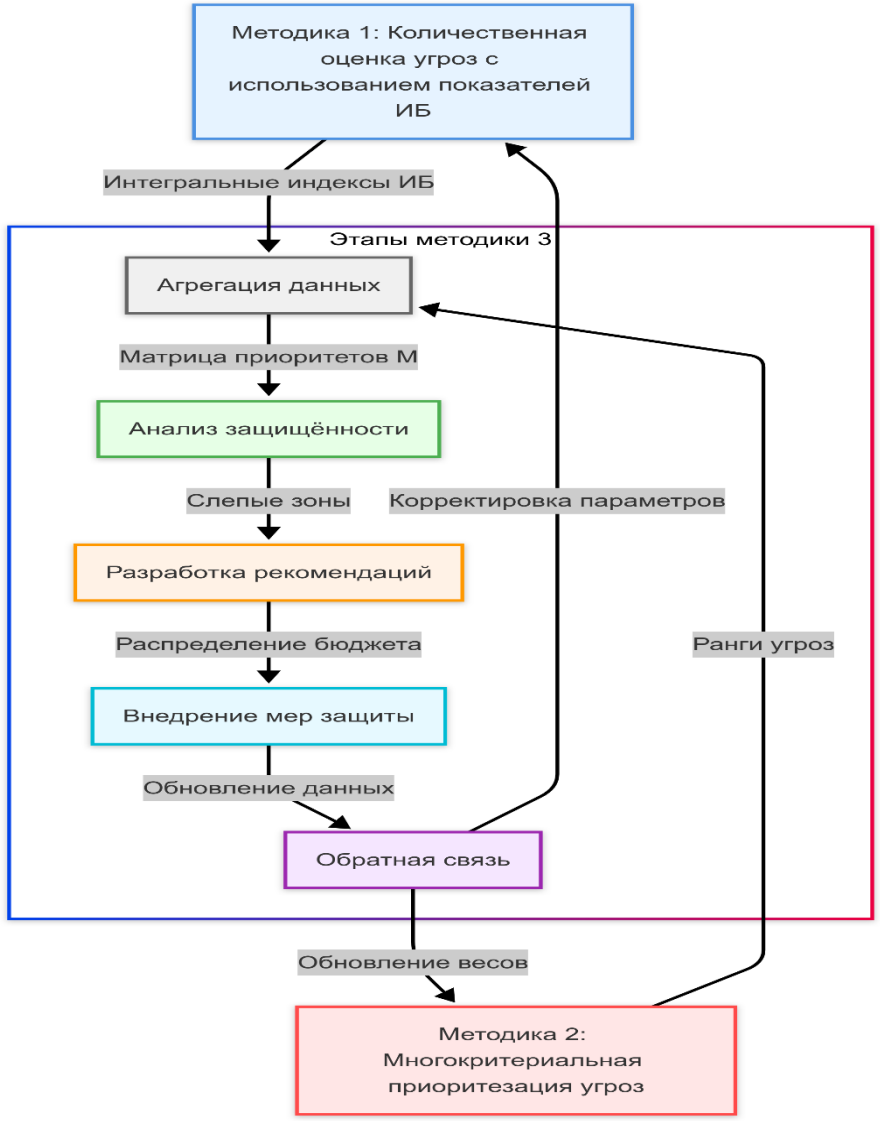
5. Комплекс методик оценки угроз ИБ объектам КИИ

Методика повышения защищенности объектов КИИ

Алгоритм методики

1. **Агрегация данных**
   Множество угроз: $T = \{T_1, T_2, \dots, T_n\},\ n = |T|$
   Для каждой угрозы T_i на вход поступают:
   — интегральный индекс $K_{\Sigma,i}$
   — ранг R_i
   — активы $A_i \subseteq A$,
   — уязвимости $V_i \subseteq V$
   Формируется матрица:
   ***Результат*:** матрица приоритетов: $M = (T_i, R_i, K_{\Sigma,i}, A_i, V_i)$
2. **Анализ защищённости**
   Сопоставление угроз T_i с мерами защиты по соответствующим A_i, V_i
   — аудит (технический, организационный)
   — симуляция атак через ЦД
   ***Результат*:** выявление угроз с высоким R_i и/или низким $K_{\Sigma,i}$ без достаточных защитных мер
3. **Разработка рекомендаций**
   Расчет бюджета: $B_i \sim K_{\Sigma,i} \times R_i$
   ***Результат*:** формирование адресных рекомендаций и распределение ресурсов на их реализацию.
4. **Обратная связь**
   — мониторинг
   — обновление данных ЦД
   — корректировка параметров (пересмотр пороговых значений интегрального индекса и изменение весов критериев ранжирования)
   Результат: адаптация методики для повышения точности и эффективности мер защиты.

Схема взаимосвязи методик



5. Комплекс методик оценки угроз ИБ объектам КИИ

Суть: Разработан комплекс взаимосвязанных методик количественной и многокритериальной оценки угроз для объектов КИИ, включающий использование ЦД, сбалансированной системы показателей и принципов Парето-оптимальности для обоснованного ранжирования выявленных угроз.

Научная новизна: Разработан комплекс взаимосвязанных методик оценки угроз для объектов КИИ, включающий использование цифрового двойника и многокритериальное ранжирование на основе принципов Парето-оптимальности. Предложенный подход отличается интеграцией цифрового двойника как элемента количественной оценки, применением Парето-оптимальности в анализе угроз информационной безопасности, а также реализацией замкнутого цикла «оценка → действие → контроль». Это позволяет обеспечить переход от данных цифрового моделирования к структурированной оценке и формированию адресных аналитических выводов.

Теоретическая значимость: Расширена методология количественной и многокритериальной оценки угроз для объектов КИИ за счет использования цифрового двойника и применения принципов Парето-оптимальности.

Практическая значимость: Разработанные методики позволяют организациям, эксплуатирующим объекты КИИ, проводить оценку и ранжирование угроз за счет данных цифрового двойника, формировать обоснованные рекомендаций для повышения уровня защищенности объекта КИИ.

Соответствие паспорту специальности:

П. 3. *Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.*

П. 10. *Модели и методы оценки защищенности информации и информационной безопасности объекта.*

Всего по данному результату опубликовано 15 работ (ВАК: 5, Scopus: 1, Программы для ЭВМ: 5)

Выводы

1. Разработана многоаспектная модель декомпозиции компонентов КИИ по пяти взаимосвязанным признакам, обеспечивающая структурированное представление угроз и интеграцию многослойного цифрового двойника для анализа угроз информационной безопасности

2. Предложен комплекс моделей цифрового двойника объекта КИИ, включающий онтологическую, концептуальную и вычислительную модели для анализа угроз объектам КИИ.

3. Разработана расширенная модель угроз информационной безопасности объектам КИИ, объединяющая нормативно-регламентированный подход ФСТЭК с технологиями цифровых двойников для динамического моделирования угроз, анализа киберфизических последствий и тестирования защитных мер в виртуальной среде.

4. Разработан метод обнаружения угроз информационной безопасности объектов КИИ с использованием цифрового двойника, включающий частотный анализ, анализ отклонений от нормального поведения и кластеризацию данных. На основе этих методов подобраны алгоритмы машинного обучения, реализованные в многослойной архитектуре (сбор данных, аналитика, реагирование), обеспечивающей автоматизированное выявление угроз в режиме реального времени без воздействия на физические объекты.

5. Разработан комплекс методик, обеспечивающий системный подход к оценке угроз ИБ объектов КИИ, сочетая количественное моделирование через цифровой двойник (ЦД), многокритериальный анализ (МКА) для выявления наиболее критичных угроз, и трансформацию аналитических данных в практические рекомендации по защите, реализующие замкнутый цикл оценки, адаптации и контроля.

Список публикаций по теме исследования

Журналы из перечня ВАК (К1 и К2)

1. Кочергин С.В., Артемова С.В., Бакаев А.А., Митяков Е.С., Вегера Ж.Г., Максимова Е.А. Повышение безопасности смарт-сетей: спектральный и фрактальный анализ как инструменты выявления кибератак // Russian Technological Journal. – 2025. – Т. 13, № 1. – С. 7–15. **(ОНР 4)** **(К1, ядро РИНЦ)**
2. Митяков Е.С., Артемов С.В., Бакаев А.А., Душкин А.В., Вегера Ж.Г. Модель оценки эффективности систем защиты информации // Безопасность информационных технологий. – 2024. – Т. 31, № 4. – С. 56–66. **(ОНР 5)** **К2**
3. Митяков Е.С., Максимова Е.А., Артемова С.В., Бакаев А.А., Вегера Ж.Г. Моделирование процессов управления инцидентами информационной безопасности на предприятии // Russian Technological Journal. – 2024. – Т. 12, № 6. – С. 39–47. **(ОНР 3)** **(К1, ядро РИНЦ)**
4. Кочергин С.В., Артемова С.В., Бакаев А.А., Митяков Е.С., Вегера Ж.Г., Максимова Е.А. Кибербезопасность смарт-сетей: сравнение подходов машинного обучения для обнаружения аномалий // Russian Technological Journal. – 2024. – Т. 12, № 6. – С. 7–19. **(ОНР 4)** **(К1, ядро РИНЦ)**
5. Митяков Е.С., Артемова С.В., Бакаев А.А., Душкин А.В., Вегера Ж.Г. Оценка эффективности информационной безопасности в условиях региональных различий // Информатизация и связь. – 2024. – № 4. – С. 83–89. **(ОНР 5)** **(К2)**
6. Артемова С.В., Бакаев А.А., Митяков Е.С., Вегера Ж.Г., Шувалова А.М. Обнаружение и устранение угроз и уязвимостей безопасности информации при работе мобильных групп поиска // Информатизация и связь. – 2024. – № 4. – С. 95–101. **(ОНР 5)** **(К2)**
7. Морозов В.Е., Артемова С.В., Бакаев А.А., Митяков Е.С., Вегера Ж.Г. Комплексные решения для минимизации внутренних угроз кибербезопасности // Защита информации. Инсайд. – 2024. – № 6 (120). – С. 36–44. **(ОНР 3)** **(К2)**
8. Митяков Е.С., Бакаев А.А., Максимова Е.А., Артемова С.В., Вегера Ж.Г. Моделирование рисков реализации кибератак в региональных экономических системах // Защита информации. Инсайд. – 2024. – № 5 (119). – С. 45–49. **(ОНР 5)** **(К2)**
9. Артемова С.В., Бакаев А.А., Митяков Е.С., Лонин А.М., Спиридонов А.С. Open-source как механизм повышения независимости и устойчивости в контексте геополитической нестабильности // Информатизация и связь. – 2024. – № 4. – С. 90–94. **(ОНР 5)** **(К2)**
10. Кочергин С.В., Артемова С.В., Бакаев А.А., Максимова Е.А., Митяков Е.С., Вегера Ж.Г. Обнаружение аномалий в энергосистемах: применение модели Isolation Forest для выявления киберугроз // Безопасность информационных технологий. – 2024. – Т. 31, № 3. – С. 112–121. **(ОНР 4)** **(К2)**

Журналы и конференции Scopus

1. Yudin A., Mityakov E., Grosheva P., Ladynin A., Myakishev Y. Agent-based modeling in multi-level industrial ecosystems development // Relacoes Internacionais no Mundo Atual. – 2023. – Vol. 4, No. 42. – P. 703–712. **(ОНР 2)** **Q3 УБС4**
2. Mityakov E.S., Tereshina V.V., Mityakov S.N., Kazakevich I.D., Ladynin A.I. Industrial Ecosystems' Information Security Processes Provision Modeling // Proceedings of the 2025 Conference of Young Researchers in Electrical and Electronic Engineering (ElCon). – 2025. – P. 411–414. **(ОНР 2)**
3. Mityakov E.S., Mityakov S.N., Ladynin A.I., Mikaeva A.S., Kryukova T.M., Kozlov Y.V. Industrial Ecosystem Knowledge-management Digital Platform Model Development // Proceedings of the 2025 Conference of Young Researchers in Electrical and Electronic Engineering (ElCon). – 2025. – P. 415–418. **(ОНР 2)**
4. Mityakov E.S., Mityakov S.N., Shmeleva A.G., Ladynin A.I., Artemova S.V., Kamenskaia M.A. Russian Regions Scientific and Technical Security Indicators' Dynamics Neural Network Modeling // 2022 III International Conference on Neural Networks and Neurotechnologies (NeuroNT). – 2022. – DOI: 10.1109/NeuroNT55429.2022.9805536. **(ОНР 4)**
5. Mityakov E.S., Ladynin A.I., Kazakevich Critical Information Infrastructures Protection Architecture Based on Hybrid Data Analysis and AI Algorithms // 2025 VI International Conference on Neural Networks and Neurotechnologies (NeuroNT). (в печати) **(ОНР 4)**
6. Mityakov E.S., Ladynin A.I., Kazakevich I.D. Mityakov E.S., Ladynin A.I.,, Shmeleva A.G., Kazakevich Critical Information Infrastructures Intelligent Protection: Digital Twins and Neural Network-Based Threat Detection Methods (в печати). // 2025 VI International Conference on Neural Networks and Neurotechnologies (NeuroNT). (в печати) **(ОНР 4)**
7. Mityakov E.S., Ladynin A.I., Karpuhina N.N. Deep Learning Enhanced Predictive Maintenance Framework Using Industrial Internet of Things Sensors for Smart Manufacturing Systems // International Journal of Industrial Engineering and Management. (в печати) **(ОНР 2)** **УБС2, Q2**
8. S. N. Mityakov, E. S. Mityakov, A. I. Ladynin, T. M. Kryukova. Toolset for Assessing the Import Substitution of Economic Systems at Various Hierarchical Levels // Studies on Russian Economic Development. – 2025. – Vol. 36, No. 2. – P. 203-211. (**ОНР 1**). **УБС2, Q3**
9. Yudin A., Mityakov E., Grosheva P., Ladynin A., Myakishev Y. Industrial Ecosystems Sustainable Development Management Conceptual Model // Journal of Lifestyle and SDG'S Review. – 2025. – Vol. 5, No. 2. – P. e04038.. **(ОНР 2)** **Q4**
10. Mityakov S. N., Mityakov E.S. Analysis of Crisis Phenomena in the Russian Economy Using Fast Indicators of Economic Security // Studies on Russian Economic Development. – 2021. – Vol. 32, No. 3. – P. 245-253. **(ОНР 4).** **УБС2, Q3**
11. Mityakov S. N., Mityakov E.S., Ladynin A.I., Nazarova E.A. Country Economic Security Monitoring Rapid Indicators System // Economies. – 2023. – Vol. 11, No. 8. – P. 208. (**ОНР 5**). **Q2**
12. Mityakov, E. Expert insights into mesolevel industrial ecosystems: pathways for economic transformation / E. Mityakov, N. Kulikova // International Journal of Industrial Engineering and Management. – 2024. – Vol. 15, No. 3. – P. 213-224. – DOI 10.24867/ijiem-2024-3-358. (**ОНР 0**). **УБС2, Q2**

Список публикаций по теме исследования

Иные публикации

1. Митяков Е.С., Абраменко Т.В. Теоретические аспекты экономической безопасности российской сферы телекоммуникаций // Развитие и безопасность. – 2024. – № 4 (24). – С. 34–47. **(ОНР 5)**
2. Митяков Е.С., Козлов Я.В. Системы искусственного интеллекта в управлении производственными системами // Региональная и отраслевая экономика. – 2024. – № 1. – С. 88–95. **(ОНР 4)**
3. Митяков Е.С., Ладынин А.И., Козлов Я.В. Концептуальная модель управления сложными производственными системами в условиях цифровой трансформации // Журнал прикладных исследований. – 2023. – № 9. – С. 38–43. **(ОНР 4)**
4. Митяков С.Н., Митяков Е.С. Машинное обучение в задачах исследования инновационных процессов // Журнал прикладных исследований. – 2020. – № 4-1. – С. 6–13. **(ОНР 4)**
5. Митяков Е.С., Козлов Я.В. Система показателей управления производственной системой в условиях цифровой трансформации // Инновации и инвестиции. – 2024. – № 2. – С. 596–600. **(ОНР 5)**
6. Митяков Е.С., Лимасов А.М. Некоторые проблемы подготовки ИТ-специалистов для цифровой экономики России // Актуальные вопросы экономики, менеджмента и инноваций. – Нижний Новгород: НГТУ, 2021. – С. 278–280. **(ОНР 0)**
7. Митяков Е.С., Ладынин А.И. Концептуальная модель информационной системы совершенствования научно-технологической безопасности // Актуальные вопросы экономики, менеджмента и инноваций. – Нижний Новгород: НГТУ, 2022. – С. 188–189. **(ОНР 0)**
8. Лапаев Д.Н., Митяков Е.С. Многокритериальный анализ регионов ПФО в системе показателей энергетической безопасности // Экономическая безопасность России: проблемы и перспективы. – Нижний Новгород: НГТУ, 2014. – С. 187–191. **(ОНР 5)**
9. Митяков Е.С. Теоретические аспекты использования имитационного, сценарного и агент-ориентированного моделирования промышленных экосистем // Актуальные вопросы экономики, менеджмента и инноваций. – Нижний Новгород, 2024. – С. 129–131. **(ОНР 4)**
10. Амосов Е.А., Митяков Е.С. Реализация NPM-пакета для анализа временных рядов в web-приложениях // Хроники цифровых трансформаций. – Москва, 2024. – С. 20–23. **(ОНР 4)**
11. Митяков Е.С., Ладынин А.И., Козлов Я.В. Процедура управления производственными системами на основе методов искусственного интеллекта // Математическое и компьютерное моделирование и бизнес-анализ. – Нижний Новгород: ННГУ, 2024. – С. 136–141. **(ОНР 4)**
12. Митяков Е.С. Междисциплинарный подход к классификации угроз информационной безопасности критическим информационным инфраструктурам (в печати). **(ОНР 3)**
13. Митяков Е.С. Эволюция концепций и технологий защиты информации в критических информационных инфраструктурах (в печати). **(ОНР 3)**
14. Митяков Е.С. К вопросу об использовании методологии сбалансированной системы показателей в задачах оценки информационной безопасности объектов критической информационной инфраструктуры (в печати). **(ОНР 5)**
15. Митяков Е. С. Проблемы использования цифровых двойников в задачах обеспечения информационной безопасности объектов критической информационной инфраструктуры // Информационные технологии и телекоммуникации. 2023. Т. 11. № 4. С. 36–47. (**ОНР 1**)
16. Митяков Е. С. Цифровые двойники как объект и инструмент информационной безопасности // Информационные технологии и телекоммуникации. 2024. Т. 12. № 4. С. 1–12. **(ОНР 2)**
17. Митяков Е.С. Цифровые двойники и безопасность критической информационной инфраструктуры: правовые и технологические аспекты // Национальная безопасность и стратегическое планирование (в печати) **(ОНР 1)**
18. Митяков Е.С., Казакевич И.Д., Ладынин А.И. Алгоритмы кластеризации машинного обучения для обнаружения угроз в критически важных информационных инфраструктурах // Математическое и компьютерное моделирование и бизнес-анализ. – Нижний Новгород: ННГУ, 2025. (в печати) (**ОНР 4**).

Свидетельства о государственной регистрации баз данных и программ для ЭВМ

1. Митяков Е.С., Смирнов М.В. База данных комплексных угроз информационной безопасности критической информационной инфраструктуры. Свидетельство № 2025621506/69. – 2025. **(ОНР 1)**
2. Митяков Е.С., Лапаев Д.Н., Корнев Е.А. Программа решения многокритериальных задач с применением методики определения ранжированных взаимоприемлемых альтернатив. Свидетельство №2015612049. – 2015. **(ОНР 5)**
3. Митяков Е.С., Лапаев Д.Н., Корнев Е.А. Программа для решения трех- и более критериальных задач. Свидетельство №2014610410. – 2014. **(ОНР 5)**
4. Митяков Е.С., Лапаев Д.Н., Корнев Е.А. Программа для ранжированного решения трех- и более критериальных задач. Свидетельство №2014610635. – 2014. **(ОНР 5)**
5. Митяков Е.С., Лапаев Д.Н., Корнев Е.А. Программа для ранжированного решения двухкритериальных задач. Свидетельство №2014610636. – 2014. **(ОНР 5)**
6. Митяков Е.С., Лапаев Д.Н., Корнев Е.А. Программа для решения трехкритериальных задач. Свидетельство №2014610637. – 2014. **(ОНР 5)**

Спасибо за внимание