



МИРЭА - Российский технологический университет

МЕТОДОЛОГИЯ АНАЛИЗА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ 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**

**Научный консультант: д.т.н., профессор
Саенко Игорь Борисович**

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

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.

Анализ угроз ИБ

Авторы: Дойникова Е.В. , Федорченко А.В. , Котенко И.В., Саенко И.Б., Захарченко Р.И., Величко Д.В., Чечулин А.А., Полубелова О.В., Sabah Suhail, Sherali Zeadally, Raja Jurdak

Результаты: Разработаны и совершенствованы методы выявления, оценки и управления угрозами информационной безопасности с применением современных моделей и технологий

ЦД в задачах ИБ

Авторы: Касимова А.Р., Золотарев В.В., Сафиуллина Л.Х., Балыбердин А.С., Минзов А.С., Невский А.Ю., Баронов О.Р., Немчанинова С.В., Водопьянов А.С., Mohammad H.H., Oscar Mogollon-Gutierrez, Andres Caro Lindo, Петровский А.

Результаты: Исследованы возможности использования цифровых двойников для повышения эффективности управления и обеспечения информационной безопасности.

ИБ КИИ

Авторы: Горбатов В.С., Гавдан А.Ю., Максимова Е.А., Паршенкова Ю.А., Калабишка М.М., Немченко А.А., Давыдов В.В., Лившиц И.И., Садыков А.М., Makrakis G.M., Maglaras L., Durojaye H.

Результаты: Предложены подходы и модели для обеспечения устойчивости и защиты критически важных инфраструктур в условиях угроз ИБ

Научная проблема

Разработка методологии анализа угроз ИБ объектов КИИ с использованием цифровых двойников для их моделирования, прогнозирования и адаптивного обнаружения.

Цель и задачи исследования

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

Критерии эффективности:

- (1) повышение точности прогнозирования угроз ИБ, характеризующейся показателями обнаружения признаков угроз ИБ;
- (2) снижение частоты ложноположительных срабатываний систем мониторинга;
- (3) сокращение времени реагирования на инциденты ИБ.

Задачи исследования:

- Разработать методологический подход к анализу угроз ИБ объектов КИИ как объектов цифрового моделирования, обеспечивающий формализацию системы через многосрезовую модель и структурированное представление угроз, их взаимодействий и форм проявления.
- Разработать комплекс моделей системы ИБ для объектов КИИ, обеспечивающий двунаправленную синхронизацию ЦД с физическим объектом и поддержку его роли как инструмента прогнозирования угроз ИБ.
- Разработать метод адаптивного выявления и анализа признаков угроз ИБ объектов КИИ на основе ЦД.
- Разработать метод и методики многокритериальной оценки угроз ИБ объектов КИИ на основе ЦД.
- Разработать архитектуру и программный прототип ЦД объекта КИИ

Объект и предмет диссертационного исследования

Объект исследования: объекты КИИ, подверженные угрозам ИБ.

Предмет исследования: подходы, методы, модели и методики анализа угроз ИБ объектов КИИ с применением ЦД

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

1. Методологический подход к анализу угроз ИБ объектов КИИ как объектов цифрового моделирования, обеспечивающий формализацию системы через многосрезовую модель и структурированное представление угроз, их взаимодействий и форм проявления
2. Комплекс моделей системы ИБ для объектов КИИ, обеспечивающий двунаправленную синхронизацию ЦД с физическим объектом и поддержку его роли как инструмента прогнозирования угроз ИБ.
3. Метод адаптивного обнаружения признаков угроз ИБ объектов КИИ на основе цифрового двойника.
4. Метод и комплекс методик многокритериальной оценки угроз ИБ объектов КИИ на основе ЦД.
5. Архитектура и программный прототип ЦД объекта КИИ

Формальная постановка задачи исследования

$$\max_{\Theta, A} \left[\sum_{k=1}^K \omega_k \Phi_k(A(X_{real}, \Theta)) \right] \quad (5.1)$$

Входные данные:

1. Телеметрия объекта КИИ

$$X_{real}(t) = \{x_1(t), x_2(t), \dots, x_D(t)\}, \quad X_{real}(t) \in R^{D \times T} \quad (5.2)$$

$x_i(t)$ — i -й параметр в момент времени t , D — число параметров, T — временной горизонт наблюдений.

2. Синтетические данные ЦД

$$D_{synth} = G(P_{phys}, P_{attack}, D_{feedback}) \quad (5.3)$$

где P_{phys} — физическая модель системы, P_{attack} — сценарии атак, $D_{feedback}$ — обратная связь, получаемая из реальных данных и работы алгоритмов.

Расшифровка обозначений

$\Theta = \{\theta_{alg}, \theta_{attack}, \theta_{metrics}\}$ — вектор параметров адаптации:

- θ_{alg} — гиперпараметры алгоритмов (например, число деревьев, размер окна, скорость обучения),
- θ_{attack} — параметры сценариев атак (тип, интенсивность, длительность),
- $\theta_{metrics} = \{\omega_k\}$ — веса критериев качества.

A — набор алгоритмов обнаружения угроз

ω_k — весовой коэффициент k -го критерия ($\sum \omega_k = 1$).

Φ_k — нормированная метрика качества ($K = 3$):

$$\Phi_1 = Recall(A) = \frac{TP}{TP+FN}, \quad \Phi_2 = 1 - FPR(A) = 1 - \frac{FP}{FP+TN}, \quad \Phi_3 = 1 - \frac{TTR(A)}{TTR_0}. \quad (5.4)$$

- $TTR(A)$ — среднее время реагирования на инцидент при использовании алгоритмов A .
- TTR_0 — базовое (референтное) время реагирования.
- $|D_{real}|, |D_{synth}|$ — объем реальных и синтетических данных.

Ограничения и допущения

Ограничения

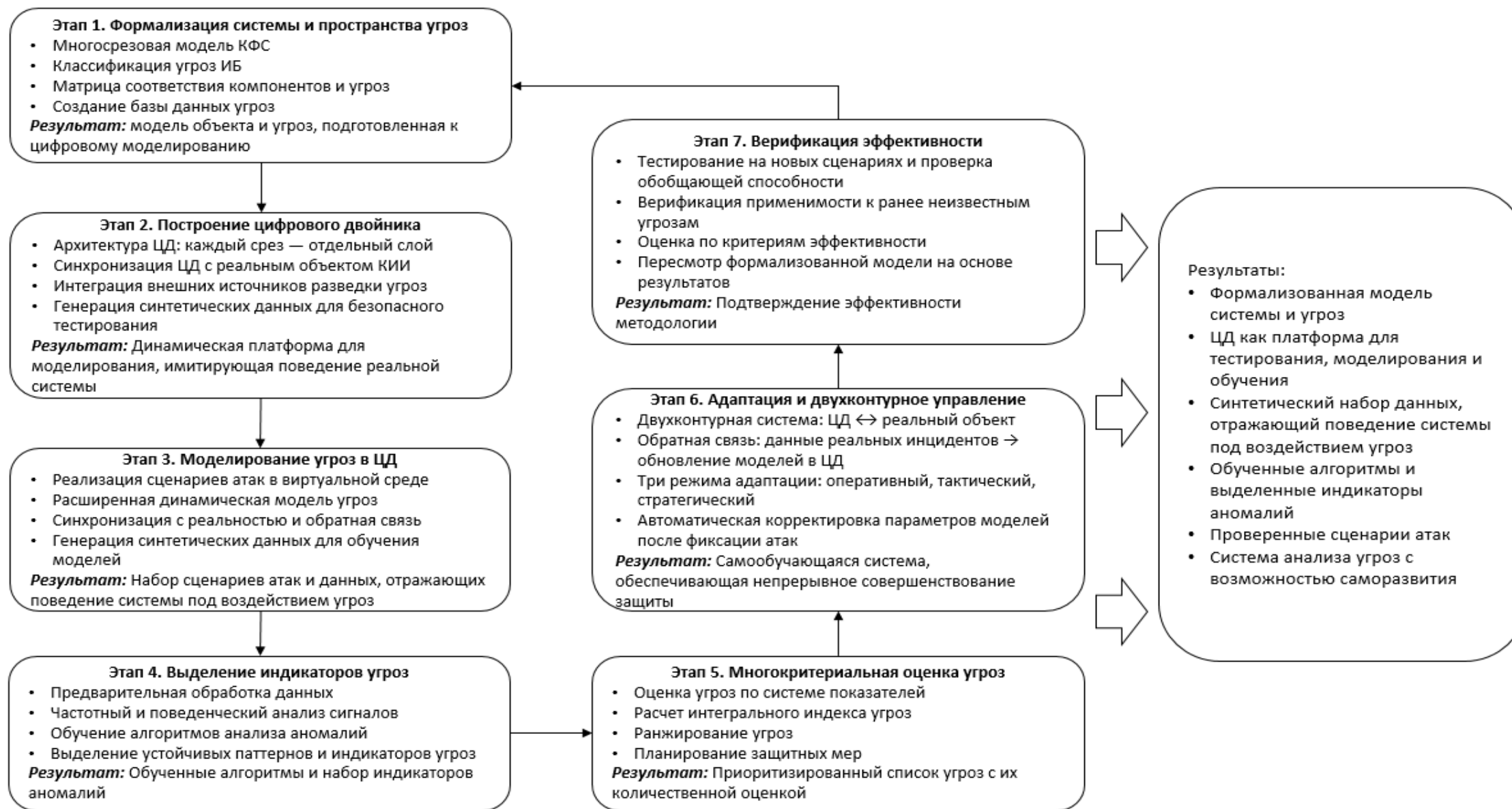
- Дефицит репрезентативных данных $|D_{real}| \ll |D_{synth}|$
- Высокая размерность данных ($D \gg 1$) требует устойчивых алгоритмов.
- Ограничения вычислительных ресурсов (например, времени адаптации).

Допущения

- Синтетические данные адекватно приближают реальные
- Метрики качества ($Recall, F1, FPR$ и т.д.) достаточны для активации механизма адаптации

1. Методологический подход к анализу угроз ИБ объектов КИИ

Концептуальная схема методологического подхода



1. Методологический подход к анализу угроз ИБ объектов КИИ

1. Формализация системы и пространства угроз

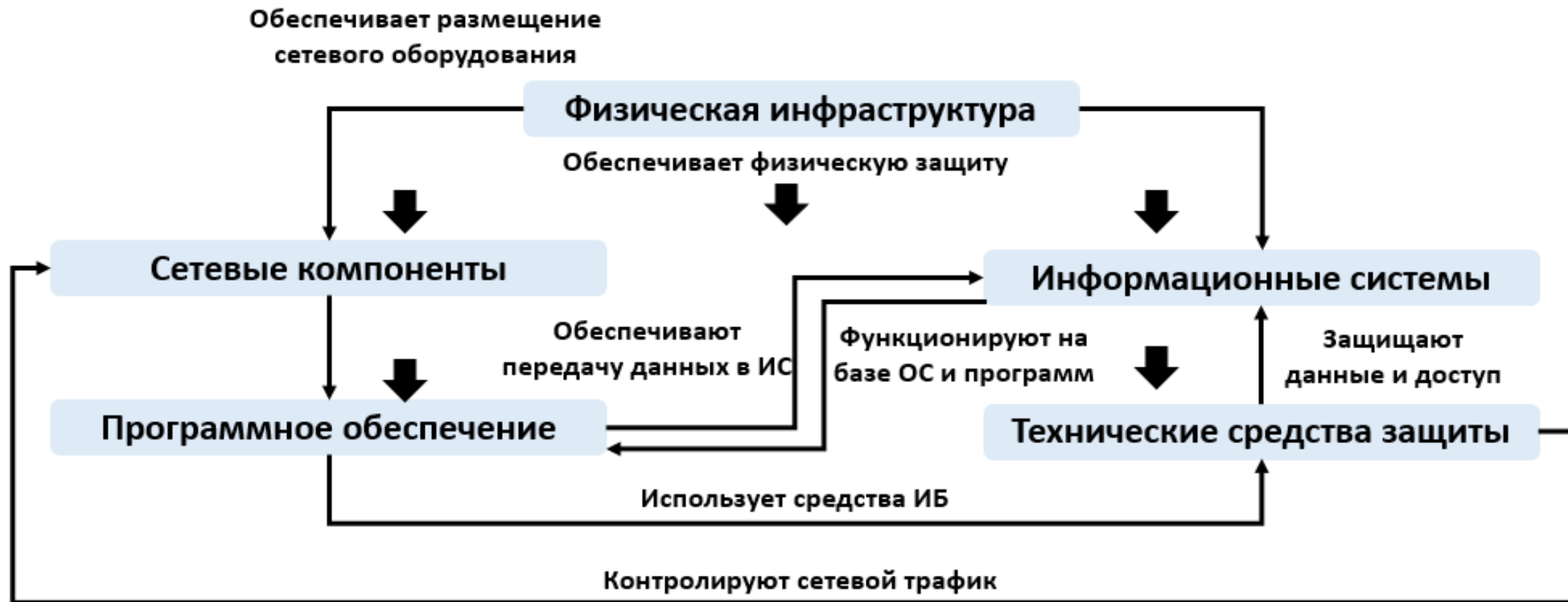
Матрица взаимовлияний декомпозиционных срезов объектов КИИ

Источники влияния Объект влияния	Технический срез	Процессный срез	Организационный срез	Функциональный срез	Отраслевой срез
Технический срез	—	Обеспечивает технические средства для реализации процедур мониторинга и реагирования на ИБ-инциденты	Ограничивает и задает технические условия для организационных мер безопасности	Поддерживает выполнение ключевых функций защиты и восстановления	Обеспечивает соответствие технических решений отраслевым стандартам защиты информации
Процессный срез	Требует надежной технической инфраструктуры для своевременного обнаружения и реагирования на угрозы	—	Зависит от организационного контроля и координации для обеспечения эффективности процессов	Опосредует выполнение функций защиты, мониторинга и восстановления	Включает процессы, адаптированные к специфике отраслевых угроз и нормативных требований
Организационный срез	Задаёт требования к техническим средствам и их эксплуатации с учетом рисков ИБ	Обеспечивает управление жизненным циклом ИБ-процессов и контроль исполнения мер защиты	—	Обеспечивает ресурсное и управленческое сопровождение функций безопасности	Внедряет отраслевые регуляции и стандарты ИБ в управленческие практики
Функциональный срез	Определяет технические требования для реализации функций защиты, мониторинга и восстановления	Определяет процессы, необходимые для выполнения функций ИБ и обеспечения их согласованности	Зависит от организационной поддержки для эффективного исполнения функций	—	Функциональные задачи адаптируются под отраслевые угрозы и требования безопасности
Отраслевой срез	Определяет специфические технические меры и стандарты защиты, применимые в конкретных секторах	Формирует отраслевые требования к процессам обеспечения безопасности и реагирования на угрозы	Влияет на организационные структуры и регулирующие требования, характерные для отрасли	Определяет приоритеты и специфику функциональных мер защиты в отрасли	—

1. Методологический подход к анализу угроз ИБ объектов КИИ

1. Формализация системы и пространства угроз

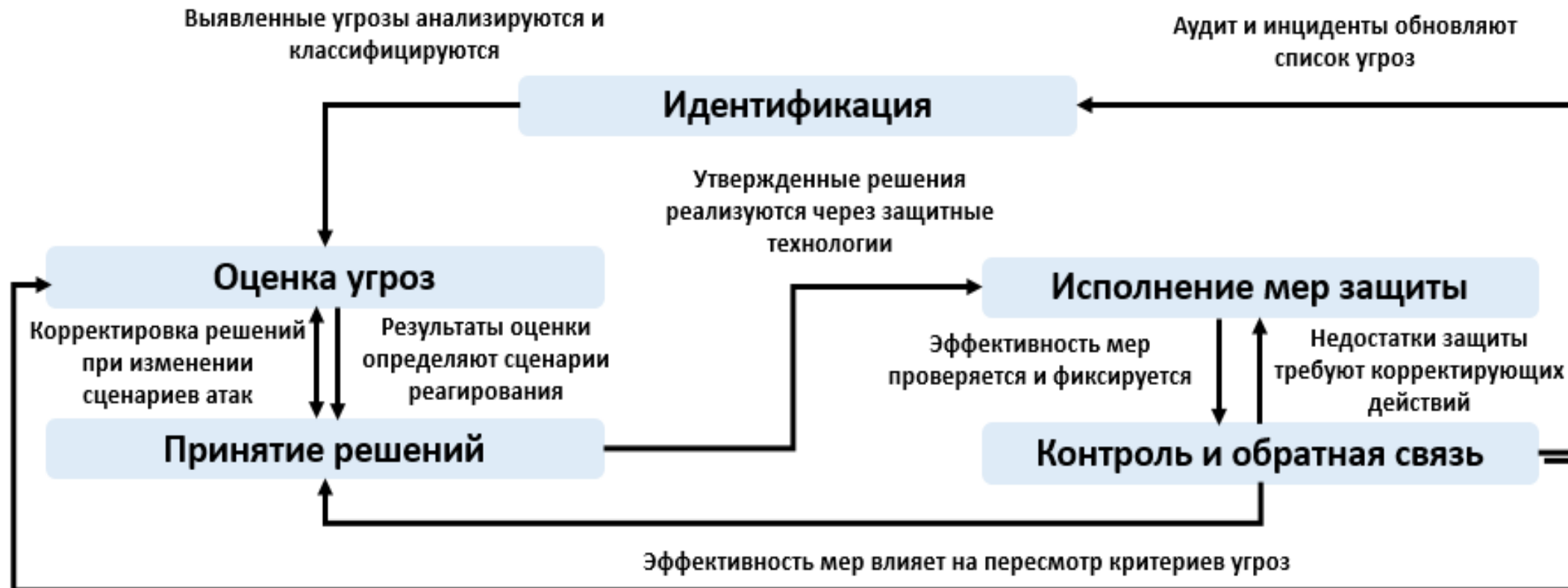
Взаимодействие в контексте технического среза



1. Методологический подход к анализу угроз ИБ объектов КИИ

1. Формализация системы и пространства угроз

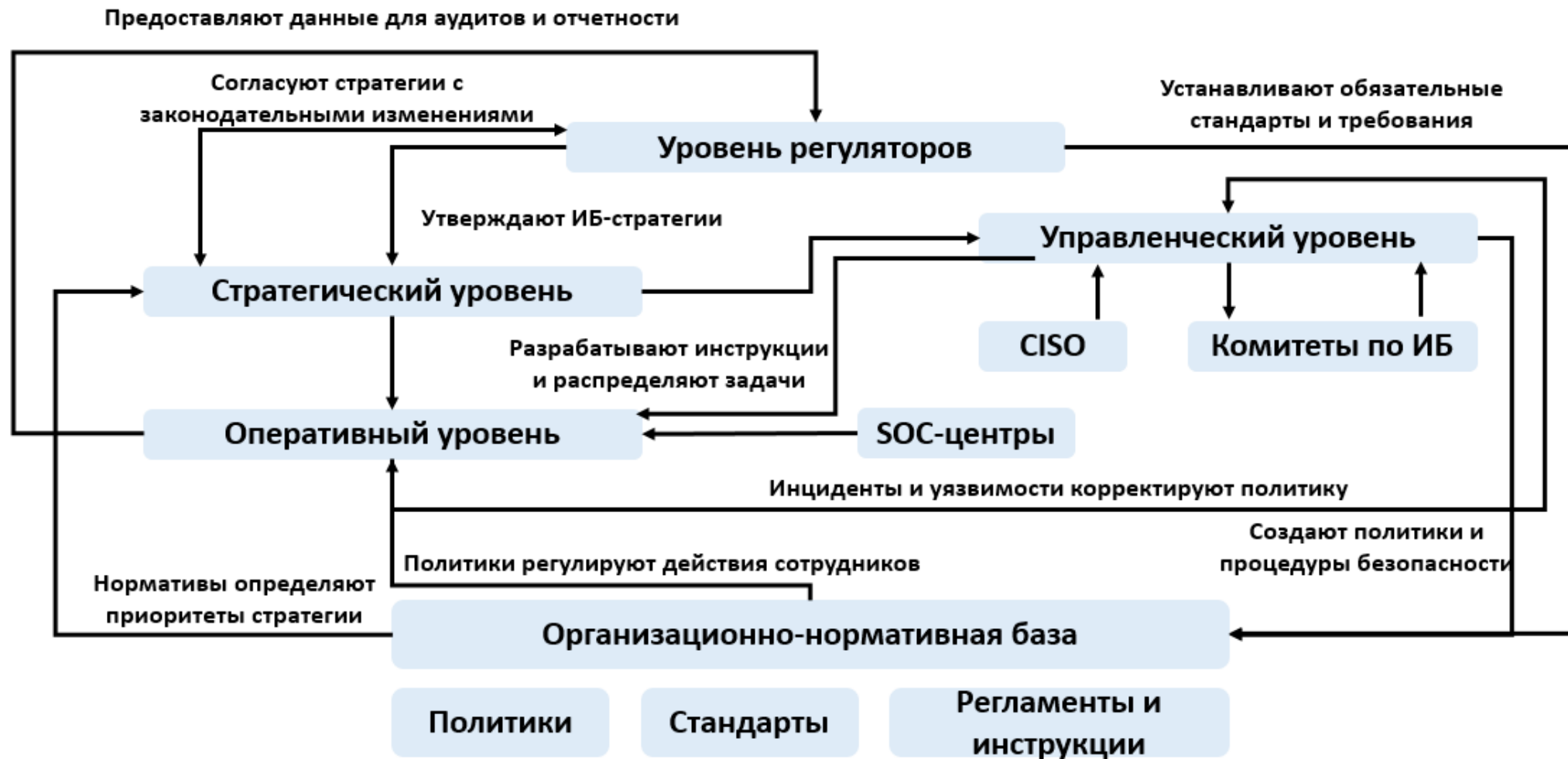
Взаимодействие в контексте процессного среза



1. Методологический подход к анализу угроз ИБ объектов КИИ

1. Формализация системы и пространства угроз

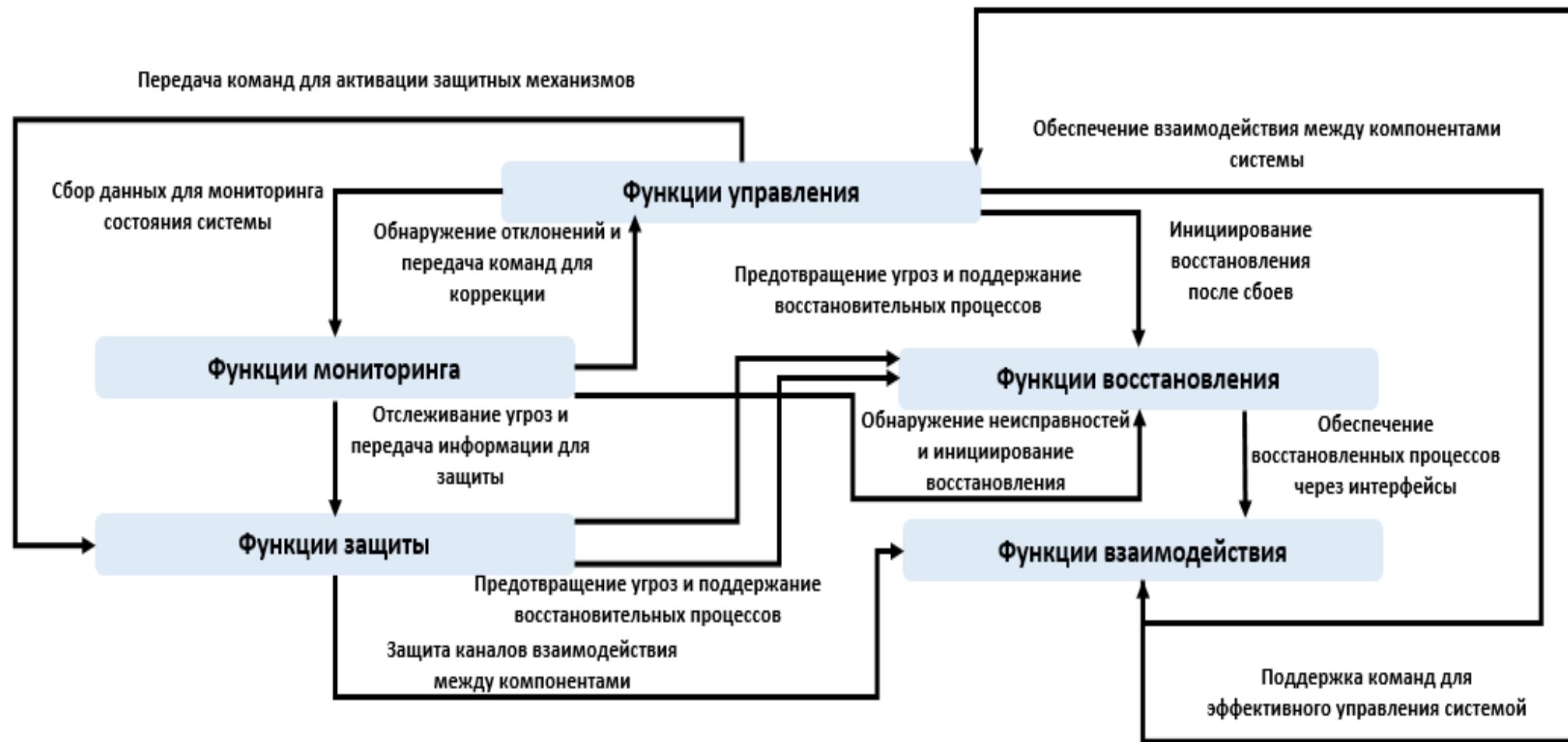
Взаимодействие в контексте организационного признака



1. Методологический подход к анализу угроз ИБ объектов КИИ

1. Формализация системы и пространства угроз

Взаимодействие в контексте функционального признака



1. Методологический подход к анализу угроз ИБ объектов КИИ

1. Формализация системы и пространства угроз

Взаимодействие в контексте отраслевого признака

Матрица усредненных экспертных оценок взаимного влияния угроз между отраслями критической информационной инфраструктуры

Источник \ Цель	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	5.00	1.15	0.95	1.20	1.05	0.85	0.30	0.95	0.25	0.10	0.15	0.10	0.05	0.10
2	1.10	5.00	2.10	2.35	1.85	1.00	1.25	2.10	1.05	0.95	1.40	0.95	0.85	0.75
3	1.25	2.20	5.00	3.40	3.10	1.30	2.05	3.15	1.15	1.00	0.85	1.00	0.90	0.85
4	2.15	3.35	4.25	5.00	4.15	2.30	4.10	4.00	2.25	1.85	1.25	1.15	1.10	1.05
5	1.15	1.05	2.05	2.10	5.00	1.95	3.00	4.10	3.05	3.00	2.10	2.95	2.20	2.10
6	0.85	0.90	0.90	1.10	1.00	5.00	2.05	1.20	0.35	0.15	0.20	0.10	0.05	0.10
7	0.25	1.10	1.10	3.05	3.25	2.05	5.00	3.05	1.00	1.10	1.05	0.10	0.10	0.15
8	1.10	1.10	3.25	3.20	4.10	2.10	3.05	5.00	3.05	3.20	2.05	3.10	2.75	2.75
9	0.25	1.05	1.10	1.20	2.85	0.45	0.50	3.10	5.00	3.80	2.75	2.05	2.10	2.00
10	0.15	0.65	0.85	1.15	2.50	0.25	0.95	3.10	3.85	5.00	3.40	2.10	2.00	2.10
11	0.20	1.75	0.90	1.20	2.10	0.15	0.75	2.10	2.45	3.30	5.00	1.90	2.00	1.95
12	0.75	0.95	0.90	0.85	3.15	0.20	0.10	3.10	2.15	2.00	2.10	5.00	3.75	3.75
13	0.80	1.00	0.90	1.00	2.85	0.15	0.15	2.80	2.10	2.00	2.05	3.65	5.00	3.80
14	0.85	0.95	0.85	1.05	2.75	0.20	0.15	2.85	2.05	2.00	1.95	3.70	3.85	5.00

Нумерация отраслей:

1. Здравоохранение
2. Наука
3. Транспорт
4. Связь
5. Энергетика
6. Государственная регистрация недвижимости
7. Банковская и финансовая сфера
8. Топливо-энергетический комплекс (ТЭК)
9. Атомная энергетика
10. Оборонная промышленность
11. Ракетно-космическая промышленность
12. Горнодобывающая промышленность
13. Металлургическая промышленность
14. Химическая промышленность

Уровень влияния от 0 до 5:

- 0 — не влияет
- 1 — слабое влияние
- 2 — умеренное влияние
- 3 — значительное влияние
- 4 — сильное влияние
- 5 — критическое влияние

Проверка согласованности экспертных оценок

1. Стандартное отклонение по парам отраслей

1. Рассчитывалось для 182 пар ($n = 20$ экспертов)
2. Большинство $SD < 0.3 \rightarrow$ хорошая согласованность

2. Внутриклассовый коэффициент корреляции (ICC(2,n))

1. Оценка абсолютной согласованности между 20 экспертами
2. $ICC = 0.87 \rightarrow$ высокая согласованность

1. Методологический подход к анализу угроз ИБ объектов КИИ

1. Формализация системы и пространства угроз

Формализация модели декомпозиции объекта КИИ

$C = \{c_1, c_2, \dots, c_n\}$ – (13.1) пространство декомпозиции.

$p(c_i) = (p_i^{(T)}, p_i^{(P)}, p_i^{(O)}, p_i^{(F)}, p_i^{(I)})$ – (13.2) признаки компонента c_i :

T – технический, P – процессный, O – организационный, F – функциональный, I – отраслевой.

$M_i = (M_{i,T}, M_{i,P}, M_{i,O}, M_{i,F}, M_{i,I})$ – (13.3) вектор влияния признаков на угрозу
 $M_{i,k}$ – степень влияния признака k на угрозу.

$T_i = \sum_{k \in \{T,P,O,F,I\}} w_k \cdot M_{i,k} \cdot \varphi_k(p_i^{(k)})$, – (13.4) угроза компонента

w_k – вес признака, $\varphi_k(\cdot)$ – числовая функция признака.

$T = \sum_{i=1}^n \alpha_i \cdot T_i$, – (13.5) суммарная угроза, α_i – вес компонента.

$T_i(x_i) = T_i \cdot (1 - \beta_i x_i + \delta_i^2 x_i^2)$, $x_i \in \{0,1\}$ – (13.6) модель защитного воздействия на угрозу; x_i – мера применена (1) или нет (0); β_i – коэффициент эффективности защиты, δ_i – параметр нелинейного эффекта.

Задача оптимизации:

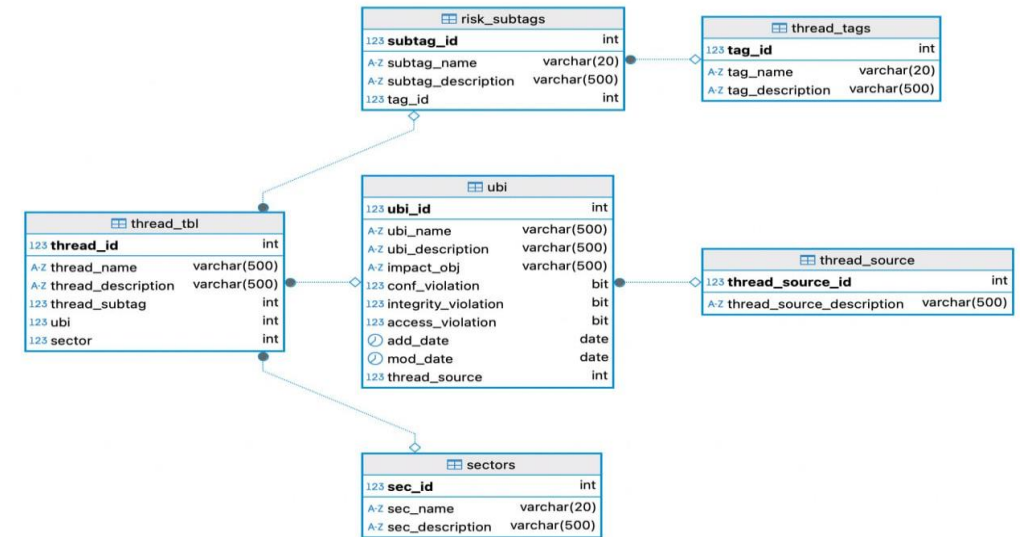
$\min_x \sum_{i=1}^n T_i(x_i) + \gamma \sum_{i=1}^n \text{cost}_i \cdot x_i$, (13.7)

при ограничениях

$\sum_{i=1}^n \text{cost}_i \cdot x_i \leq B$, (13.8)

cost_i – стоимость защиты, B – бюджет, γ – коэффициент, отражающий баланс риска и затрат

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 (срезов) угроз
threat_subtags	Справочник подсрезов угроз

1. Методологический подход к анализу угроз ИБ объектов КИИ

2. Многослойная архитектура ЦД

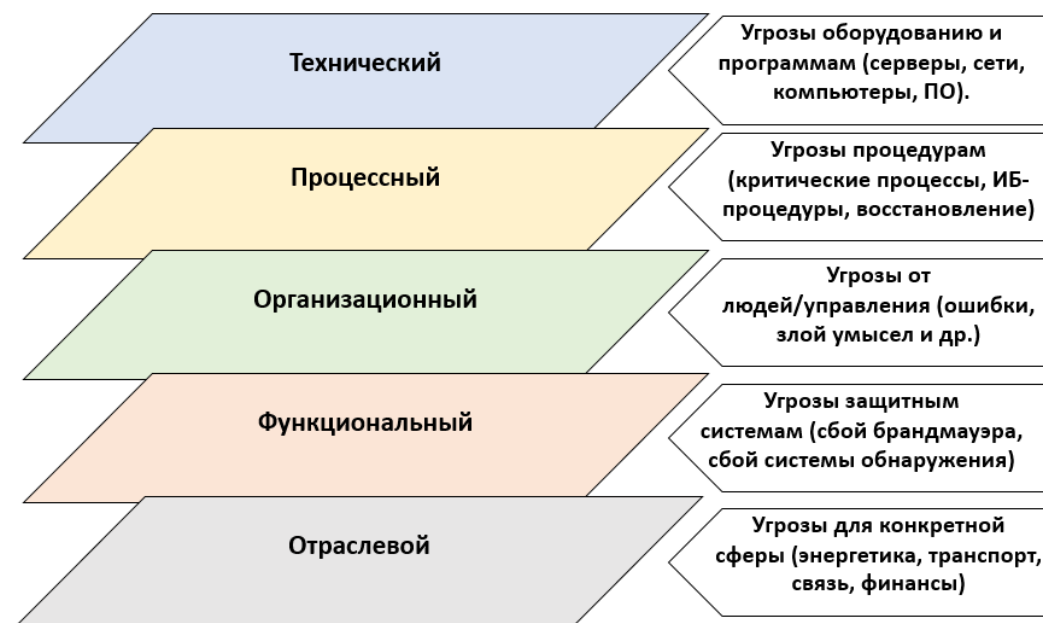
Архитектура цифрового двойника объекта КИИ

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).

Верификация методологического подхода

1. Генерация данных в ЦД для обучения
2. Предобработка и фильтрация данных
3. Обучение алгоритмов
4. Генерация новых реализаций угроз и аварийных ситуаций
5. Тестирование

Модель цифрового двойника



1. Методологический подход к анализу угроз ИБ объектов КИИ

3. Моделирование угроз в ЦД



Интеграция ЦД в процесс моделирования угроз обеспечивает:

- Повышение точности анализа за счет учета реальных данных о состоянии объекта.
- Оперативность принятия решений благодаря симуляции сценариев в режиме, близком к реальному времени.

1. Методологический подход к анализу угроз ИБ объектов КИИ

3. Моделирование угроз в ЦД

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.

Базовая модель

$$T = S \otimes V \otimes O \rightarrow (I \rightarrow C), \quad (16.1)$$

S — источник угрозы,

V — уязвимость,

O — объект воздействия,

I — способ реализации угрозы,

C — последствия.

$\otimes$ — оператор синергетического взаимодействия

$\rightarrow$ — оператор импликации

Расширенная модель

$$T_{\text{ext}} = (S \otimes V \otimes O \otimes K \otimes D) \rightarrow (I \otimes C \otimes DT), \quad (16.2)$$

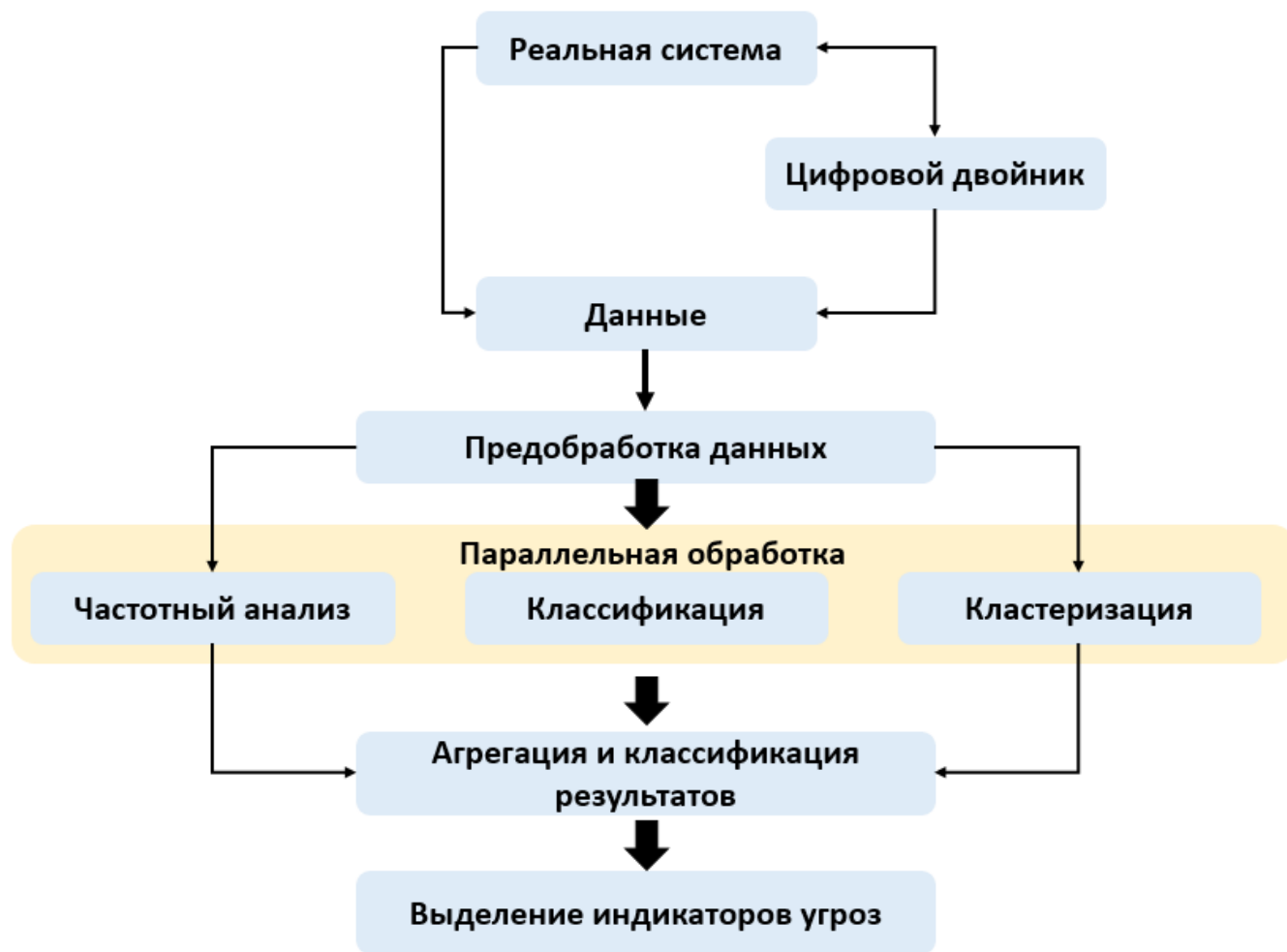
K — контекст системы, D — динамические факторы, DT — цифровой двойник системы, включающий четыре компонента:

$$DT = \text{Sim}(A) \otimes \text{Pred}(C) \otimes \text{Resp}(M) \otimes \text{Test}(R), \quad (16.3)$$

где $\text{Sim}(A)$ — функция моделирования атак, A — множество сценариев атак; $\text{Pred}(C)$ — функция прогнозирования последствий, C — множество возможных последствий; $\text{Resp}(M)$ — функция автоматизированного ответа, M — множество мер противодействия; $\text{Test}(R)$ — функция оценки устойчивости, R — множество метрик устойчивости.

1. Методологический подход к анализу угроз ИБ объектов КИИ

4. Выделение индикаторов угроз



5. Многокритериальная оценка угроз

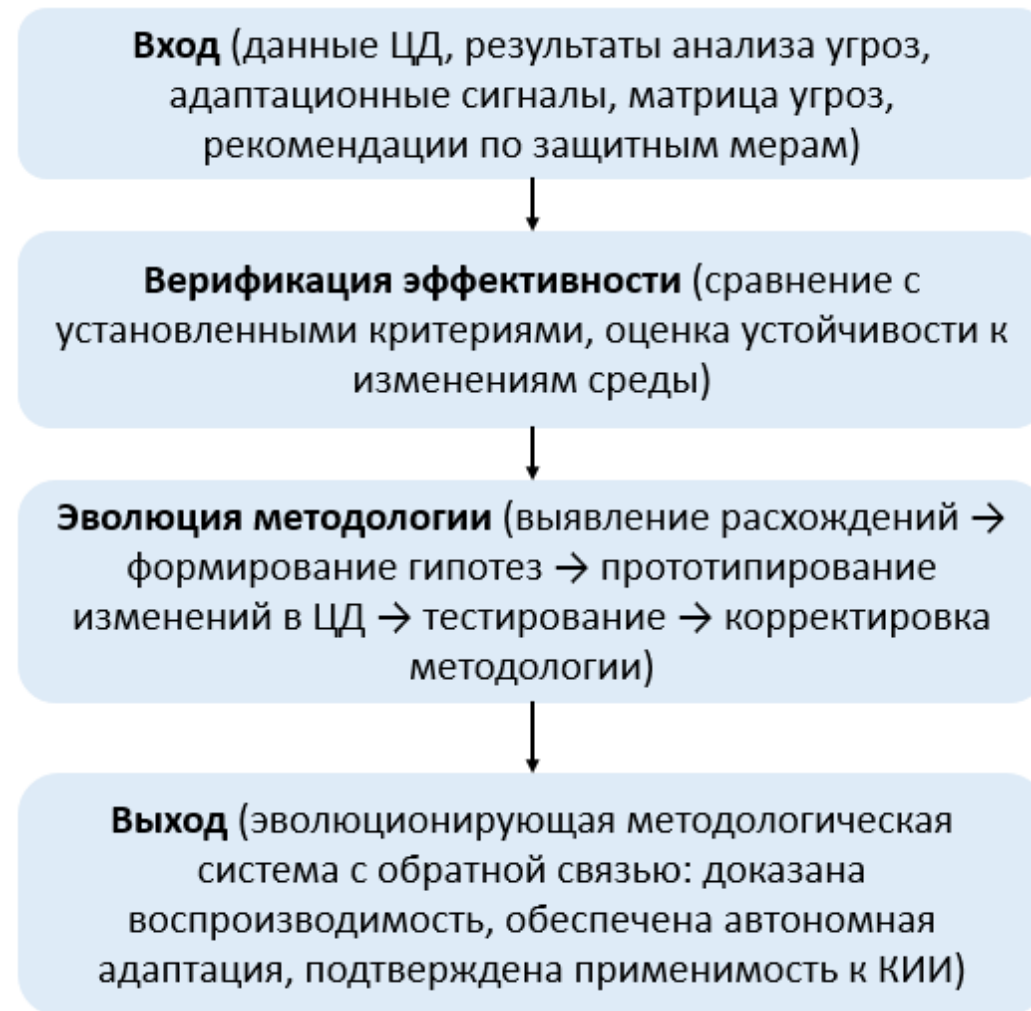


1. Методологический подход к анализу угроз ИБ объектов КИИ

6. Адаптация и двухконтурное управление



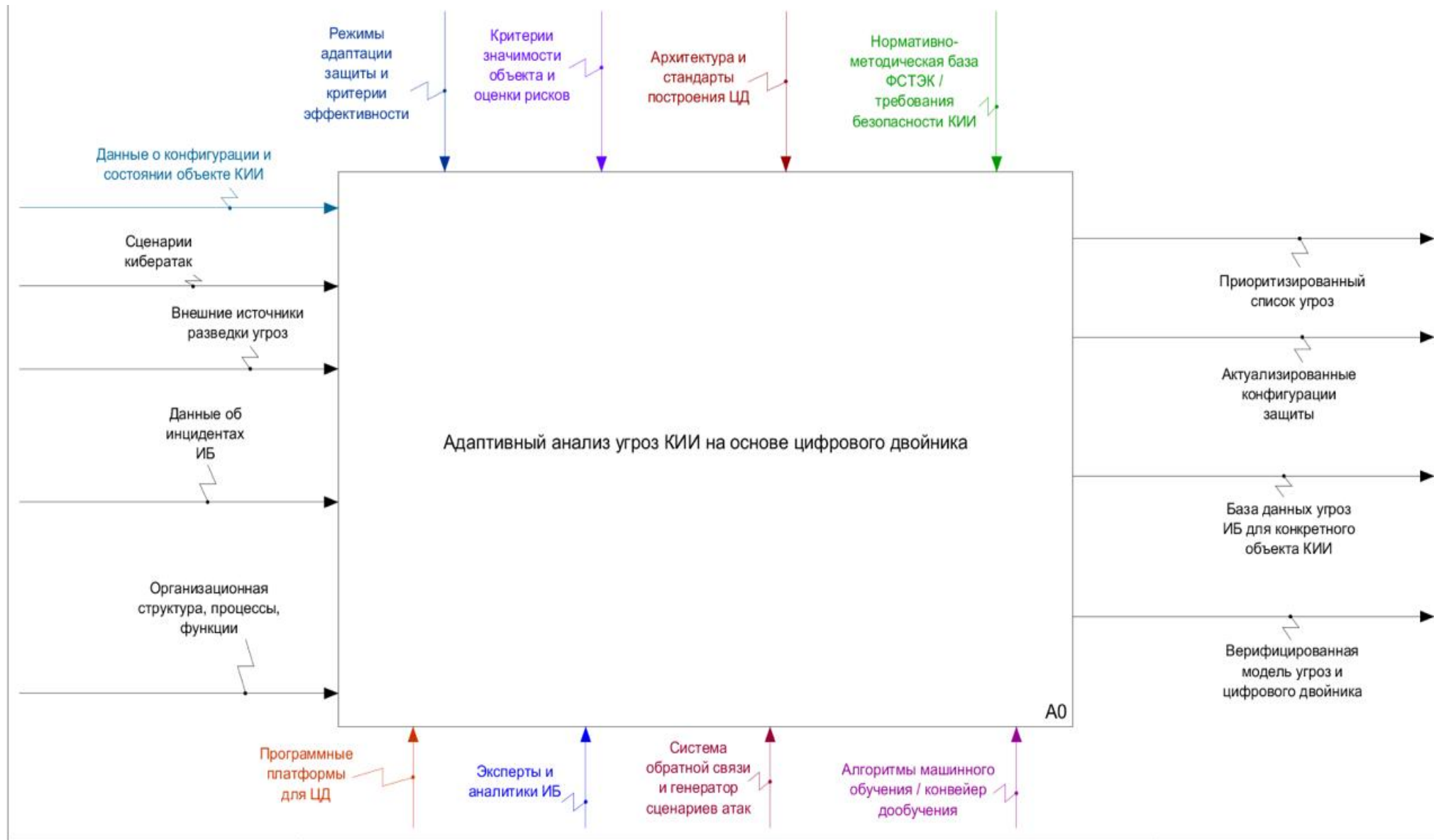
7. Верификация эффективности и эволюция методологии



1. Методологический подход к анализу угроз ИБ объектов КИИ

Функциональная модель анализа угроз ИБ объектов КИИ на основе ЦД

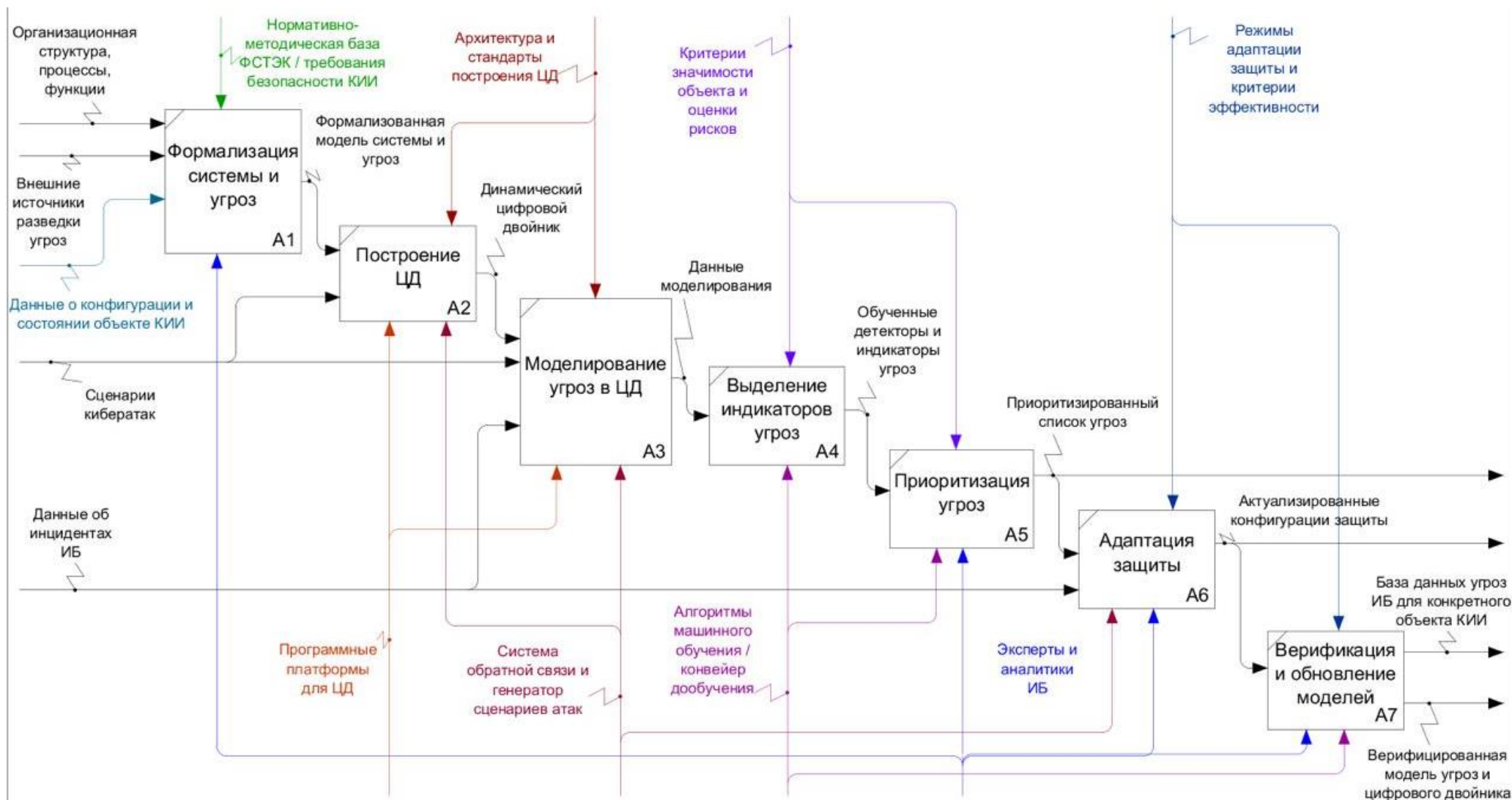
Контекстная диаграмма (уровень A-0)



1. Методологический подход к анализу угроз ИБ объектов КИИ

Функциональная модель анализа угроз ИБ объектов КИИ на основе ЦД

Декомпозиция процесса анализа угроз на уровне A0



1. Методологический подход к анализу угроз ИБ объектов КИИ

Суть. Разработан методологический подход к анализу угроз информационной безопасности объектов критически важной информационной инфраструктуры на основе цифрового двойника и многосрезового описания системы.

Научная новизна. Предложен новый методологический подход к анализу угроз ИБ объектов КИИ, реализуемый в виде семи последовательных этапов: формализация системы и пространства угроз; построение архитектуры цифрового двойника; моделирование угроз в ЦД; выделение индикаторов угроз; многокритериальная оценка угроз; адаптация и динамическое управление защитой; верификация эффективности контрмер. Подход отличается интеграцией цифрового двойника на всех этапах, реализацией самообучающейся системы защиты и использованием виртуальной среды для безопасного тестирования.

Теоретическая значимость. Расширена теория анализа угроз ИБ за счёт формализации многосрезовой модели и внедрения цифрового двойника как единой платформы для динамического моделирования угроз, выявления индикаторов угроз и оценки их проявлений.

Практическая значимость. Методологический подход применим при создании баз данных угроз, разработке имитационных моделей, проектировании адаптивных систем защиты и регламентов управления ИБ объектов КИИ. Он позволяет автоматизировать прогнозирование, отработку сценариев атак и тестирование контрмер в безопасной виртуальной среде.

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 17 работ (Scopus: 6, ВАК: 4, Программы ЭВМ (БД): 1, Иные публикации: 6)

2. Комплекс моделей системы ИБ для объектов КИИ

Онтологическая модель анализа угроз ИБ объектам 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 системы ИБ для объектов КИИ

Архитектурная модель обеспечения ИБ объектов КИИ на основе ЦД

- *Модель А.* Архитектура без цифрового моделирования.
- *Модель В.* Киберполигон (без ЦД).
- *Модель С.* ЦД (без киберполигона).
- *Модель D.* ЦД со встроенным симулятором киберполигона.
- *Модель Е.* Использование ЦД и изолированного киберполигона.

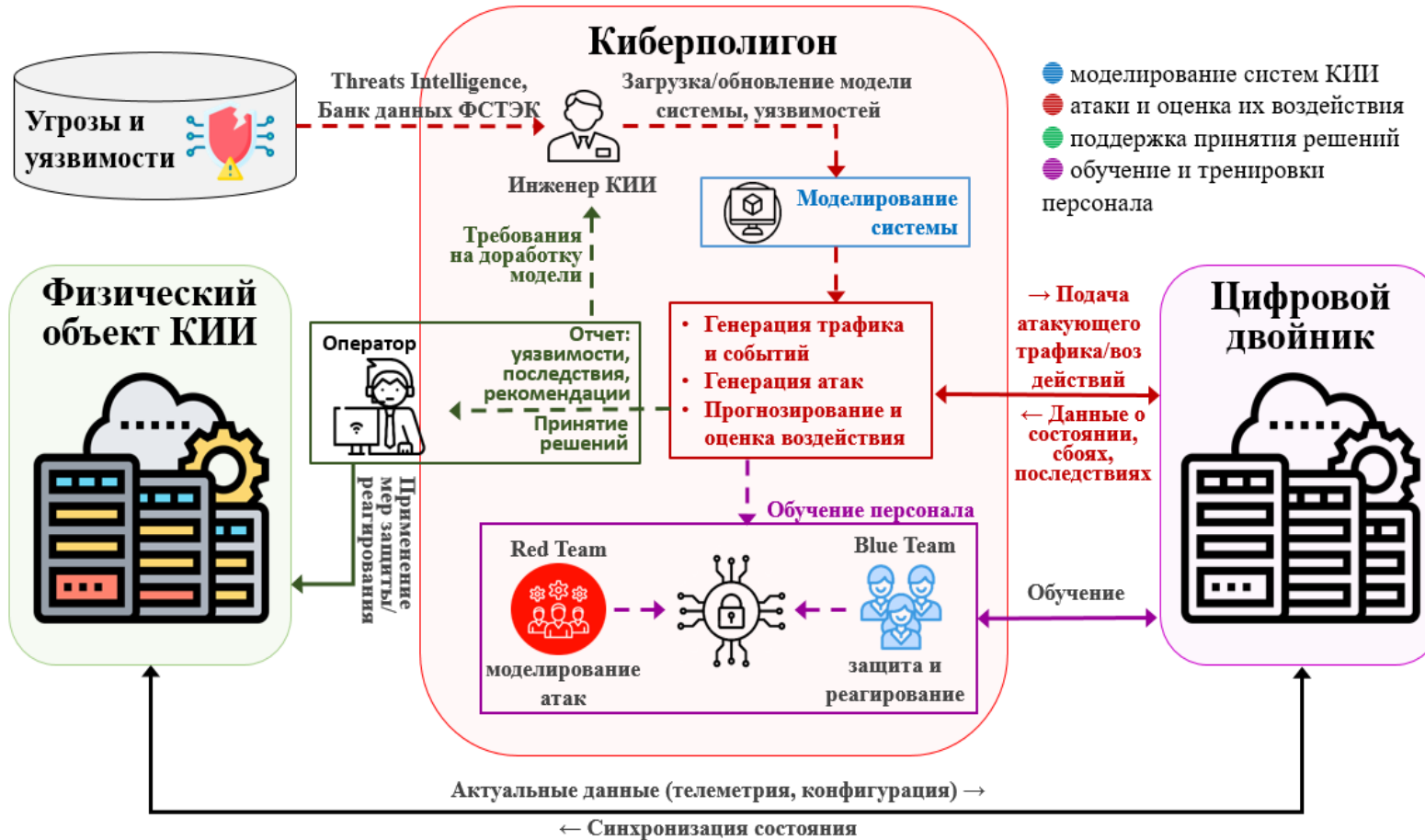
Сравнительная таблица оценки архитектурных моделей

Критерий	Модель А	Модель В	Модель С	Модель D	Модель Е
Безопасность тестирования	—	+	±	±	+
Реализм моделирования	—	+	±	+	+
Проактивность	—	±	±	±	+
Ситуационная осведомлённость	—	—	+	+	+
Гибкость и масштабируемость	—	±	±	±	+
Поддержка подготовки персонала	—	+	+	+	+
Архитектурная изоляция	—	+	±	±	+

2. Комплекс моделей системы ИБ для объектов КИИ

Архитектурная модель обеспечения ИБ объектов КИИ на основе ЦД

Схема модели



Количественные показатели результата эксперимента

Показатель	Значение	Комментарий
Количество реализованных сценариев атак	12	Включая MITM, DoS и внедрение ложных команд
Успешных атак, повлиявших на ЦД	9 (75%)	Вызвали сбои и нарушения управления
Среднее время реакции Blue Team	3,2 минуты	Время от обнаружения до начала реагирования
Эффективность нейтрализации атак	88%	Доля атак, нейтрализованных без серьёзных последствий
Количество выявленных новых уязвимостей	6 (2 критические)	Обнаружены в ходе анализа после атак

2. Комплекс моделей системы ИБ для объектов КИИ

Концептуальная модель двустороннего взаимодействия ЦД в системе ИБ

Схема концептуальной модели

Единая модульная архитектура, обеспечивающая замкнутый информационно-технологический цикл ИБ



Формализация модели

$$\left\{ \begin{array}{l} D(t) = \Phi(S(t)) + \epsilon(t) \\ P(T_i|D(t)) = f_{ML}(D(t), H) \\ A(t) = \Gamma(D(t), T) \\ \Delta(t) = \Psi(D(t), M(t)) \\ R(t) = \Lambda(\Delta(t)) \\ M(t) = \Theta(D(t)) \\ Input_B(t) = A(t) \\ D(t+1) = D(t) + \Sigma(t) \end{array} \right. \quad (25.1)$$

$D(t)$ — 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 В из подсистемы А

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

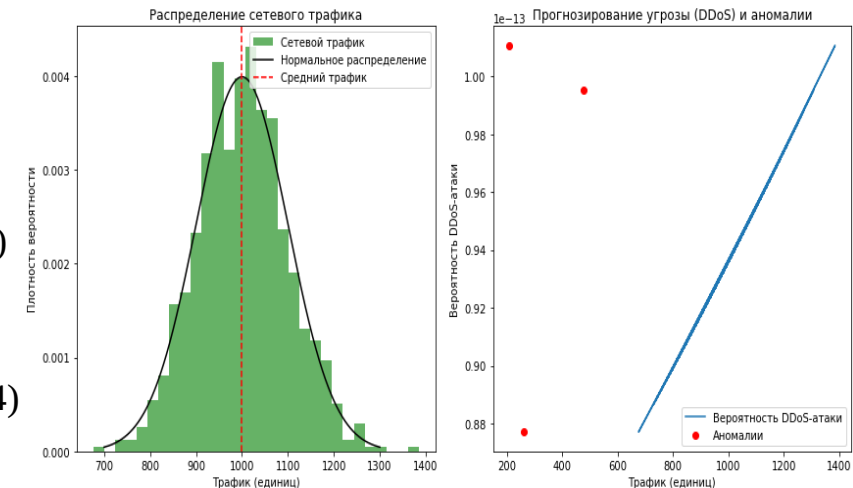
Пример моделирования

$$D(t) = x_t, x_t \sim N(\mu, \sigma^2), t \in \{1, 2, \dots, 1000\} \quad (25.2)$$

$$P(T_{DDoS} | D(t)) = \frac{1}{1 + e^{-(\alpha \cdot x_{\text{норм}} + \beta)}} \quad (25.3)$$

$$x_{\text{норм}} = \frac{(x - \mu)}{\sigma}$$

$$Anomaly(t) = \begin{cases} 1, & \text{если } |D(t) - \mu| > 3\sigma \\ 0, & \text{иначе} \end{cases} \quad (25.4)$$



2. Комплекс моделей системы ИБ для объектов КИИ

Суть: Предложен комплекс взаимосвязанных моделей, обеспечивающий синхронизацию ЦД с физическим объектом КИИ и поддержку его роли как инструмента прогнозирования в замкнутом цикле оценки, моделирования и реагирования угроз ИБ.

Научная новизна: Впервые предложен комплекс взаимосвязанных моделей системы ИБ объектов КИИ, основанный на интеграции ЦД в процессы анализа, прогнозирования и реагирования на угрозы ИБ. Модели включают онтологическое представление угроз ИБ, архитектуру взаимодействия ЦД с киберполигоном и физической инфраструктурой, а также концептуальную схему двусторонней синхронизации ЦД с физическим объектом защиты. Предложенный комплекс *отличается* включением ЦД в замкнутый контур ИБ как предиктивного элемента и объекта защиты, что *позволяет* реализовать непрерывную адаптацию защитных механизмов в реальном времени с учетом изменяющихся условий функционирования объекта.

Теоретическая значимость: Расширена теория ИБ объектов КИИ за счет интеграции онтологической модели угроз, архитектурного взаимодействия ЦД с киберполигоном и концепции двусторонней синхронизации цифрового и физического уровней в рамках динамической модели защиты.

Практическая значимость: Полученные результаты применимы при разработке комплексных решений для защиты КИИ, автоматизации анализа и прогнозирования киберугроз, а также при тестировании и адаптивном управлении защитными мероприятиями в реальных условиях эксплуатации.

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 12 работ (Scopus: 2, ВАК: 5, Иные публикации: 5)

3. Метод обнаружения признаков угроз ИБ на основе ЦД

Схема метода



3. Метод обнаружения индикаторов угроз ИБ на основе ЦД

Адаптационный механизм

Условия активации:

Адаптация запускается, если хотя бы одна метрика M_i выходит за допустимый диапазон $[T_i^{min}, T_i^{max}]$:

$$\bigvee_i (M_i \notin [T_i^{min}, T_i^{max}]). \quad (28.1)$$

В частности, в случае метрик:

- F1 — F1-мера,
- FPR — частота ложноположительных срабатываний,
- Recall — полнота классификации,
- Precision — точность классификации.

$$(F_1 < F_1^{min}) \vee (FPR > FPR_{max}) \vee (Recall < Recall_{min}) \vee (Precision < Precision_{min}) \quad (28.2)$$

Режимы адаптации:

Оперативный:

Дообучение модели без изменения архитектуры:

$$\theta' = \arg \min_{\theta} L(\theta; D_{train} \cup D_{new}) \quad (28.3)$$

где L — функция потерь, D_{train} — обучающая выборка, D_{new} — новые данные

Тактический:

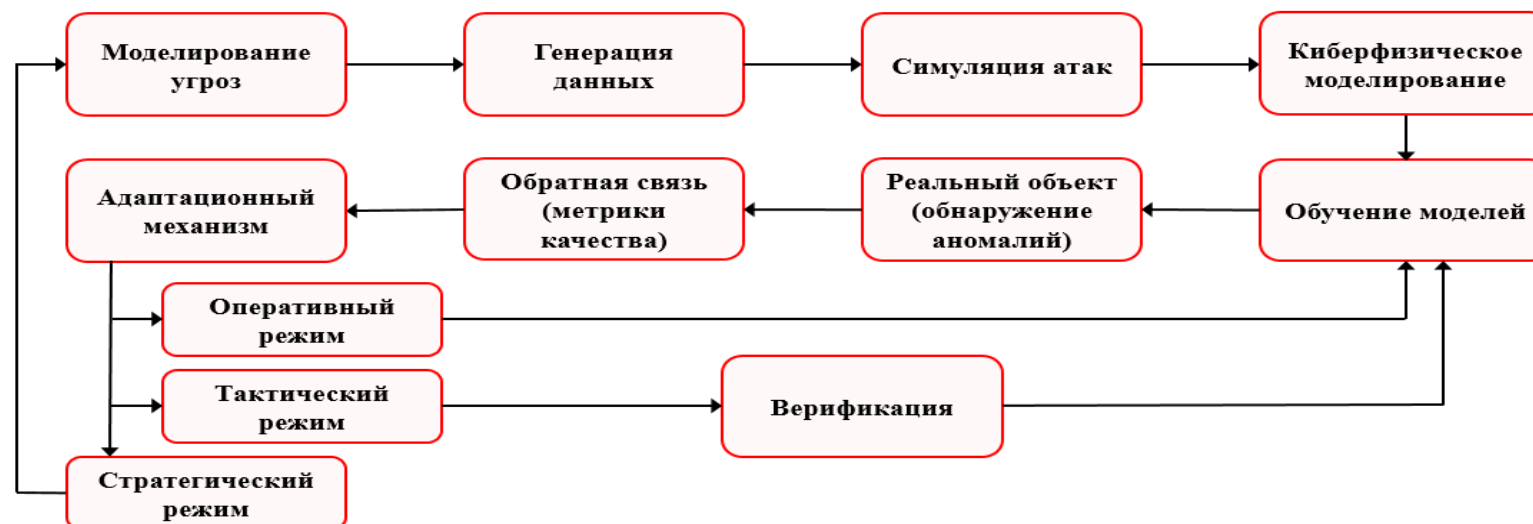
Пересмотр архитектуры и гиперпараметров:

$$\theta', h' = \arg \min_h L(\theta, h; D_{train} \cup D_{new}) \quad (28.4)$$

где h — гиперпараметры модели (архитектура, пороги и др.).

Стратегический:

Возврат к моделированию сценариев и формированию новой обучающей выборки с последующим переобучением моделей



Замкнутый цикл адаптации

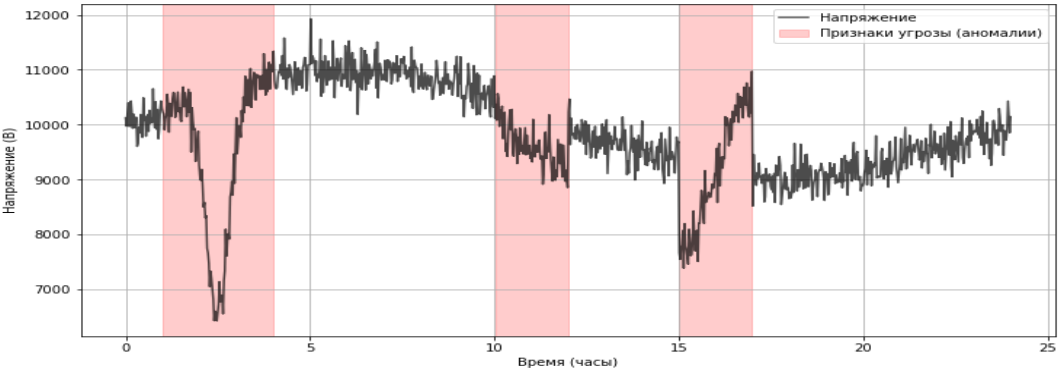
3. Метод обнаружения индикаторов угроз ИБ на основе ЦД

Адаптационный механизм

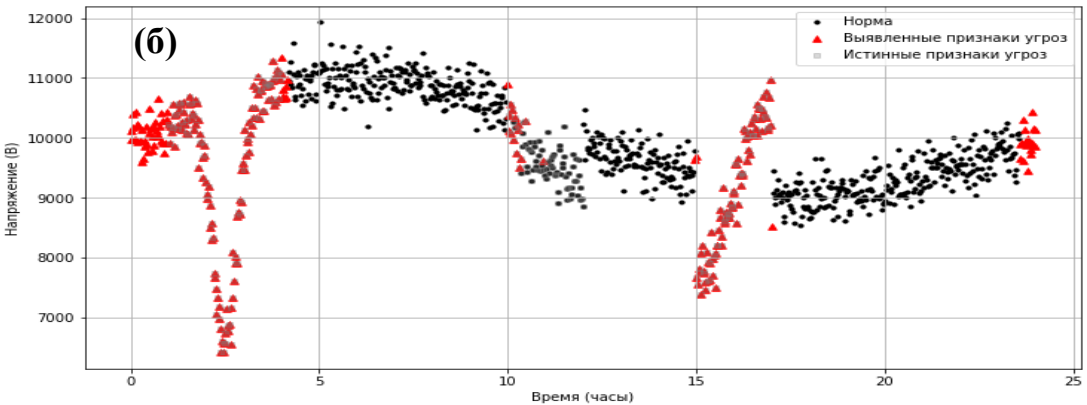
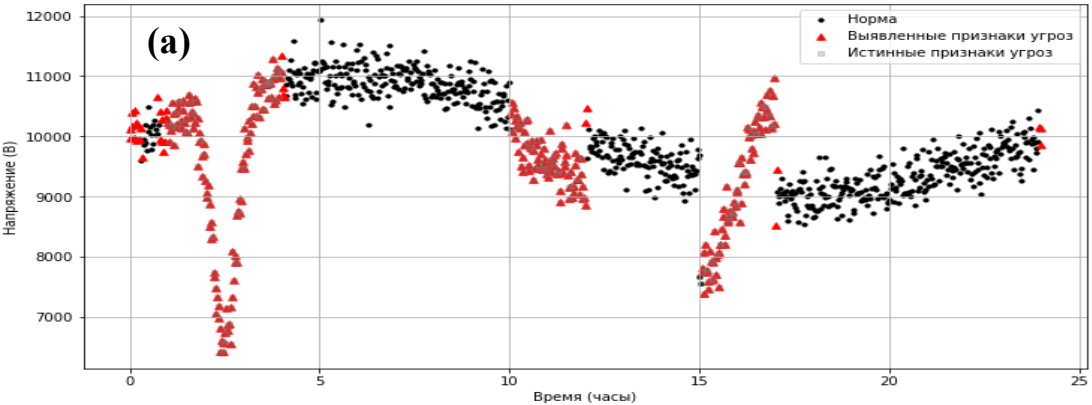
Три класса режимов:

- Нормальная работа – синусоидальный сигнал с частотой 50 Гц, суточной модуляцией амплитуды ($\pm 10\%$) и гауссовым шумом ($\sigma = 5\%$);
- Аварийные состояния – плавные изменения частоты (45–55 Гц) и амплитуды (до $\pm 25\%$);
- Потенциально деструктивные воздействия (признаки угроз) – импульсные искажения (до -40%), фазовые сдвиги ($0.1-0.4\pi$) и низкочастотные модуляции.

Пример временного ряда с аннотированными аномалиями



Обнаружение признаков угроз ИБ с использованием алгоритма Isolation Forest (а - до адаптации; б – после адаптации)

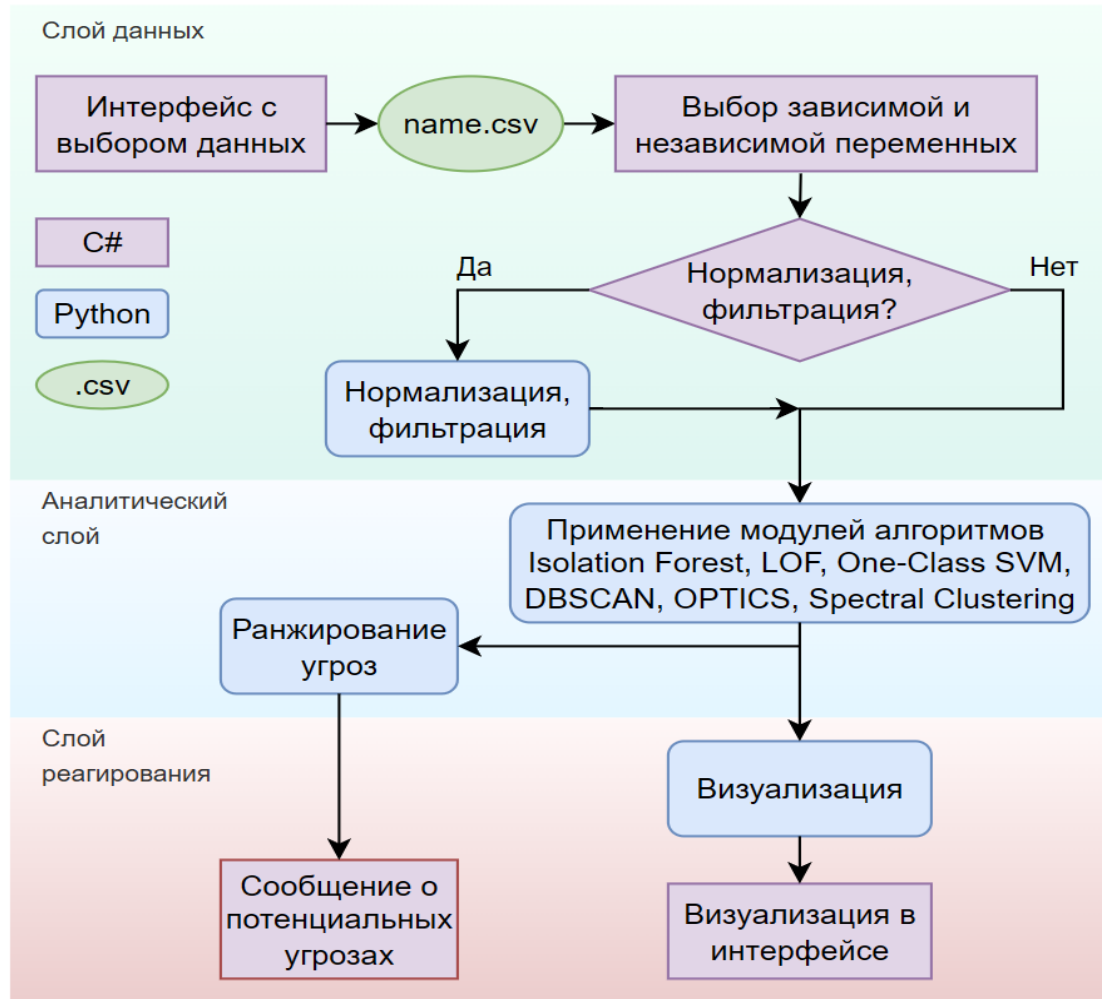


Сравнительные характеристики модели до и после адаптации

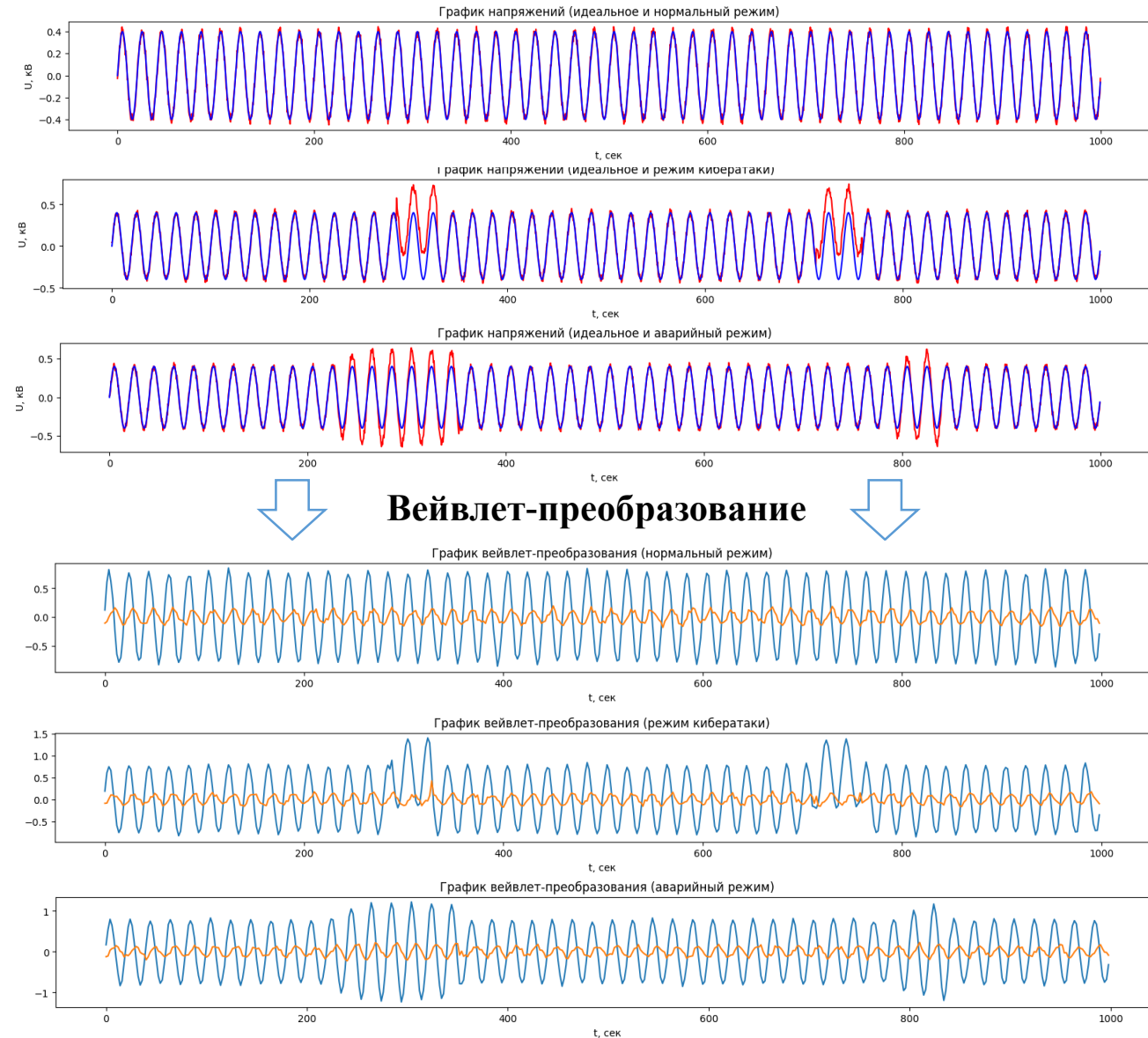
Показатель	До адаптации	После адаптации	Изменение
F1-score	0.76	0.94	+23.7%
FPR (%)	10.01%	4.94%	-50.6%
Recall	0.76	0.99	+30.3%
Precision	0.76	0.89	+17.1%

3. Метод обнаружения индикаторов угроз ИБ на основе ЦД

Архитектура системы обнаружения индикаторов угроз

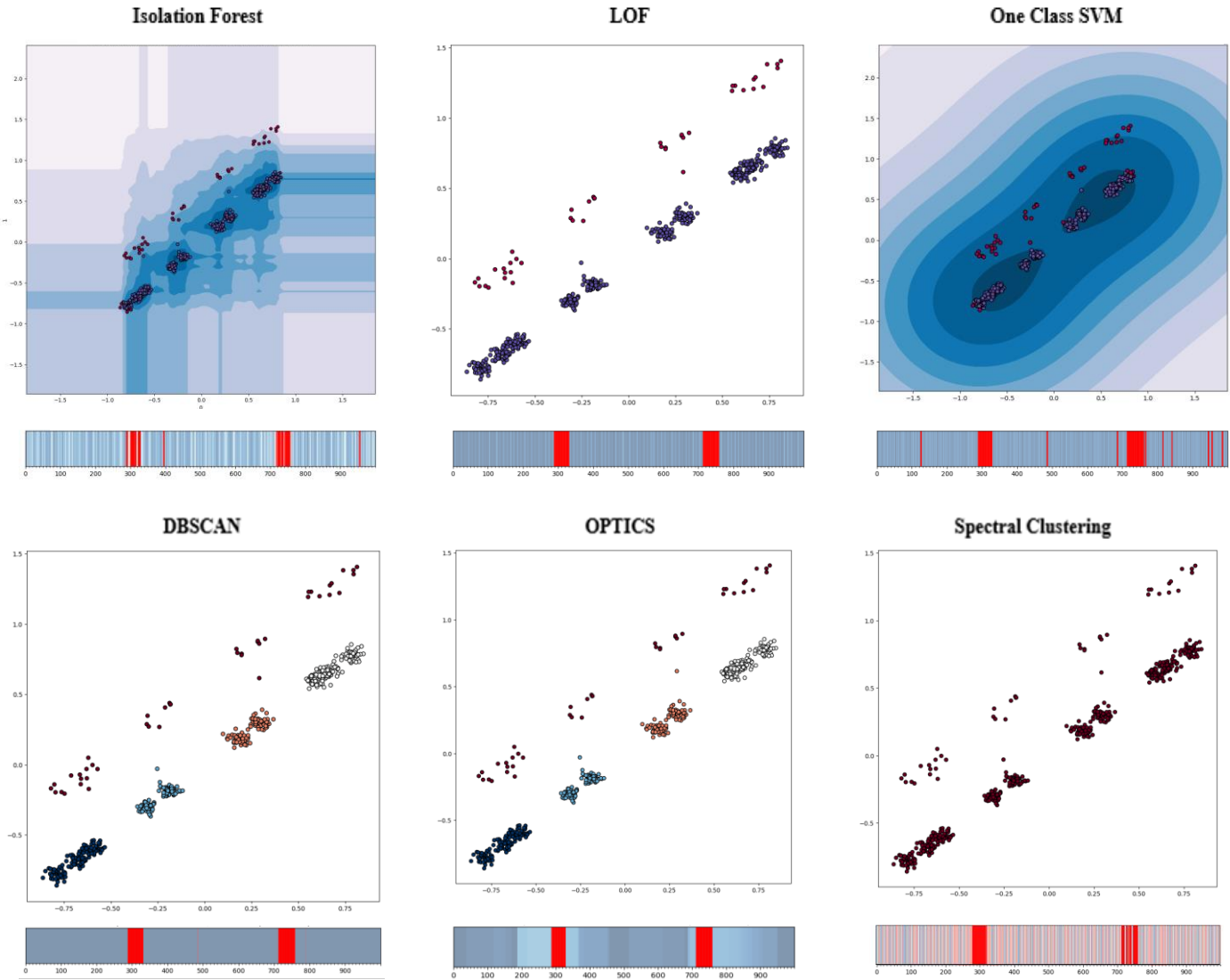


Пример исходных данных для моделирования



3. Метод обнаружения индикаторов угроз ИБ на основе ЦД

Графики выделения аномальных данных в режиме КА



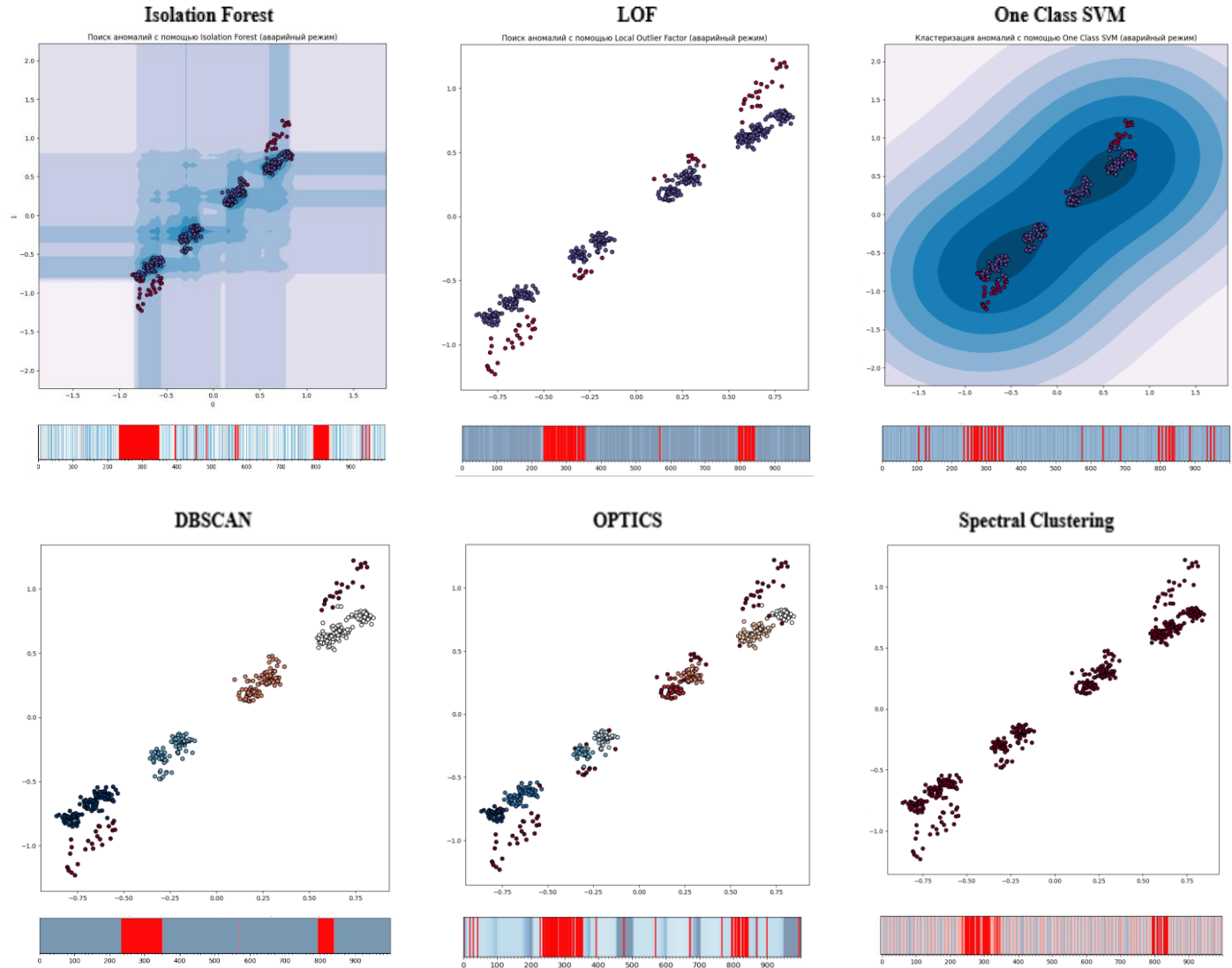
Метрики оценки

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%
DBSCAN	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%

Верхние графики: по оси X — аппроксимирующий коэффициент вейвлет-преобразования сигнала напряжения в нормальном режиме (A_2 , усл. ед.), по оси Y — тот же коэффициент в режиме кибератаки (A_2 , усл. ед.); нижние графики: аномальность во времени (ось X — время, с; цвет — уровень отклонения от нормы).

3. Метод обнаружения индикаторов угроз ИБ на основе ЦД

Графики выделения аномальных данных в аварийном режиме



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%
DBSCAN	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%

Верхние графики: по оси X — аппроксимирующий коэффициент вейвлет-преобразования сигнала напряжения в нормальном режиме (A_2 , усл. ед.), по оси Y — тот же коэффициент в режиме кибератаки (A_2 , усл. ед.); нижние графики: аномальность во времени (ось X — время, с; цвет — уровень отклонения от нормы).

3. Метод обнаружения индикаторов угроз ИБ на основе ЦД

Суть: Предложен метод обнаружения признаков угроз ИБ объектов КИИ, основанный на использовании ЦД для генерации синтетических данных, обучения моделей и адаптивного выявления аномалий в режиме реального времени.

Научная новизна: Разработан *новый* метод обнаружения признаков угроз ИБ объектов КИИ на основе анализа аномалий с применением цифрового двойника. Метод *отличается* применением двухконтурного подхода, включающего виртуальную среду моделирования и реальный объект, а также интеграцией генерации синтетических данных, вейвлет-преобразований, кластеризации и автоматизированной адаптации моделей. Метод *позволяет* различать киберугрозы и технические сбои, поддерживать актуальность моделей при изменении условий функционирования.

Теоретическая значимость: Развита теоретические основы применения ЦД для анализа поведения объектов КИИ и выявления слабовыраженных признаков угроз, что повышает точность диагностики и устойчивость к нехватке реальных данных.

Практическая значимость: Метод может применяться разработчиками и операторами систем ИБ КИИ для безопасного моделирования атакующих сценариев, обучения и внедрения алгоритмов обнаружения угроз без вмешательства в функционирование защищаемых объектов.

Соответствие паспорту специальности:

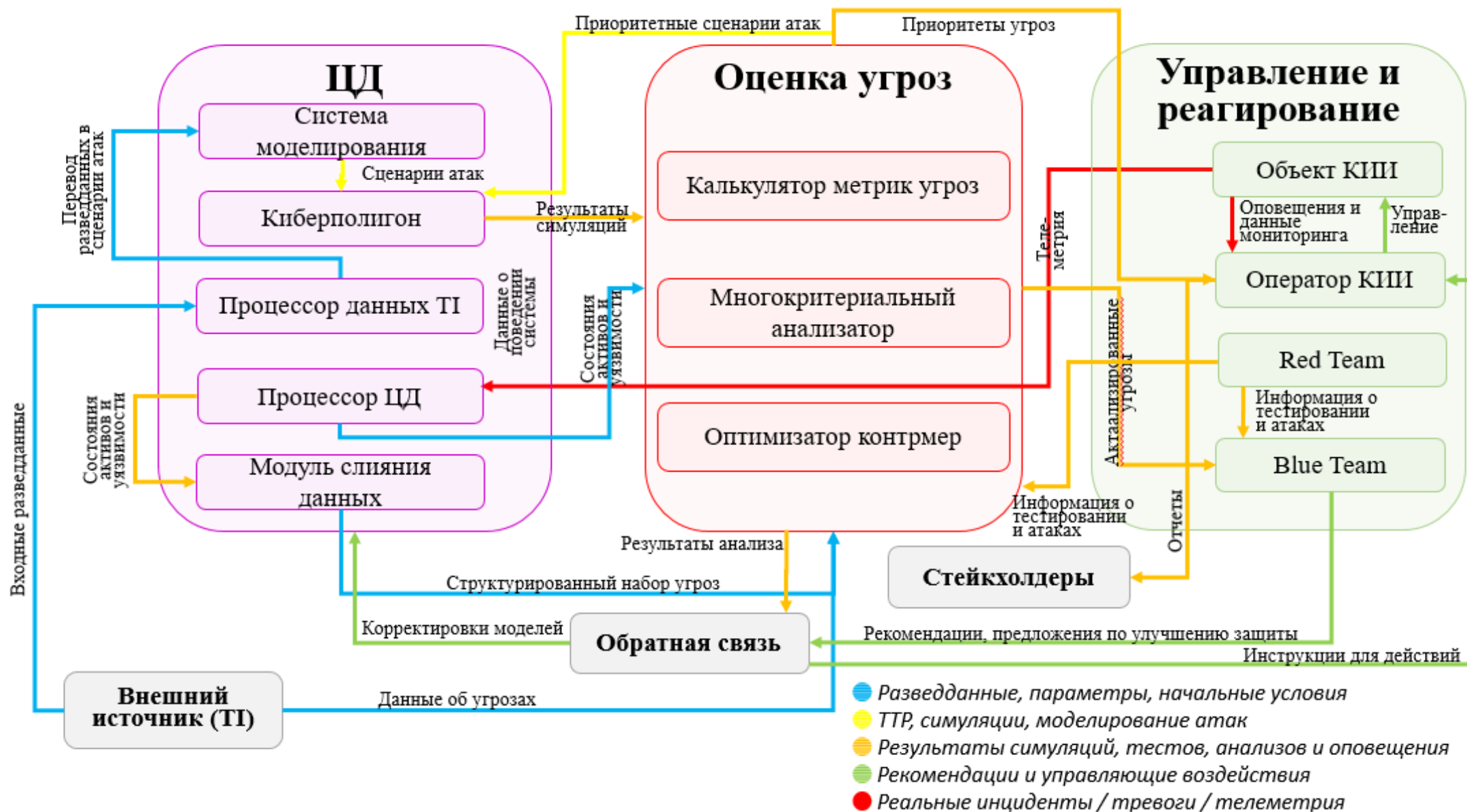
П. 3. Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.

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: 2, ВАК: 6, Программы ЭВМ (БД): 2, Иные публикации: 4)

4. Метод и методики многокритериальной оценки угроз ИБ объектов КИИ

Метод многокритериальной оценки угроз



4. Метод и методики многокритериальной оценки угроз ИБ объектов КИИ

Система показателей для оценки угроз

Показатель	Методика расчета	Источник данных
Тяжесть последствий (S)		
S1: Нормированное количество категорий ущерба	Определяется как отношение количества затронутых категорий ущерба (из трех возможных — У1, У2, У3) к максимальному числу категорий (3). Категории ущерба определены на основе методик ФСТЭК для КИИ.	Экспертная оценка на основе данных TI
S2: Индекс критичности последствий	Экспертная оценка тяжести последствий по шкале от 1 (низкая) до 5 (катастрофическая), базирующаяся на отчетах TI и стандартах MITRE Impact.	Разведка угроз (РУ) (отчеты, MITRE Impact)
S3: Нормированные ожидаемые потери	Оценка фактических финансовых потерь в тыс. рублей с нормализацией на максимальные потери в домене. Используется комбинированный анализ TI и ЦД с учетом оценки критичности актива.	РУ + ЦД
Возможности нарушителя (A)		
A1: Уровень возможностей	Категории возможностей нарушителя классифицируются по уровню (от 1 до 4), определяемому на основе атрибуции и отчетов TI.	РУ (атрибуция, отчеты)
A2: Индекс мотивации	Экспертная оценка мотивации атакующей группы по шкале 1–5, учитывающая цели и задачи, выявленные в анализе TI (например, цели APT-групп).	РУ (анализ целей APT)
A3: Категория доступа	Бинарная характеристика доступа: внешний (0) или внутренний (1), определяемая на основе анализа учетных записей и внутренних цифровых данных.	ЦД (анализ учетных записей)
Уязвимость объекта (V)		
V1: Нормированное количество уязвимых интерфейсов	Отношение количества уязвимых интерфейсов системы к максимальному количеству интерфейсов в аналогичных системах.	ЦД (инвентаризация)
V2: Индекс защищенности	Обратная величина оценки защищенности, полученной в ходе pentest-симуляций по шкале 1–3, нормированная для оценки уязвимости.	ЦД (pentest-симуляции)
V3: Критичность объекта	Двоичный индикатор критичности объекта, отражающий его принадлежность к критическим объектам инфраструктуры, согласно модели бизнес-процессов КИИ.	ЦД (модель бизнес-процессов КИИ)
Сложность реализации атаки (F)		
F1: Нормированное количество сценариев	Отношение количества известных сценариев реализации угрозы к максимальному числу сценариев для данного типа угрозы, на основе анализа TTP.	РУ (анализ TTP)
F2: Индекс сложности атаки	Обратная величина оценки сложности атаки по шкале 1–3 с учетом CVSS, MITRE и наличия эксплойтов в ЦД.	РУ + ЦД
F3: Нормированное время реализации	Обратная нормированная оценка времени, необходимого для реализации атаки, учитывающая сложность обхода систем защиты.	РУ + ЦД
Эффективность защиты (C)		
C1: Покрытие мерами защиты	Процент сценариев атаки, которые блокируются существующими мерами защиты, полученный на основе результатов симуляций в ЦД.	ЦД (результаты симуляций)
C2: Уровень мониторинга	Оценка эффективности мониторинга событий безопасности на основе анализа SIEM-правил, выраженная в баллах по шкале 1–3.	ЦД (анализ SIEM-правил)

4. Метод и методики многокритериальной оценки угроз ИБ объектов КИИ

Методика расчета обобщенного индекса угрозы

Алгоритм методики

1. Нормализация показателей

- Для обеспечения сопоставимости разноразмерных показателей проводится нормализация значений к диапазону $[0,1]$, с учетом направления оптимизации (максимизация или минимизация).

2. Агрегация показателей по проекциям

- Для каждой проекции $P \in \{S, A, V, F, C\}$ рассчитывается агрегированный показатель:

$$\Sigma P = \sum_{i=1}^n w_i \cdot K_{norm,i}, \quad \sum_{i=1}^n w_i = 1, \quad (36.1)$$

$K_{norm,i}$ – нормализованное значение i -го показателя,

w_i – весовой коэффициент показателя i в пределах проекции.

3. Расчет обобщённого уровня угрозы

На основе агрегированных показателей по проекциям:

$$\Sigma T = w_S \cdot \Sigma S + w_A \cdot \Sigma A + w_V \cdot \Sigma V + w_F \cdot \Sigma F + w_C \cdot \Sigma C, \quad (36.2)$$

$$\sum_{P \in \{S,A,V,F,C\}} w_P = 1,$$

w_P – весовой коэффициент для проекции P .

Примеры расчетов

Показатель	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
S1	0,33	0,67	0,00	0,67	0,33	0,67	0,33	0,67	0,00	0,33
S2	0,20	0,40	0,00	0,50	0,30	0,60	0,40	0,70	0,10	0,30
S3	0,45	0,60	0,10	0,80	0,40	0,70	0,30	0,90	0,20	0,50
ΣS	0,33	0,56	0,03	0,66	0,34	0,66	0,34	0,76	0,10	0,38
A1	0,25	0,50	0,00	0,75	0,25	0,50	0,25	0,75	0,00	0,50
A2	0,40	0,30	0,10	0,50	0,20	0,60	0,30	0,70	0,00	0,40
A3	0,00	1,00	0,00	1,00	0,00	1,00	0,00	1,00	0,00	1,00
ΣA	0,22	0,60	0,03	0,75	0,15	0,70	0,18	0,82	0,00	0,63
V1	0,70	0,60	0,30	0,50	0,80	0,40	0,90	0,30	0,50	0,70
V2	0,67	0,55	0,30	0,40	0,70	0,50	0,40	0,80	0,60	0,40
V3	0,00	1,00	0,00	1,00	0,00	1,00	0,00	1,00	0,00	1,00
ΣV	0,46	0,72	0,20	0,63	0,50	0,63	0,43	0,70	0,37	0,70
F1	0,55	0,40	0,30	0,60	0,70	0,50	0,40	0,60	0,20	0,50
F2	0,55	0,70	0,60	0,60	0,30	0,50	0,20	0,20	0,30	0,40
F3	0,60	0,50	0,20	0,70	0,30	0,40	0,30	0,80	0,10	0,60
ΣF	0,57	0,53	0,37	0,63	0,43	0,47	0,30	0,53	0,20	0,50
C1	0,80	0,70	0,90	0,40	0,15	0,25	0,30	0,40	0,10	0,20
C2	0,67	0,33	1,00	0,60	0,20	0,40	0,30	0,70	0,10	0,30
ΣC	0,74	0,52	0,95	0,50	0,18	0,33	0,30	0,55	0,10	0,25
ΣT	0,46	0,58	0,32	0,63	0,32	0,56	0,31	0,67	0,15	0,49

4. Метод и методики многокритериальной оценки угроз ИБ объектов КИИ

Методика ранжирования угроз ИБ объектов КИИ

Алгоритм методики

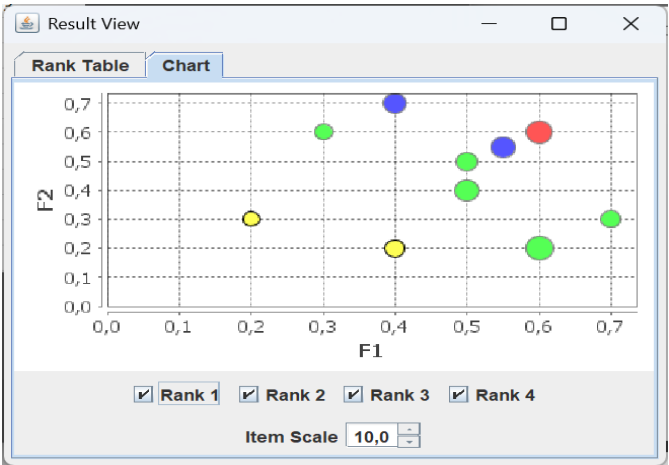
- Формирование исходных данных:**
Определяется множество угроз: $T = \{T_1, T_2, \dots, T_m\}$;
задаются критерии оценки: $C = \{C_1, C_2, \dots, C_k\}$.
- Выделение значимых угроз по критериям:**
Для каждого критерия C_i отбираются угрозы с граничными значениями:
 $T_1^{(1)}, T_2^{(1)}, \dots, T_k^{(1)}$. (3.1)
- Формирование объединённого множества:**
Объединяются угрозы, отобранные по всем критериям:
 $T^{(1)} = \bigcup_{i=1}^k T_i^{(1)}$. (37.2)
- Исключение доминируемых угроз:**
Удаляются угрозы, уступающие остальным по всем критериям одновременно.
- Итерационный анализ:**
Шаги 2–4 повторяются для оставшихся угроз, пока на итерации $t = T$ не останется менее двух элементов.
На каждой итерации формируется:
 $T^{(t)} = \bigcup_{i=1}^k T_i^{(t)}$. (37.3)
- Формирование итогового множества:**
Все полученные в итерациях подмножества объединяются:
 $M_{\text{итог}} = \bigcup_{t=1}^T T^{(t)}$. (37.4)
- Сопоставление с требованиями:**
Проверяется соответствие угроз нормативам и стратегическим приоритетам, при необходимости корректируются показатели.
- Финальное ранжирование:**
Множество $M_{\text{итог}}$ упорядочивается по степени значимости угроз, формируется итоговая классификация.

Результаты ранжирования по пяти критериям $\Sigma S, \Sigma A, \Sigma V, \Sigma F, \Sigma C$

Угроза	Ранг	ΣT
T_9	1	0,153
T_3	1	0,317
T_5	1	0,320
T_7	1	0,312
T_1	2	0,460
T_{10}	2	0,492
T_2	3	0,584
T_4	3	0,635
T_6	3	0,556
T_8	3	0,671

Результаты ранжирования по трем критериям F1, F2, F3

Result View					
Rank Table					
Name	Rank	F1	F2	F3	
T9	1	0.2	0.3	0.1	
T7	1	0.4	0.2	0.3	
T3	2	0.3	0.6	0.2	
T8	2	0.6	0.2	0.8	
T6	2	0.5	0.5	0.4	
T5	2	0.7	0.3	0.3	
T10	2	0.5	0.4	0.6	
T2	3	0.4	0.7	0.5	
T1	3	0.55	0.55	0.6	
T4	4	0.6	0.6	0.7	



4. Метод и методики многокритериальной оценки угроз ИБ объектов КИИ

Методика повышения защищенности объектов КИИ

Алгоритм методики

Этап 1. Агрегация и оценка угроз

Сбор данных из сетевых журналов, телеметрии, ЦД, систем мониторинга, внешней разведки угроз.

Для каждой угрозы T_i фиксируются параметры:

- K_i — интегральный индекс критичности;
- R_i — ранг угрозы;
- A_i — активы, находящиеся под воздействием;
- V_i — уязвимости, которые могут быть использованы для реализации угрозы.

Формируется матрица приоритетов угроз:

$$M = \begin{bmatrix} T_1 & R_1 & K_1 & A_1 & V_1 \\ T_2 & R_2 & K_2 & A_2 & V_2 \\ \dots & \dots & \dots & \dots & \dots \\ T_n & R_n & K_n & A_n & V_n \end{bmatrix} \quad (38.1)$$

Этап 2. Анализ защищённости

- Технический аудит;
- Организационный аудит;
- Имитационное моделирование (с помощью ЦД);
- Поиск «слепых зон» в защите.

Этап 3. Приоритезация и планирование

Формирование защитных мероприятий по каждой угрозе T_i с учётом матрица приоритетов угроз.

Этап 4. Внедрение защитных мер

- Настройка систем защиты;
- Обновление конфигураций центра детектирования;
- Корректировка политик безопасности и регламентов;
- Интеграция новых правил в платформу аналитики угроз.

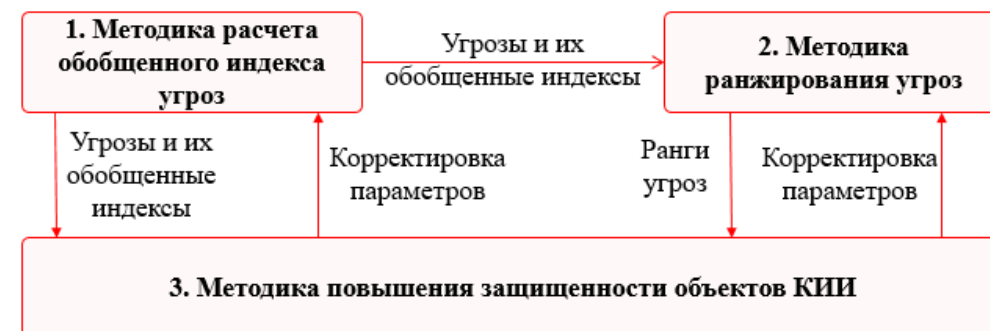
Этап 5. Мониторинг и адаптация

- Контроль изменений параметров угроз (K_i , R_i);
- Выявление аномалий и новых угроз;
- Корректировка: алгоритмов оценки, весов критериев, стратегий реагирования.

Замкнутый цикл ПАУ



Взаимосвязь методик



4. Метод и методики многокритериальной оценки угроз ИБ объектов КИИ

Методика повышения защищенности объектов КИИ

Апробация методики

Контекст апробации

- Объект: Цифровой двойник (ЦД) АСУ smart-сети
- Архитектура: телеметрия, управляющие модули, ПАУ
- Цель: оценка и ранжирование 5 угроз из Банка данных ФСТЭК

Метод оценки угроз

Для каждой угрозы T_i :

- Ранг угрозы: R_i — экспертная критичность (1 — максимальная)
- Индекс критичности: K_i — ущерб с учётом активов и вероятности
- Итоговая метрика:

$$W_i = \frac{K_i}{R_i} \quad (39.1)$$

где W_i — вес угрозы для приоритизации

Этапы апробации

Агрегация — поступление телеметрии и ИОС, автоматическое назначение R_i, K_i

Анализ — моделирование угроз в ЦД, выявлены «слепые зоны» для ID 11 и 37

Планирование — формирование матрицы приоритетов по W_i , генерация рекомендаций

Внедрение — тестирование мер в ЦД, обновление политик и правил ПАУ

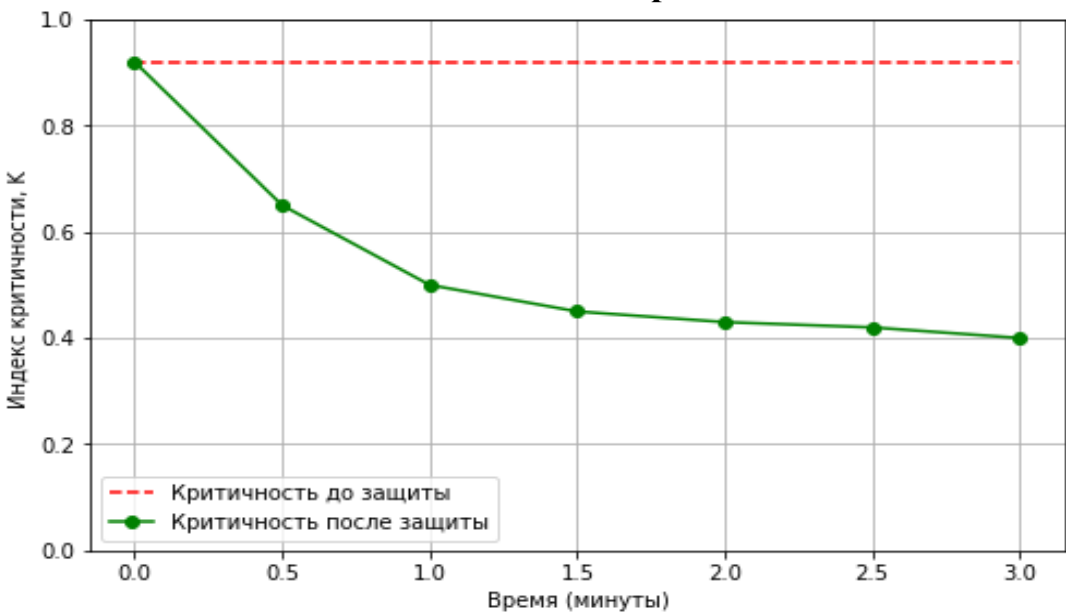
Мониторинг — измерение эффективности; пример:

▼ K_2 снизился на 50% за 1 минуту после вмешательства (см. график)

Параметры угроз

№	УБИ ID	Угроза	Ri	Ki	Wi
1	2	Агрегирование данных	1	0.92	0.920
2	4	Сброс пароля BIOS	2	0.83	0.415
3	11	Подмена ID-данных	3	0.71	0.237
4	22	Скрытый канал в коде	4	0.55	0.138
5	37	Обход межсетевого экрана	5	0.47	0.094

Изменение индекса критичности угрозы ID 2 после внедрения защитных мер



4. Метод и методики многокритериальной оценки угроз ИБ объектов КИИ

Суть. Разработан метод многокритериальной оценки угроз для объектов КИИ, в рамках которого создан комплекс взаимосвязанных методик. Метод основан на использовании цифрового двойника, системы количественных показателей характеристик угроз и принципов Парето-оптимальности.

Научная новизна. Предложен новый подход к многокритериальной оценке угроз ИБ объектов КИИ, реализуемый через интеграцию цифрового двойника как источника актуальных данных, применение системы количественных показателей для расчёта обобщённого индекса угроз, использование принципов Парето-оптимальности для их ранжирования и внедрение методики динамической корректировки защитных мер. Комплекс методик обеспечивает выявление и ранжирование приоритетных угроз, а также динамическую адаптацию мер защиты на основе поступающих данных из цифрового двойника и разведки угроз.

Теоретическая значимость. Уточнены и развиты теоретические подходы к многокритериальной оценке угроз ИБ объектов КИИ за счёт введения системы количественных характеристик угроз, а также интеграции цифрового моделирования, потоковой аналитики и методов ранжирования.

Практическая значимость. Предложенные методики могут быть использованы операторами КИИ для формализованной оценки и ранжирования угроз ИБ, выбора защитных мер.

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.

По данному результату опубликовано 13 работ (Scopus: 2, ВАК: 4, Программы ЭВМ (БД): 5, Иные публикации: 2)

5. Архитектура и программный прототип ЦД объекта КИИ (на примере АСУ интеллектуальной энергосистемы)

Функциональные подсистемы умной сети



Структура технических компонентов интеллектуальной энергетической сети по уровням управления



5. Архитектура и программный прототип ЦД объекта КИИ (на примере АСУ интеллектуальной энергосистемы)

Типы нарушителей и их возможности в контексте смарт-сетей

Тип нарушителя	Уровень доступа	Возможные действия	Характер воздействия
Внешний нарушитель (хакеры, конкуренты, иностранные спецслужбы и др.)	Отсутствие прямого доступа к элементам смарт-сети	- Поиск уязвимостей в интерфейсах и шлюзах - Атаки через внешние ИТ-сервисы - Социальная инженерия	Преднамеренный
Разработчик ПО/устройств	Доступ к исходным кодам, прошивкам, технической документации	- Внедрение уязвимостей и «закладок» - Интеграция вредоносного функционала на стадии разработки	Преднамеренный / случайный
Внутренний субъект без полномочий (обслуживающий персонал, посетители)	Физический доступ к инфраструктуре (например, в центрах управления, распределительных подстанциях)	- Подключение несанкционированных устройств - Физическое вмешательство в элементы сети	Случайный / преднамеренный
Пользователь внешних платформ (через API или облачные сервисы)	Ограниченный доступ к внешним ИТ-сервисам, связанным с энергетической сетью	- Злоупотребление доступами - Распространение вредоносного кода через открытые интерфейсы	Преднамеренный
Администратор внешней ИТ-инфраструктуры	Полный доступ к телекоммуникационному оборудованию и внешним каналам связи	- Подмена маршрутов, внедрение устройств перехвата - Неправильная настройка оборудования	Преднамеренный / случайный
Авторизованный пользователь смарт-сети (операторы, диспетчеры, инженеры)	Доступ к сегментам систем управления и мониторинга	- Нарушение конфигурации - Подлог телеметрии и управляющих команд	Преднамеренный / случайный
Администратор смарт-сети	Полные права на конфигурирование и администрирование систем	- Манипуляции с настройками, доступами и журналами - Установка/удаление компонентов системы	Преднамеренный / случайный
Внешний обслуживающий персонал (поставщики решений, интеграторы)	Удалённый доступ для обслуживания и обновления оборудования и ПО	- Неавторизованные изменения в конфигурации - Неосторожное вмешательство в работу системы	Преднамеренный / случайный

5. Архитектура и программный прототип ЦД объекта КИИ (на примере АСУ интеллектуальной энергосистемы)

Возможные уязвимости смарт-сети

Категория уязвимостей	Описание уязвимостей
Недостатки эксплуатации и администрирования	• Отсутствие формализованных правил разграничения доступа для подрядчиков и временного персонала. • Использование устаревшего оборудования и ПО из-за сложности замены в критических узлах. • Администрирование осуществляется с неконтролируемых или уязвимых рабочих мест. • Игнорирование принципов безопасной конфигурации систем и сетей. • Недостаток логирования и мониторинга активности пользователей и устройств.
Программные уязвимости в прикладном и системном обеспечении	• Наличие уязвимостей в пользовательском интерфейсе диспетчерских систем и ПО операторов. • Уязвимости в ПО обработки телеметрии и диспетчерского анализа. • Непатченные дыры в ОС и стороннем ПО, установленном на узловых серверах. • Ошибки в программной логике конфигурационных утилит и инженерного ПО.
Недостатки в архитектуре сетевых протоколов	• Использование незашифрованных или устаревших протоколов для обмена между узлами управления и полевыми устройствами. • Отсутствие механизмов верификации источника данных, что открывает путь к подмене информации. • Передача данных в открытом виде, позволяющая пассивный перехват и анализ трафика. • Использование общедоступных протоколов без настройки защиты по умолчанию.
Уязвимости оборудования и устройств	• Аппаратные закладки или скрытые функции в ПЛК и интеллектуальных контроллерах. • Недокументированные интерфейсы связи у промышленных шлюзов и преобразователей. • Слабая защищенность сенсоров, приводов, интеллектуальных счетчиков и систем АВР. • Уязвимости в промышленных сетевых устройствах (маршрутизаторы, коммутаторы и пр.).
Организационные пробелы в области кибербезопасности	• Отсутствие регулярного аудита безопасности и оценки текущих рисков. • Недостаточная подготовка персонала в области защиты информации и реагирования на инциденты. • Отсутствие требований к вендорам на этапе проектирования и закупки решений. • Низкий приоритет вопросов ИБ в общей стратегии эксплуатации смарт-сети.

5. Архитектура и программный прототип ЦД объекта КИИ (на примере АСУ интеллектуальной энергосистемы)

Пример описания угрозы внедрения вредоносного кода или данных для компонентов смарт-сети

Угроза	Внедрение вредоносного кода или данных
Сценарий реализации	Злоумышленник получает возможность внедрить вредоносный код или иные неавторизованные данные в компоненты ИТ-инфраструктуры смарт-сети. Атака может осуществляться напрямую (через уязвимые интерфейсы и протоколы), посредством подмены обновлений, социальной инженерии или через сторонние интеграционные сервисы. Код может активироваться автоматически (по событию или расписанию) либо запускаться вручную пользователем, не подозревающим о наличии вредоносной составляющей. Цель — нарушение работы системы, утечка данных, подмена управляющих команд или использование вычислительных ресурсов в обход установленного контроля.
Целевые компоненты (объекты воздействия)	• Узлы сбора и передачи телеметрии (RTU, датчики, интеллектуальные счетчики) • Компоненты подсистемы диспетчеризации и SCADA • Серверы управления данными и журналами • Промышленные контроллеры (ПЛК) • Устройства телемеханики • Промышленные АРМ операторов и инженеров • Коммутационное и маршрутизирующее оборудование • Межсетевые экраны и шлюзы • Системы синхронизации времени и резервного копирования
Типовые уязвимости	• Уязвимости SCADA/HMI-интерфейсов • Отсутствие проверки целостности ПО и обновлений • Использование ОС общего назначения без должной защиты • Уязвимые конфигурации • Открытые сетевые порты и сервисы • Недостаточный контроль прав доступа • Отсутствие систем контроля целостности и антивирусной защиты • Низкий уровень кибергигиены персонала (например, открытие вложений из сомнительных писем) • Использование стандартных учетных записей и паролей по умолчанию
Потенциальные источники угроз	• Внешние атакующие (хакеры, криминальные группы, конкуренты) • Разработчики программного/аппаратного обеспечения (при наличии доступа к исходному коду или проектным данным) • Пользователи внешних интеграционных сервисов и облачных платформ • Администраторы внешней инфраструктуры или провайдеры удалённого обслуживания

Описание киберфизических последствий угроз для смарт-сетей

Подсистема	Возможные последствия при нарушении функционирования подсистемы
Система управления энергопотреблением	• Потеря контроля за распределением энергии, что может привести к перегрузке сети или отключениям.
Система мониторинга и управления оборудованием	• Некорректная работа датчиков и контроля, что может вызвать сбои в функционировании сетевого оборудования.
Система управления распределением мощности	• Неоптимальное распределение энергии, что приведет к экономическим потерям и возможным авариям в сетевой инфраструктуре.
Автоматизированные подсистемы учета	• Искажение данных об энергопотреблении, что может привести к потерям в расчетах и неправильному начислению.
Протоколы передачи данных	• Нарушение безопасности передачи данных, что приведет к утечке конфиденциальной информации или внедрению вредоносного кода.
Системы коммуникации с клиентами	• Потеря связи с клиентами, что может повлиять на своевременное информирование об авариях или отключениях.
Системы безопасности и защиты данных	• Уязвимости в защите данных могут позволить несанкционированный доступ, изменяя данные о потреблении или инфраструктуре.
Система управления зарядными станциями	• Нарушение работы зарядных станций для электромобилей, что приведет к снижению качества обслуживания клиентов и снижению доступности зарядных точек.
Метрологические системы	• Ошибки в измерениях могут привести к некорректной информации об энергопотреблении, что затруднит работу всего процесса управления.
Системы энергообеспечения	• Потери энергии из-за неэффективной работы оборудования и нарушений в управлении потреблением энергии.

5. Архитектура и программный прототип ЦД объекта КИИ (на примере АСУ интеллектуальной энергосистемы)

Архитектура взаимодействия АСУ и ЦД



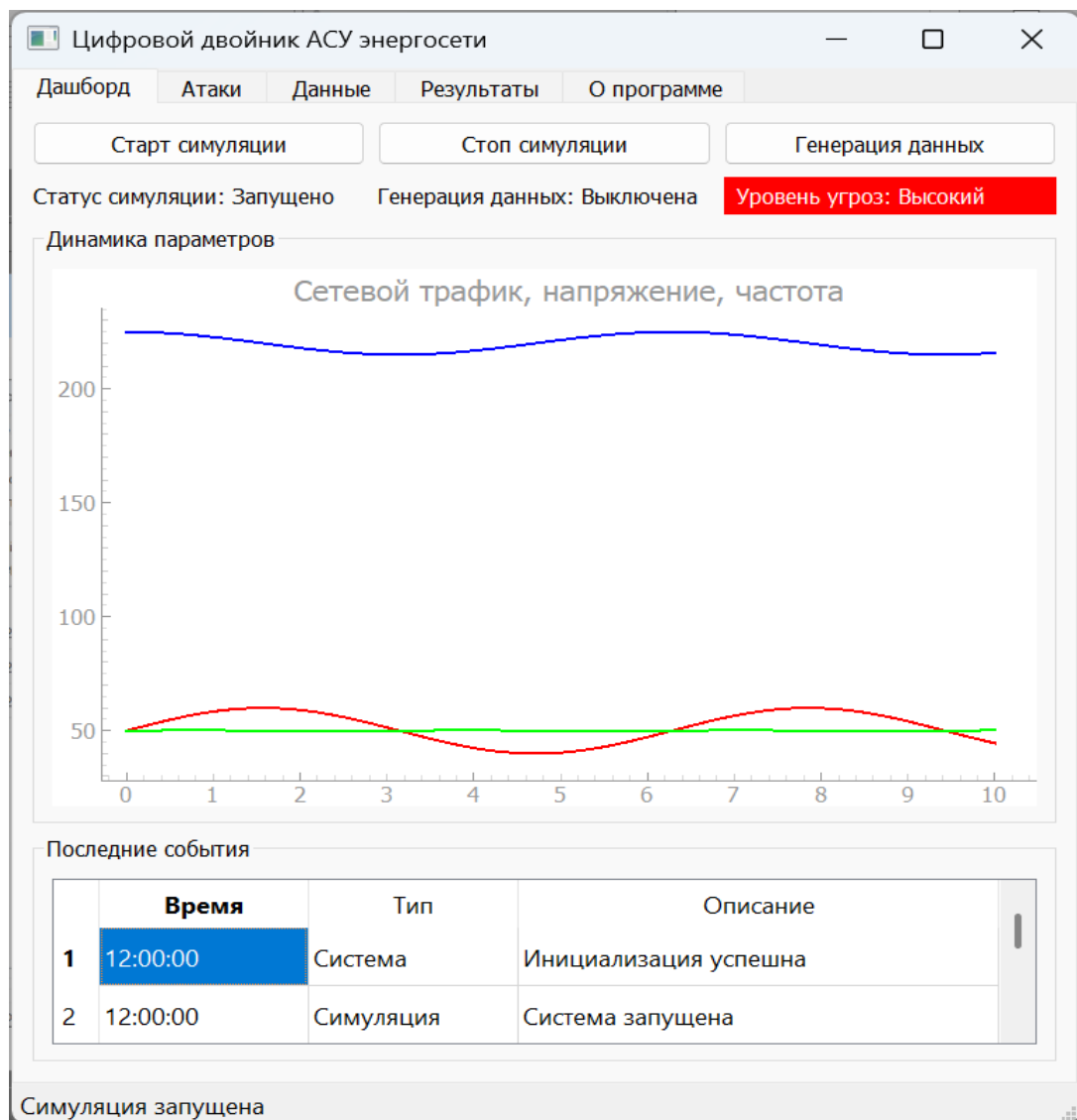
5. Архитектура и программный прототип ЦД объекта КИИ (на примере АСУ интеллектуальной энергосистемы)

Функциональная структура прототипа ЦД АСУ интеллектуальной энергосети

№	Наименование модуля	Назначение	Входы (источники данных)	Выходы (направление данных)
1	Модуль киберфизического моделирования	Имитация структуры и поведения АСУ интеллектуальной энергосети	- Из модуля 2 – уязвимости компонентов - Из модуля 4 – команды на проведение атак	- В модули 5 и 6 – реальные/синтетические данные - В модуль 7 – последствия атак (сбои, ущерб)
2	Модуль моделирования угроз ИБ	Управление знаниями об угрозах: классификация нарушителей, уязвимости, сценарии атак, последствия.	- Из модуля 3 – эталонные сценарии атак - Из модуля 1 – структура сети	- В модуль 1 – уязвимости компонентов - В модуль 4 – сценарии атак
3	Модуль генерации синтетических данных	Формирование синтетических наборов данных и эталонных сценариев атак	- Из внешних источников (ФСТЭК, MITRE, Threat Intelligence) - Из модуля 2 – описание атак	- В модуль 6 – синтетические данные - В модуль 2 – обновление модели угроз
4	Модуль симуляции атак	Исполнение атак по заданным сценариям в условиях, близких к реальным	- Из модуля 2 – что атаковать и как - От исследователя – когда запускать атаку	В модуль 1 – команды на проведение атаки
5	Модуль обнаружения аномалий	Выявление признаков кибератак	- Из модуля 6 – исторические данные - Из модуля 1 – онлайн-поток в режиме реального времени	- В модуль 7 – сигналы о выявленных атаках - В модуль 8 – метрики качества (Precision, Recall и др.)
6	Модуль агрегации данных	Хранение и предоставление объединенных наборов «реальных» и синтетических данных	- Из модуля 1 – данные киберфизической модели - Из модуля 3 – синтетические данные	В модуль 5 – данные для анализа
7	Модуль оценки угроз	Расчет и ранжирование угроз ИБ по множеству критериев	- Из модуля 1 – последствия атак - Из модуля 5 – характеристики выявленных атак - Из модуля 2 – сведения об уязвимостях	В модуль 8 – агрегированные оценки и приоритеты
8	Модуль верификации	Оценка корректности моделей и эффективности общей методологии анализа угроз, выводы по результатам анализа.	- Из модуля 5 – метрики обнаружения - Из модуля 7 – оценки угроз - Из модулей 1 и 4 – сведения о последствиях атак	Исследователю – рекомендации, выводы по точности и применимости методологии

5. Архитектура и программный прототип ЦД объекта КИИ (на примере АСУ интеллектуальной энергосистемы)

Экранные формы



Цифровой двойник АСУ энергосети

Дашборд Атаки Данные Результаты О программе

Управление атаками

Тип атаки: DoS

Цель: Автоматический уровень

Интенсивность:

Запустить атаку

Остановить атаку

Атака активна: Компрометация сигнала на Автоматический уровень (5/10)

Симуляция запущена

5. Архитектура и программный прототип ЦД объекта КИИ (на примере АСУ интеллектуальной энергосистемы)

Экранные формы

Цифровой двойник АСУ энергосети

Дашборд Атаки Данные Результаты О программе

Управление данными

☒ Использовать синтетические данные

Процент аномалий:

Текущий режим: реальные + синтетические данные

Пример данных

	Время	Значение	Тип
1	12:00:01	220.3	Нормальное
2	12:00:02	215.8	Нормальное
3	12:00:03	50.1	Аномалия

Система остановлена

Цифровой двойник АСУ энергосети

Дашборд Атаки Данные Результаты О программе

Статус: Нет угроз

Метрики модели

	Метрика	Реальные данные	Синтет.+Реальные
F1	F1	84%	90%
Ассиметри...	Ассиметри...	88%	91%

График обнаружения аномалий

Аномалии по времени

История обнаружений

	Время	Тип атаки	Результат	Статус
1	12:05:10	DoS	Обнаружено	Сработала сигн...
2	12:07:45	Компромети...	Не обнаружено	Передан ве...

Сбросить результаты

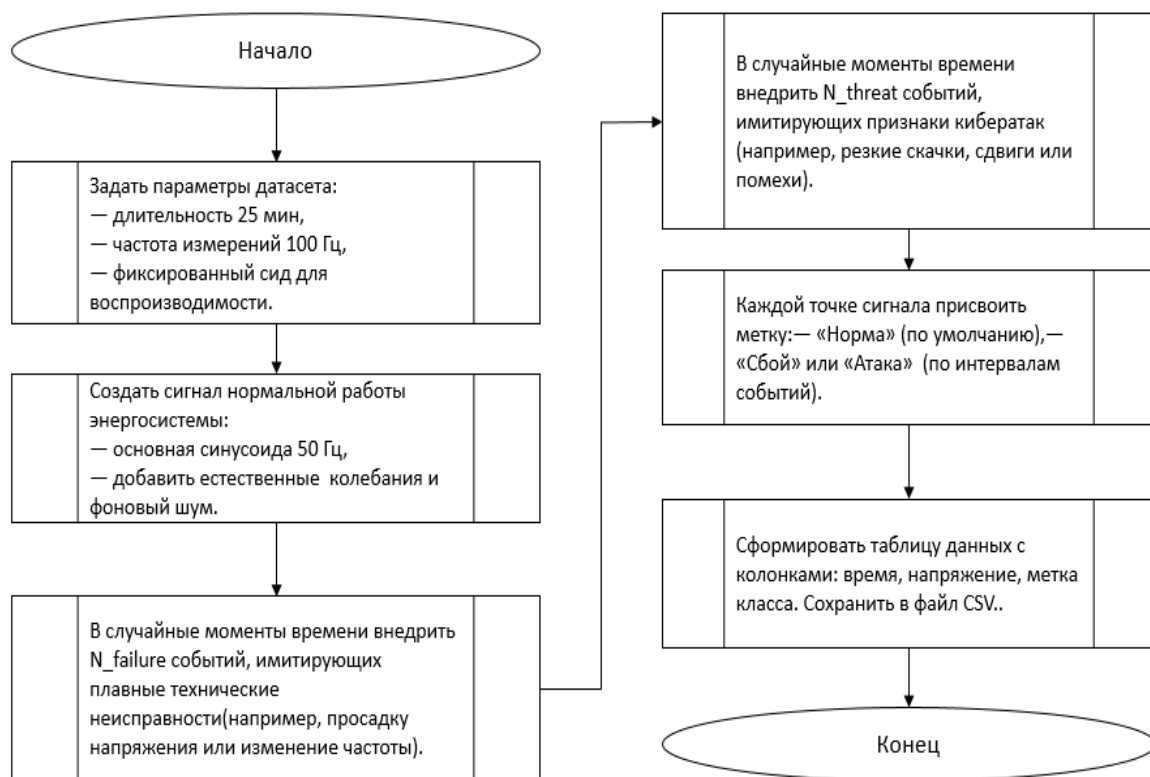
Заметки исследователя:

Система остановлена

5. Архитектура и программный прототип ЦД объекта КИИ (на примере АСУ интеллектуальной энергосистемы)

Серия экспериментов

Алгоритм генерации синтетического датасета для обучения и верификации моделей

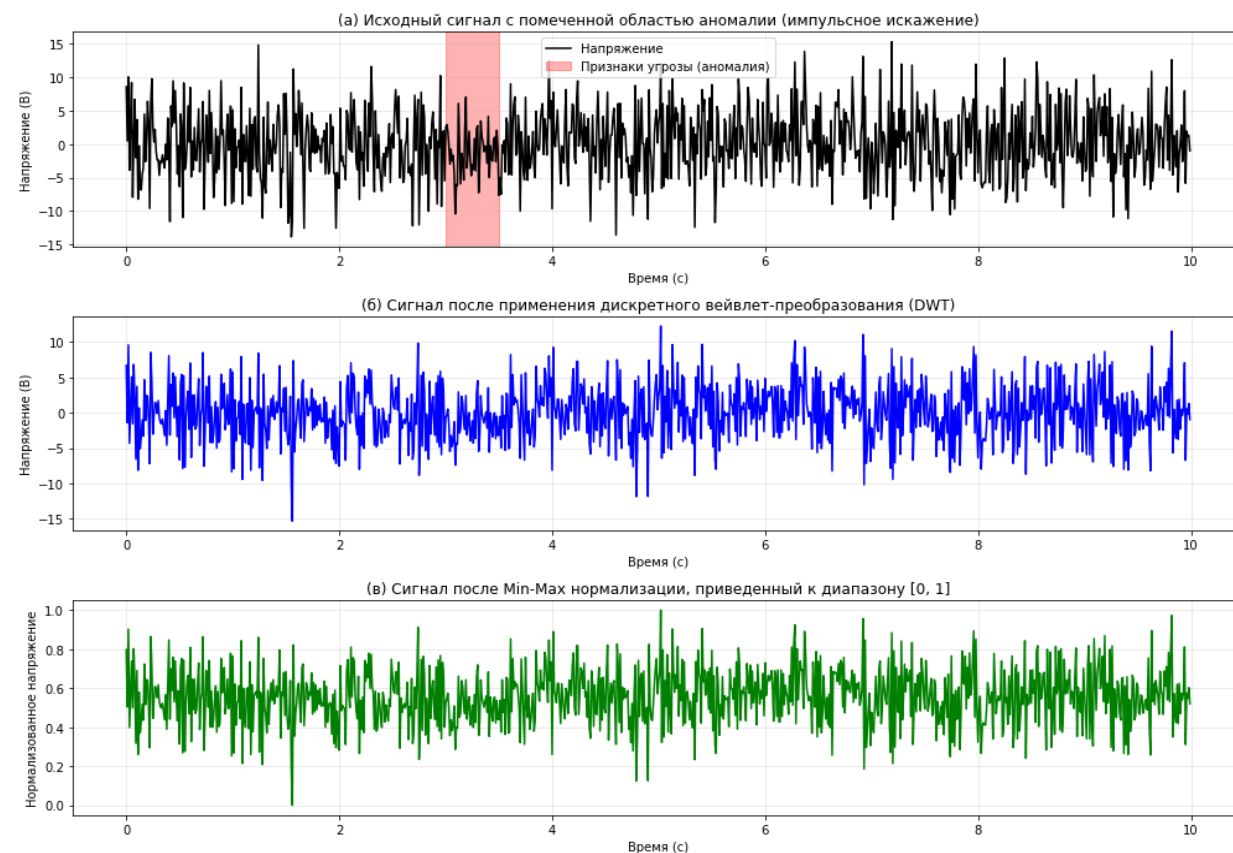


Пример сэмпла данных и его предобработки

(а) исходный сигнал с помеченной областью аномалии (импульсное искажение);

(б) сигнал после применения дискретного вейвлет-преобразования;

(в) сигнал после Min-Max нормализации.



5. Архитектура и программный прототип ЦД объекта КИИ (на примере АСУ интеллектуальной энергосистемы)

Серия экспериментов

Эксперимент 1 — Валидация адаптационного механизма (режимы оперативного и тактического обучения)

Алгоритм: *Isolation Forest*, обучение на 70К записях класса «Норма» → адаптация по обратной связи
Для оценки работоспособности замкнутого цикла адаптации применён двухэтапный механизм:

- Оперативный режим: инкрементное дообучение модели на дополнительных 7 500 записях «нормального» поведения из валидационной выборки;
- Тактический режим: оптимизация гиперпараметров (*n_estimators*, *contamination*) методом сеточного поиска на валидационном наборе.

Результат:

Метрика	До	После	Δ
Recall	82.5%	83.3%	+0.7%
FPR	17.5%	16.8%	−0.7%
F1-score	75.8%	76.1%	+0.2%

Эксперимент 2 — Влияние синтетических данных ЦД
Алгоритм: *Isolation Forest* → сравнение обучения на статичных внешних данных vs. динамически сгенерированных в ЦД

Эксперимент спроектирован как контролируемое сравнение при фиксированном объеме обучающих данных (85 000 записей):

- Baseline: обучение на 15 000 аномалий (классы «Failure», «Threat»), случайно выбранных из валидационной выборки;
- Proposed: обучение на 15 000 аномалий, сгенерированных детерминированным алгоритмом в модуле генерации ЦД (имитация импульсов, фазовых сдвигов, низкочастотной модуляции).

Результат:

Метрика	Baseline	Proposed	Δ
FPR	55.3%	51.8%	−6.4%
Recall	44.7%	48.3%	+8.0%
F1-score	55.0%	57.6%	+4.7%

5. Архитектура и программный прототип ЦД объекта КИИ (на примере АСУ интеллектуальной энергосистемы)

Серия экспериментов

Эксперимент 3 — Моделируемое сокращение времени реагирования (TTR)

Алгоритм: Расчёт совокупного времени реагирования (TTR) на основе предсказаний моделей до/после адаптации (Эксперимент 1)

Формализация TTR:

$$TTR = TP \times T_{true} + FP \times T_{false}$$

где TP — количество истинных срабатываний (угроза корректно определена), FP — количество ложных срабатываний (норма ошибочно классифицирована как угроза), $T_{true} = 1800$ сек — среднее время обработки истинного инцидента (верификация, инициация контрмер), $T_{false} = 300$ сек — среднее время обработки ложного срабатывания (анализ логов, отклонение тревоги).

Результат:

Сценарий	TP	FP	TTR (сек.)	Δ
До адаптации	2 231	2 621	4 802 100	—
После адаптации	2 147	2 513	4 618 500	−183 600 (−3.8%)

Расчет функции оптимизации

Показатель	До адаптации	После адаптации	Δ
$\Phi_1 (Recall)$	0.8253	0.8325	+0.0072
$\Phi_2 (1 - FPR)$	0.8253	0.8325	+0.0072
$\Phi_3 (1 - TTR/TTR_0)$	0.0000	0.0382	+0.0382
$F(\Theta, A)$ $= \sum \omega_k \Phi_k$	≈ 0.5502	≈ 0.5677	+0.0175 (+3.2%)

Выводы по 3-м экспериментам:

- Адаптация модели повышает точность прогнозирования (Recall ↑) и снижает ложные срабатывания (FPR ↓).
- Использование синтетических данных ЦД превосходит статичные данные по всем метрикам.
- Снижение FPR ведет к моделируемому сокращению времени реагирования.

5. Архитектура и программный прототип ЦД объекта КИИ
(на примере АСУ интеллектуальной энергосистемы и ЖД инфраструктуры)

Серия экспериментов

Эксперименты 4, 5. Многопараметрическая валидация в условиях расширенной телеметрии для энергосистемы и железной дороги

Параметр	Интеллектуальная энергосеть	Железнодорожная инфраструктура
Объект	Телеметрия напряжения в распределённой сети	Телеметрия контактной сети + SCADA-сигналы
Типы атак	- Скачок (резкое, мгновенное изменение уровня сигнала) - Дрейф (постепенное, непрерывное изменение сигнала во времени) - Имитация (подделка сигнала так, чтобы он статистически и визуально напоминал нормальное поведение системы) - ВЧ-колебания (наложение на сигнал высокочастотных гармоник или шумоподобных колебаний) - Комплексные (комбинация нескольких типов возмущений) - Скрытые (минимальные по амплитуде и длительности возмущения, специально спроектированные так, чтобы оставаться в пределах естественных флуктуаций сигнала)	- DNP3 spoofing — имитация подмены команд в SCADA (ложное разрешение движения); - Radio jamming — радиоподавление в канале экстренного торможения (CVE-2025-1727); - Rail circuit — подавление тока в рельсовой цепи (искусственное «освобождение» пути); - Stealth brake — незаметная команда торможения; - Modbus flood — перегрузка Modbus-канала; - Signal spoof — подделка сигналов (например, «зелёный» вместо «красного»)
Базовый сигнал	$x_{\text{норм}}(t) = U_0 + A_1 \sin(\omega_1 t) + A_2 \sin(\omega_2 t) + \varepsilon(t)$ U_0 — номинальное напряжение, A_1, A_2 — амплитуды гармоник, ω_1, ω_2 — частоты, $\varepsilon(t)$ — гауссов шум	То же (адаптировано под параметры ЖД)
Атака	$x(t) = x_{\text{норм}}(t) + \sum_{i=1}^{N_{\text{attack}}} a_i(t; \varphi_i) \cdot I[t_i, t_i + T_i](t)$ I — индикаторная функция, t_i — время начала, T_i — длительность, $a_i(t; \varphi_i)$ — функция возмущения	То же (с адаптированными функциями a_i)
Признаки	8: статистические (скользящее среднее, стандартное отклонение, межквартильный размах, асимметрия) и спектральные	12: статистические, спектральные и энтропийные (меры неопределенности сигнала)
Цель адаптации	Максимизация функции 5.1	
Триггер адаптации	$\Delta R = Recall_{val} - Recall_{test} > \Delta \text{порог} \text{ или } FPR_{test} > FPR_{max}$ $Recall_{val/test}$ — полнота на валидационной/тестовой выборке, $\Delta \text{порог}$ — порог падения полноты, FPR — доля ложных срабатываний	
Механизм адаптации	$D_{new} = D_{train} \cup FN_{sel}$ D_{train} — исходная обучающая выборка, FN_{sel} — отобранное подмножество ложнопущенных атак (False Negatives)	

5. Архитектура и программный прототип ЦД объекта КИИ
(на примере АСУ интеллектуальной энергосистемы и ЖД инфраструктуры)

Серия экспериментов

Эксперименты 4, 5. Многопараметрическая валидация в условиях расширенной телеметрии для энергосистемы и железной дороги

Характеристики датасетов

Параметр	Интеллектуальная энергосеть	Железнодорожная инфраструктура
Общий объём данных	10 000 отсчётов	
Частота дискретизации	1 Гц	
Доля аномалий	4% (400)	4.4% (440)
Обучающая выборка	6 000 отсчётов (180 аномалий)	6 000 отсчётов (210 аномалий)
Тестовая выборка	4 000 отсчётов (220 аномалий)	4 000 отсчётов (230 аномалий)
Количество признаков	8	12
Типы признаков	Статистические + спектральные	Статистические + спектральные + энтропийные
Количество типов атак	6	
Модель обнаружения	Random Forest	
Учет дисбаланса классов	Да	

Оценка функции эффективности (5.1) (усреднено по 20 запускам)

Объект	Модель	$Recall(\Phi_1)$	$1 - FPR(\Phi_2)$	$F(\Theta, A) = (\Phi_1 + \Phi_2)/2^*$
Интеллектуальная энергосеть	Базовая модель	0.520	0.929	0.725
	Адаптированная модель	0.830	0.986	0.908
Железнодорожная инфраструктура	Базовая модель	0.048	0.995	0.522
	Адаптированная модель	0.843	0.986	0.915

* Критерий Φ_3 в выражении (5.4) не рассчитывался, так как в экспериментах не измерялось время обработки инцидентов (TTR), а исходные значения Recall делают TTR_0 нерепрезентативным.

5. Архитектура и программный прототип ЦД объекта КИИ

Суть: На базе типового объекта КИИ реализован ЦД, предназначенный для апробации и оценки эффективности комплекса моделей и методов анализа угроз ИБ. ЦД обеспечивает безопасное моделирование кибератак, генерацию синтетических данных и тестирование алгоритмов обнаружения аномалий, формируя замкнутый контур для адаптивного анализа угроз. Апробация проведена на объектах АСУ интеллектуальной энергосистемы и железнодорожной инфраструктуры.

Научная новизна: Впервые реализована и экспериментально апробирована архитектура ЦД объекта КИИ, интегрированная с комплексом моделей и методов анализа угроз ИБ. Архитектура включает замкнутый цикл симуляции атак, генерации синтетических данных, обнаружения аномалий и оценки угроз, управляемый метриками качества на основе обратной связи от реального объекта.

Теоретическая значимость: Уточнены и дополнены принципы построения ЦД для объектов КИИ с учетом требований ИБ, включая необходимость двунаправленной синхронизации, поддержки сценарного моделирования угроз и интеграции механизмов оценки устойчивости.

Практическая значимость: Разработанный программный прототип ЦД использован в качестве испытательной среды для отработки сценариев кибератак и тестирования алгоритмов обнаружения угроз. Экспериментальная валидация на объектах АСУ интеллектуальной энергосистемы и железнодорожной инфраструктуры подтвердила эффективность методологии: использование синтетических данных ЦД позволило снизить частоту ложных срабатываний, а механизм целевого дообучения на ложнопущенных атаках обеспечил повышение полноты обнаружения, что в совокупности привело к росту обобщенной эффективности системы 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. 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: 6, Программы ЭВМ (БД): 2, Иные публикации: 2)

Оценка степень достижения цели исследования

Цель: Повышение эффективности анализа угроз ИБ объектов КИИ за счет разработки методологии, основанной на применении ЦД.

Результаты однопараметрических экспериментов

Критерий эффективности	Достигнутый результат	Количественное улучшение	Подтверждающий эксперимент
1. Повышение точности прогнозирования	Стабильный рост полноты обнаружения	• Рост Recall на 0.7% (с 82.5% до 83.3%)	Эксперимент 1
2. Снижение ложных срабатываний	Повышение надежности прогнозов	• Снижение FPR на 0.7% (с 17.5% до 16.8%) • Снижение FPR на 6.4% при использовании данных ЦД	Эксперимент 1, 2
3. Сокращение времени реагирования	Снижение операционной нагрузки	• Сокращение TTR на 3.8% (183 600 сек.)	Эксперимент 3
Интегральная эффективность	Комплексное улучшение	• Рост $F(\Theta, A)$ на 3.2%	Эксперименты 1-3

Результаты многопараметрических экспериментов

Критерий эффективности	Достигнутый результат	Количественное улучшение	Подтверждающий эксперимент
1. Повышение точности прогнозирования	Существенный рост полноты обнаружения	• Рост Recall на 61.5% (энергосистема) • Рост Recall с 4.8% до 84.3% (ж/д инфраструктура)	Эксперименты 4, 5
2. Снижение ложных срабатываний	Повышение достоверности прогнозов	• Рост 1-FPR до 0.986 на обоих объектах	Эксперименты 4, 5
Интегральная эффективность	Значительный рост качества системы	• Рост $F(\Theta, A)$ на 25.2% (энергосистема) • Рост $F(\Theta, A)$ на 75.3% (ж/д инфраструктура)	Эксперименты 4, 5

Оценка степень достижения цели исследования

№	Наименование положения	Вклад в достижение цели
1	Методологический подход к анализу угроз ИБ на основе ЦД	Сформировал концептуальные основы для реализации полного жизненного цикла анализа защищенности, обеспечивающего итеративную адаптацию моделей к эволюции угроз
2	Комплекс моделей цифрового двойника объекта КИИ	Предоставил формализованный аппарат для синхронизированного моделирования киберфизических процессов и безопасного исследования уязвимостей в изолированной среде
3	Метод обнаружения угроз ИБ с использованием цифрового двойника	Реализовал механизм двухконтурной адаптации, непосредственно обеспечивающий оптимизацию метрик точности обнаружения и минимизацию ложных positives
4	Метод и комплекс методик многокритериальной оценки угроз ИБ объектов КИИ	Обеспечил переход к обоснованному управлению рисками через формализацию процедур количественной оценки и ранжирования угроз по степени критичности
5	Прототип ЦД АСУ объекта КИИ	Эмпирически верифицировал корректность и практическую применимость методологии в условиях, аппроксимирующих реальную эксплуатационную среду

Выводы

1. Разработан методологический подход к анализу угроз ИБ КИИ на основе ЦД и многосрезового описания, объединяющий семь этапов — от формализации до верификации — с использованием виртуальной среды для динамического моделирования и адаптивного управления защитой.
2. Предложен комплекс взаимосвязанных моделей, включающий ЦД, онтологическое описание угроз и архитектуру взаимодействия с физической инфраструктурой, что обеспечивает двустороннюю синхронизацию и адаптивное реагирование на угрозы в реальном времени.
3. Разработан метод выявления признаков угроз ИБ объектов КИИ на основе анализа аномалий, синтетической генерации данных цифровым двойником и обучения алгоритмов выявления угроз с возможностью автоматического реагирования и адаптации в реальном времени.
4. Разработан метод многокритериальной оценки угроз ИБ КИИ, основанный на использовании комплекса взаимосвязанных методик, интегрирующих цифровой двойник как источник актуальных данных, количественные показатели угроз и принципы Парето-оптимальности для ранжирования.
5. Создана архитектура и программный прототип цифрового двойника АСУ объекта КИИ (например интеллектуальной энергосистемы) для апробации методологии адаптивного обнаружения угроз. Экспериментальная валидация подтвердила эффективность методологии по оцениваемым критериям эффективности.
6. Дальнейшее развитие может быть направлено на формализацию и стандартизацию процессов верификации и валидации ЦД в контексте требований регуляторов КИИ. Это включает разработку критериев соответствия для оценки адекватности цифрового двойника реальному объекту, а также методов подтверждения достоверности синтетически генерируемых данных в целях сертификации решений ИБ.

Список публикаций по теме исследования

Журналы из перечня ВАК (К1 и К2)

1. 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. **(К2, УБС 3) (ОНР 4)**
2. 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. **(К1, ядро РИНЦ, RSCI, УБС 2) (ОНР 2)**
3. 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. **(К1, ядро РИНЦ, RSCI, УБС 2) (ОНР 3)**
4. 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. **(К2, УБС 3) (ОНР 4)**
5. 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. **(К2, , УБС 3) (ОНР 1)**
6. 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. **(К2) (ОНР 1)**
7. 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. **(К2) (ОНР 5)**
8. 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. **(К2, УБС 3) (ОНР 2)**
9. 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. **(К2, УБС 3) (ОНР 3)**
10. 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. **(К1, ядро РИНЦ, RSCI, УБС 2) (ОНР 3)**
11. Митяков Е.С. Моделирование ИБ-угроз объектам критической информационной инфраструктуры с использованием цифровых двойников // Защита информации. Инсайд. – 2025. – №5. – С. 2–8. **(К2) (ОНР 1)**.
12. Митяков Е.С. Онтологическое моделирование анализа угроз информационной безопасности объектам критической информационной инфраструктуры на основе цифровых двойников // Защита информации. Инсайд. – 2025. **(К2) (ОНР 2)** (в печати).
13. Митяков Е.С. Архитектурная модель обеспечения информационной безопасности объектов КИИ на основе цифрового двойника // Информатизация и связь. – 2025. – №3. – С. 119–124. **(К2, УБС 3) (ОНР 2)**
14. Митяков Е.С., Саенко И.Б., Садовников В.Е. Модель декомпозиции объектов критической информационной инфраструктуры для анализа угроз информационной безопасности // Информация и космос – 2025. – №3. – С. 63–70. **(К2) (ОНР 3)**.
15. Котенко И. В., Саенко И. Б., Митяков Е. С. Многокритериальная оценка угроз информационной безопасности на основе технологий цифровых двойников и разведки угроз // Прикладная информатика. 2025. Т. 20. № 5. С. 64–84. **(К1, ядро РИНЦ, RSCI, УБС 2) (ОНР 4)**.
16. Митяков Е.С., Адиев М.М. Функциональная модель анализа угроз информационной безопасности объектов критической информационной инфраструктуры на основе цифрового двойника // Информатизация и связь. – 2025. – №4. **(К2, УБС 3) (ОНР 1)** (в печати)
17. Котенко И. В., Саенко И. Б., Митяков Е. С. Адаптивная оценка киберугроз в критической информационной инфраструктуре железнодорожного транспорта с использованием цифрового двойника // Вопросы кибербезопасности. – №6. **(К1, ядро РИНЦ, RSCI, УБС 2) (ОНР 5)** (в печати)
18. Митяков Е.С. Метод обнаружения признаков угроз информационной безопасности объектов критической информационной инфраструктуры на основе цифровых двойников // Computational Nanotechnology. 2025. Т. 12. № 3. С. 115–122. **(К2, УБС 4) (ОНР 3)**
19. Митяков Е.С. Разработка прототипа цифрового двойника автоматизированной системы управления интеллектуальной энергосетью для анализа угроз информационной безопасности // Computational Nanotechnology. – 2025. – №4. **(К2, УБС 4) (ОНР 5)** (в печати).
20. Митяков Е.С. Методика категорирования объектов критической информационной инфраструктуры с учетом отраслевой критичности // Computational Nanotechnology. – 2025. – №5. **(К2, УБС 4) (ОНР 1)** (в печати).
21. Митяков Е.С. Методика многокритериального ранжирования угроз информационной безопасности объектов критической информационной инфраструктуры на основе данных цифрового моделирования // Защита информации. Инсайд. – 2026. – №1. **(К2) (ОНР 4)** (в печати).
22. Митяков Е.С. Динамическая адаптация защиты объектов КИИ на основе цифрового двойника и потоковой аналитики угроз // Защита информации. Инсайд. – 2026. – №2. **(К2) (ОНР 3)** (в печати).
23. Митяков Е.С. Интегрированная архитектура защиты объектов критической информационной инфраструктуры с использованием цифрового двойника и киберполигона // Защита информации. Инсайд. – 2026. – №3. **(К2) (ОНР 2)** (в печати).
24. Котенко И. В., Саенко И. Б., Митяков Е. С. Адаптивная система обнаружения кибератак в интеллектуальных энергетических системах на основе цифрового двойника (в подготовке) **(ОНР 5)**

Список публикаций по теме исследования

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. **Q3 УБС4 (ОHP 1)**
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. **(ОHP 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. **(ОHP 5)**
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. **(ОHP 3)**
5. Mityakov E. S. , Ladynin A. I. , Shmeleva A. G. and Kazakevich I. D. Critical Information Infrastructures Intelligent Protection: Digital Twins and Neural Network-Based Threat Detection Methods // 2025 VI International Conference on Neural Networks and Neurotechnologies (NeuroNT), Saint Petersburg, Russian Federation, 2025, pp. 22-25, doi: 10.1109/NeuroNT66873.2025.11049978. **(ОHP 3)**
6. Mityakov E. S., Ladynin A. I. and Kazakevich I. D. Critical Information Infrastructures Protection Architecture Based on Hybrid Data Analysis and AI Algorithms // 2025 VI International Conference on Neural Networks and Neurotechnologies (NeuroNT), Saint Petersburg, Russian Federation, 2025, pp. 26-29, doi: 10.1109/NeuroNT66873.2025.11049963. **(ОHP 2)**
7. Mityakov S. N. , Mityakov E. S. , Ladynin A. I. , Kryukova T. M. . 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. **УБС2, Q3 (ОHP 1)**
8. 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. **Q4 (ОHP 1)**
9. 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. **УБС2, Q3 (ОHP 4)**
10. 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. **Q2 (ОHP 4)**
11. 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. **УБС2, Q2 (ОHP 1)**
12. Котенко И.В., Саенко И.Б., Митяков Е.С., Кочин В.П. Методология анализа угроз информационной безопасности с использованием цифровых двойников // Журнал Белорусского государственного университета. Математика. Информатика. – 2025 (в печати). **УБС3, Q4 (ОHP 1)**
13. Mityakov E., Kotenko I., Saenko I. The Model of Information Security Threats to Critical Information Infrastructure Objects // 2025 International Ural Conference on Electrical Power Engineering (UralCon), Magnitogorsk, Russian Federation, 2025 **(ОHP 1)** (в печати).
14. Mityakov E., Ladynin A. and Goprinenko G. Cross-Sectoral Analysis of Threat Interdependencies in Critical Information Infrastructure **(ОHP 1)** (в печати).
15. Mityakov E., Ladynin A. and Besedin M. Digital Twin of the Power Grid ICS: A Platform for Simulating and Assessing Information Security **(ОHP 5)** (в печати).
16. Kotenko I., Saenko I., Mityakov E. An Adaptive Digital Twin-Based Framework for Cyber-Threat Detection in Smart Grid Control Systems. Energies **УБС2, Q1 (ОHP 5)** (в подготовке)
17. Mityakov E., Ladynin A., Shmeleva N. Software and Analytical Complex for Supporting the Balanced Development of Electric Power Ecosystems **(ОHP 5)** (в подготовке)

Свидетельства о государственной регистрации базы данных и программ для ЭВМ

1. Митяков Е.С., Лапаев Д.Н., Корнев Е.А. Программа для решения трех- и более критериальных задач. Свидетельство №2014610410. – 2014. **(ОHP 4)**
2. Митяков Е.С., Лапаев Д.Н., Корнев Е.А. Программа для ранжированного решения трех- и более критериальных задач. Свидетельство №2014610635. – 2014. **(ОHP 4)**
3. Митяков Е.С., Лапаев Д.Н., Корнев Е.А. Программа для ранжированного решения двухкритериальных задач. Свидетельство №2014610636. – 2014. **(ОHP 4)**
4. Митяков Е.С., Лапаев Д.Н., Корнев Е.А. Программа для решения трехкритериальных задач. Свидетельство №2014610637. – 2014. **(ОHP 4)**
5. Митяков Е.С., Лапаев Д.Н., Корнев Е.А. Программа решения многокритериальных задач с применением методики определения ранжированных взаимоприемлемых альтернатив. Свидетельство №2015612049. – 2015. **(ОHP 4)**
6. Митяков Е.С., Смирнов М.В. База данных комплексных угроз информационной безопасности критической информационной инфраструктуры. Свидетельство №2025622435. – 2025. **(ОHP 1)**
7. Митяков Е.С., Ладынин А.И., Казакевич И.Д. Программный комплекс предупреждения угроз на основе комбинации методов выявления аномалий. Свидетельство № 025667291 – 2025. **(ОHP 3)**
8. Митяков Е.С. Беляевская-Плотник Л. А. Приложение для визуализации уровня безопасности «Радар-Контроль». Свидетельство № 2025668256 – 2025. **(ОHP 5)**
9. Митяков Е.С., Ладынин А.И., Казакевич И.Д. Программный комплекс раннего предупреждения угроз на основе анализа опережающих индикаторов. Свидетельство № 2025680237 – 2025. **(ОHP 3)**
10. Митяков Е.С., Беседин М.Д., Беседин Д.Д. Цифровой двойник АСУ смарт-сети. Свидетельство № 2025681061 – 2025. **(ОHP 5)**

Список публикаций по теме исследования

Иные публикации

1. Д. Н. Лапаев, Е. С. Митяков, Е. А. Корнев. Программный комплекс многокритериального сравнительного анализа экономических систем // Экономика, статистика и информатика. Вестник УМО. – 2014. – № 6-2. – С. 466-469 **УБС 2 (ОНР 4)**.
2. Митяков С.Н., Митяков Е.С. Машинное обучение в задачах исследования инновационных процессов // Журнал прикладных исследований. – 2020. – № 4-1. – С. 6–13. **УБС 4 (ОНР 1)**
3. Митяков Е.С., Ладынин А.И., Шмелева А.Г. Разработка подходов к управлению наукоемкими предприятиями в условиях цифровизации процессов поддержки принятия решений // Журнал прикладных исследований. – 2021. – № 2-1. – С. 6-12. **УБС 4 (ОНР 1)**
4. Митяков Е.С., Ладынин А.И., Шмелева А.Г. Модель прогнозирования уровня научно-технической безопасности наукоемких организаций на основе методов теории случайных процессов // Развитие и безопасность. – 2022. – № 2(14). – С. 45-56. – DOI 10.46960/2713-2633_2022_2_45. **УБС 4 (ОНР 2)**
5. Митяков Е.С., Ладынин А.И. Концептуальная модель информационной системы совершенствования научно-технологической безопасности // Актуальные вопросы экономики, менеджмента и инноваций : Материалы Международной научно-практической конференции, Нижний Новгород, 16 ноября 2022 года. – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2022. – С. 188-189. **(ОНР 2)**
6. 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)**
7. 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. **УБС 4 (ОНР 2)**
8. Митяков Е. С. Цифровые двойники как объект и инструмент информационной безопасности // Информационные технологии и телекоммуникации. 2024. Т. 12. № 4. С. 1–12. **(ОНР 2)**
9. Митяков Е.С. Цифровые двойники и безопасность критической информационной инфраструктуры: правовые и технологические аспекты // Национальная безопасность и стратегическое планирование. 2024. №. 4. С. 29-34. **(ОНР 1)**
10. Митяков Е.С. Теоретические аспекты использования имитационного, сценарного и агент-ориентированного моделирования промышленных экосистем // Актуальные вопросы экономики, менеджмента и инноваций : материалы Международной научно-практической конференции ученых, специалистов, преподавателей вузов, аспирантов, студентов, Нижний Новгород, 23 ноября 2023 года. – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2024. – С. 129-131. **(ОНР 1)**
11. Амосов Е.А., Митяков Е.С. Реализация NPM-пакета для анализа временных рядов в web-приложениях // Хроники цифровых трансформаций : Сборник научных трудов по материалам круглых столов, стратегических и форсайт-сессий, панельных дискуссий, посвящённых решению практических задач, Москва, 16–17 марта 2023 года. – Москва: МИРЭА - Российский технологический университет, 2024. – С. 20-23. **(ОНР 3)**
12. Митяков Е.С., Козлов Я.В. Системы искусственного интеллекта в управлении производственными системами // Региональная и отраслевая экономика. – 2024. – № 1. – С. 88–95. **УБС 4 (ОНР 3)**
13. Митяков Е.С., Козлов Я.В. Система показателей управления производственной системой в условиях цифровой трансформации // Инновации и инвестиции. – 2024. – № 2. – С. 596–600. **(ОНР 4)**
14. 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 в условиях цифровизации экономики : Сборник научных статей по итогам IV Всероссийского научно-практического семинара, Нижний Новгород, 23 апреля 2024 года. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2024. – С. 136-141. **(ОНР 3)**
15. Митяков Е. С. К вопросу об управлении промышленными экосистемами с использованием цифровых двойников // Концепции, теория и методика фундаментальных и прикладных научных исследований : Сборник статей Национальной (Всероссийской) научно-практической конференции с международным участием, Челябинск, 22 августа 2024 года. – Уфа: ООО "Омега сайнс", 2024. – С. 68-70. **(ОНР 2)**
16. Митяков Е.С. Горпиненко Г.В. Междисциплинарный подход к классификации угроз информационной безопасности критическим информационным инфраструктурам // Информационные технологии и интеллектуальные системы : Сборник научных трудов по материалам III ежегодной национальной конференции, Москва, 18–20 марта 2025 года. – Москва: МИРЭА - Российский технологический университет, 2025. – С. 638-642. **(ОНР 1)**
17. Митяков Е.С. Горпиненко Г.В. К вопросу об использовании методологии сбалансированной системы показателей в задачах оценки информационной безопасности объектов критической информационной инфраструктуры // Информационные технологии и интеллектуальные системы : Сборник научных трудов по материалам III ежегодной национальной конференции, Москва, 18–20 марта 2025 года. – Москва: МИРЭА - Российский технологический университет, 2025. – С. 643-646. **(ОНР 4)**
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 в условиях цифровизации экономики : Сборник научных статей по итогам V Всероссийского научно-практического семинара, Нижний Новгород, 23 апреля 2025 года. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2025. – С 66-72. **(ОНР 3)**
19. Митяков Е.С. Эволюция концепций и технологий защиты информации в критических информационных инфраструктурах // Математическое и компьютерное моделирование и бизнес-анализ в условиях цифровизации экономики : Сборник научных статей по итогам V Всероссийского научно-практического семинара, Нижний Новгород, 23 апреля 2025 года. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2025. – С 169-174. **(ОНР 5)**
20. Смирнов М. В., Митяков Е.С. Разработка модели базы знаний по управлению устойчивым развитием промышленных экосистем // Computational Nanotechnology. – 2025. – Т. 12, № 1. – С. 129-137. **УБС 4 (ОНР 2)**
21. Митяков Е.С., Смирнов М.В., Владыко И.Ю. Программно-аналитический комплекс поддержки сбалансированного развития промышленных экосистем // Computational Nanotechnology. 2025. Т. 12. № 3. С. 123–129. **УБС 4 (ОНР 5)**

Спасибо за внимание