УДК 004.056

Буркацкий Кирилл Александрович,
старший преподаватель кафедры «Защита информации»
МГТУ им. Н.Э. Баумана, г. Москва
Чаркин Владимир Константинович студент
3 курс, факультет «Информатика и системы управления»
МГТУ им. Н.Э. Баумана
Россия, г. Москва
Литвин Антон Александрович студент
3 курс, факультет «Информатика и системы управления»
МГТУ им. Н.Э. Баумана
Россия, г. Москва
Сатановская Елизавета Андреевна,
студент,
3 курс, факультет «Информатика и системы управления»
МГТУ им. Н.Э. Баумана
Россия, г. Москва
Научный руководитель: Владыченская Варвара Александровна

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ПРОАКТИВНОГО МОНИТОРИНГА АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация: *В статье представлен комплексный анализ методологических аспектов перехода от реактивных к проактивным моделям защиты автоматизированных информационных систем (АИС), входящих в состав критической информационной инфраструктуры (КИИ) Российской Федерации. Проведено детальное исследование эволюции нормативно-правовой базы — от базового ФЗ-149 до профильного ФЗ-187*

и детализирующих его актов ФСТЭК России (приказы № 239, 31, 235, 21, 117) и ФСБ России (приказы № 378, 416/489), а также национального стандарта ГОСТ Р 57580.1-2017. Выявлена устойчивая тенденция к ужесточению требований по времени обнаружения и реагирования на инциденты, формирующая нормативный императив для внедрения предиктивных технологий. Предложена иерархическая система метрик безопасности, сгруппированная по пяти уровням мониторинга (аппаратный, сетевой, программный, пользовательский, контекстный), и разработана архитектура гибридной математической модели проактивного реагирования, интегрирующей детерминированные правила, статистическое прогнозирование и методы машинного обучения (ансамбль LSTM + Isolation Forest).

Ключевые слова: *критическая информационная инфраструктура; проактивный мониторинг; нормативно-правовая база; машинное обучение; метрики безопасности; SIEM; гибридная модель; АИС КИИ; кибербезопасность*

Annotation: *The article presents a comprehensive analysis of methodological aspects of the transition from reactive to proactive protection models for automated information systems (AIS) within the critical information infrastructure (CII) of the Russian Federation. The study traces the evolution of the regulatory framework from the foundational Federal Law No. 149 to the specialized Federal Law No. 187 and its implementing acts issued by the FSTEC of Russia (Orders No. 239, 31, 235, 21, 117), the FSB of Russia (Orders No. 378, 416/489), and the national standard GOST R 57580.1-2017. A consistent trend toward stricter requirements for incident detection and response time is identified, creating a regulatory imperative for predictive technology adoption. A hierarchical security metrics system grouped across five monitoring levels (hardware, network, software, user, and contextual) is proposed, and the*

architecture of a hybrid mathematical model for proactive incident response is developed, integrating deterministic rules, statistical forecasting, and machine learning methods (LSTM + Isolation Forest ensemble).

Key words: *critical information infrastructure; proactive monitoring; regulatory framework; machine learning; security metrics; SIEM; hybrid model; CII AIS; cybersecurity*

Введение

Цифровая трансформация отраслей КИИ (энергетика, связь, здравоохранение, финансы, транспорт) привела к созданию высокосложных, распределённых и взаимозависимых АИС. Уязвимость таких систем в условиях эскалации гибридных угроз демонстрирует растущая статистика. По оценкам отраслевых исследований, более 60% успешных кибератак на объекты КИИ в 2023–2024 гг. начинались с эксплуатации уязвимостей в периферийном сетевом оборудовании и серверах, а тренды 2025 года указывают на смещение фокуса злоумышленников в сторону атак через цепочку поставок (supply chain) и компоненты инфраструктурного ПО с использованием методов искусственного интеллекта. По данным аналитического отчета Positive Technologies CODE RED 2026, во второй половине 2024 года и в первых трех кварталах 2025 года Россия оставалась одной из приоритетных целей киберпреступников: на ее долю приходилось 14–16% всех успешных кибератак в мире, а среди российских организаций наиболее часто атакам подвергались промышленные предприятия, государственные учреждения, IT-компании и телекоммуникационные организации [16].

Регуляторы, осознавая эти риски, последовательно формируют и актуализируют НПБ, которая не только предписывает защиту, но и де-факто требует перехода к проактивной парадигме. Особенно важно, что в 2024–2025 гг. принят ряд новых документов, которые конкретизируют требования

к средствам защиты информации (СЗИ), их интеграции в АИС КИИ и использованию передовых методов анализа. Однако между абстрактными требованиями регулятора и конкретными инженерно-техническими решениями существует методологический разрыв, связанный с отсутствием формализованных подходов к анализу данных. Настоящая статья развивает результаты предшествующего исследования авторов, посвящённого обзору подходов проактивного реагирования на инциденты в сетевом оборудовании с применением искусственного интеллекта [17], распространяя предложенную методологию на весь спектр АИС КИИ с учётом требований отечественной НПБ.

Целью данной работы является построение методологического моста между требованиями НПБ РФ и практикой построения систем проактивного мониторинга АИС КИИ через:

1. Системный анализ эволюции НПБ с акцентом на проактивность, включая новые акты 2024–2025 гг.По состоянию на начало 2026 года к числу актуальных актов добавились: Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (вступает в силу 01.03.2026); Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов КИИ, утверждённая ФСТЭК России 11.11.2025; редакция Приказа ФСТЭК России № 239, введённая Приказом № 159 от 28.08.2024. Все указанные документы размещены на официальном сайте ФСТЭК России [7, 8, 12].

2. Формализацию системы измеримых метрик безопасности.

3. Разработку архитектуры гибридной аналитической модели.

В настоящей работе под **таксономией инцидентов** понимается иерархическая классификация возможных нарушений безопасности или сбоев в работе АИС КИИ, структурированная по причинам, воздействию и требуемым методам проактивного обнаружения. Она служит основой для построения модели угроз на этапе планирования (этапа планирования (Plan)) и позволяет целесообразно выбирать методы из гибридного контура реагирования.

1. Анализ нормативно-правовой базы в контексте проактивности

1.1. Эволюция требований: от констатации к предупреждению

Эволюция НПБ РФ демонстрирует четкий вектор ужесточения и конкретизации требований, создающий правовую основу для проактивных мер.

- ФЗ-149 «Об информации, информационных технологиях и о защите информации» от 27.07.2006 [1] заложил базовые понятия, но носил рамочный характер, не затрагивая специфику КИИ.
- ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 (зарег. в Минюсте России) [2] стал поворотным пунктом, введя ключевое понятие «критическая информационная инфраструктура» (КИИ) и установив цель — «устойчивое функционирование». Статья 8 прямо обязывает субъектов КИИ «принимать меры по предупреждению компьютерных инцидентов», формируя юридический императив для проактивности.
- Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 28.08.2024, Приказ № 159) «Об утверждении Требований по обеспечению

безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [7] детализирует положения ФЗ-187. Ключевые для проактивности пунктам: обеспечение безопасности в ходе эксплуатации, включая реагирование на компьютерные инциденты (п. 13.5) и комплекс мер по их выявлению (меры ИНЦ.1–ИНЦ.5 Приложения к Приказу). Сроки информирования ГосСОПКА — не позднее 3 часов с момента обнаружения для ЗОКИИ — установлены Приказом ФСБ России от 19.06.2019 № 282 (п. 8).

- Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 15.03.2021) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [4] регулирует защиту информации в АСУ ТП на критически важных объектах, предписывает автоматическое обнаружение компьютерных атак и контроль целостности, что является прямым мандатом на внедрение SIEM (система управления событиями и инцидентами безопасности), EDR (средство обнаружения угроз и реагирования на конечных узлах) и PAM (система управления привилегированным доступом).

1.2. Документы ФСТЭК России: от базовых требований к проактивным мерам

Нормативное поле в области защиты КИИ продолжает активно развиваться. Ниже представлены ключевые акты ФСТЭК России, формирующие основу проактивного мониторинга АИС КИИ.

- Приказ ФСТЭК России от 21.12.2017 № 235 (ред. от 20.04.2023) «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (зарег. в Минюсте 22.02.2018, рег. № 50118) [6]. Устанавливает организационную структуру систем безопасности: требования к составу и полномочиям подразделений, планированию мероприятий и взаимодействию с ГосСОПКА. Ключевое для проактивности положение — обязательное создание подразделений (или назначение должностных лиц), ответственных за непрерывный мониторинг защищённости.
- Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 28.08.2024, Приказ № 159) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (зарег. в Минюсте 26.03.2018, рег. № 50524) [7]. Детализирует положения ФЗ-187. Ключевые для проактивности пункты: требование обеспечения безопасности в ходе эксплуатации, включая «реагирование на компьютерные инциденты» (п. 13.5) и меры по их выявлению (меры ИНЦ.1–ИНЦ.5 Приложения к Приказу). Сроки информирования ГосСОПКА — не позднее 3 часов с момента обнаружения для ЗОКИИ — установлены Приказом ФСБ России от 19.06.2019 № 282 (п. 8).
- Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 15.03.2021) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (зарег. в Минюсте 30.06.2014, рег. №

32919) [4]. Предписывает автоматическое обнаружение компьютерных атак и контроль целостности — прямой мандат на внедрение SIEM, EDR и PAM.

- Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов КИИ (утв. ФСТЭК России 02.05.2024, акт. 11.11.2025) [12]. Методический документ (не нормативный приказ), но обязателен при оценке защищённости субъектов КИИ. Вводит количественный показатель КЗИ и порядок его расчёта, включая метрики MTTD (среднее время обнаружения угрозы; англ. Mean Time To Detect) и MTTR (среднее время реагирования и устранения; англ. Mean Time To Respond/Remediate) и полноты охвата мониторингом. Формирует измеримую основу для KPI (ключевые показатели эффективности; англ. Key Performance Indicators) в области ИБ.
- Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (зарег. в Минюсте 14.05.2013, рег. № 28375) [5]. Регулирует защиту ПДн в ИСПДн (ФЗ-152) [3]; при пересечении с КИИ применяется параллельно с Приказом № 239. Меры, релевантные для проактивного мониторинга: обязательный аудит (РСБ), СОВ и антивирусная защита.
- Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (зарег. в Минюсте 16.06.2025, рег. № 82619; вступает в силу 01.03.2026) [8]. Пункт 48 устанавливает

требования к управлению привилегированным доступом: МФА, персонификация учётных записей, полный аудит сессий — нормативная основа для PAM-систем с интеграцией в SIEM. Применяется к ГИС; при пересечении с КИИ — совместно с Приказом № 239.

- Обновление Банка данных угроз безопасности информации ФСТЭК России (БДУ ФСТЭК, декабрь 2025 г.). Реестр: [13]. Впервые внесены угрозы для систем ИИ: кража ML-моделей, data poisoning, adversarial attacks, промпт-инъекции. Субъекты КИИ обязаны учитывать их при моделировании угроз. Приказ № 117 (п. «т» раздела 34) дополнительно вводит мероприятие «защита информации при использовании ИИ»: запрет внешних ИИ-сервисов для обработки информации ограниченного доступа.

1.3. Документы ФСБ России: криптографическая защита и управление доступом

Требования ФСБ России дополняют нормативную базу ФСТЭК в части криптографической защиты информации и использования сертифицированных СКЗИ. Совместный приказ ФСБ/ФСТЭК приведён здесь как документ смежного действия.

- Совместный приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31.08.2010 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования» (зарег. в Минюсте 13.10.2010, рег. № 18704). Текст на сайте ФСТЭК: [9]. Остаётся базовым для объектов КИИ, обрабатывающих ПДн, и устанавливает требования к применению сертифицированных СЗИ.
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости» (зарег. в Минюсте 18.08.2014, рег. № 33620). Текст: [10]. Предписывает обязательное использование отечественных СКЗИ и систем обнаружения вторжений (СОВ) на критических границах сети, задавая архитектурный шаблон для проактивного анализа трафика.

1.4. Методологический прорыв: ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» [11] выполняет ключевую методологическую функцию. Он впервые на уровне НПБ вводит и определяет понятие «проактивного контроля» как деятельность, направленную на выявление и предотвращение инцидентов до момента их совершения на основе анализа рискованного поведения и отклонений от нормальных шаблонов. Данное определение создаёт прецедент и понятийный аппарат для распространения проактивного подхода на все объекты КИИ.

1.5. Выявленные «белые пятна» и требование к математической формализации

Несмотря на прогрессивность и конкретизацию НПБ, остаются области, требующие дальнейшей методологической проработки:

1. **Отсутствие формализованных моделей анализа.** Требования к «обнаружению» и «мониторингу» не конкретизируют

математический аппарат. Для выполнения этих требований необходима формализация применения:

- Статистических моделей временных рядов (ARIMA (модель авторегрессии — проинтегрированного скользящего среднего; англ. AutoRegressive Integrated Moving Average), экспоненциальное сглаживание).
- Методов машинного обучения без учителя (Isolation Forest, one-class SVM).
- Графовых моделей для анализа взаимодействий в сети.

2. **Дефицит нормативов на прогнозирование.** Фокус на уже произошедших инцидентах; методики предиктивного техобслуживания (Predictive Maintenance) для ИБ-инфраструктуры не отражены.
3. **Неопределенность с автоматизацией работы с индикаторами.** Не регламентированы алгоритмы автоматизированного сопоставления телеметрии с индикаторами компрометации и поведения.

2. Формализованная система метрик и индикаторов для проактивного мониторинга

Безопасность АИС КИИ должна быть измерима. На основе требований НПБ РФ (ФЗ-187, приказы ФСТЭК №239, №31, №235) и лучших международных практик (NIST CSF (Система управления кибербезопасностью Национального института стандартов и технологий США), MITRE ATT&CK (база знаний тактик и техник атак; англ. Adversarial Tactics, Techniques, and Common Knowledge)) [14, 15] предлагается иерархическая система метрик. Данная система не только служит для контроля, но и формирует основу входных данных (признаков (features — входных переменных модели машинного обучения)) для

гибридной математической модели, классифицируя их по уровням мониторинга и типу математической обработки.

2.1. Иерархия метрик и их связь с гибридной моделью

Предлагаемая система классифицирована по пяти уровням мониторинга. Каждый уровень содержит не менее семи метрик с формализованными порогами, нормативными ссылками и рекомендуемыми методами анализа в рамках гибридной математической модели.

I. Аппаратный уровень (Уровень 1) — Основа для предиктивного анализа

Назначение: Охватывает физическую инфраструктуру АИС КИИ: серверы, системы хранения, сетевое оборудование и источники питания. Задача — непрерывный сбор телеметрии (SMART (технология самодиагностики накопителей; англ. Self-Monitoring Analysis and Reporting Technology), IPMI (интерфейс управления аппаратной платформой; англ. Intelligent Platform Management Interface), SNMP (простой протокол управления сетью; англ. Simple Network Management Protocol)) для предсказания и предотвращения аппаратных отказов до их наступления.

Угрозы: Деградация и катастрофический отказ компонентов, компрометация прошивок BMC/BIOS (контроллер управления материнской платой / базовая система ввода-вывода; англ. Baseboard Management Controller / Basic Input-Output System), атаки через цепочку поставок (Supply Chain-атаки) на встроенное ПО оборудования.

Нормативное основание: ФЗ-187 (устойчивое функционирование); Приказ ФСТЭК №239, меры АУД.7 Приложения (мониторинг безопасности); Приказ ФСТЭК №31, меры ОЦЛ.1, ОЦЛ.2 Приложения 2 (контроль целостности ПО и прошивок).

Методы анализа: Статистическое прогнозирование временных рядов: ARIMA, ETS, EWMA (экспоненциально взвешенное скользящее среднее; англ. Exponentially Weighted Moving Average), CUSUM (метод кумулятивных сумм для обнаружения изменений; англ. Cumulative Sum), контрольные карты Шухарта.

Таблица 1. Иерархия метрик аппаратного уровня

№	Метрика	Источник данных	Порог аномалии	Норм. ссылка	Метод анализа
1.1	Динамический коэффициент MTBF (среднее время наработки на отказ; англ. Mean Time Between Failures) дискового массива	SMART-логи, SNMP, RAID-контроллер (контроллер массива независимых дисков; англ. Redundant Array of Independent Disks)	Расчётный MTBF снизился более чем на 25% от паспортного значения за последние 30 дней	ФЗ-187; Пр. ФСТЭК №239, п. 13.3.е	ARIMA / ETS — тренд деградации
1.2	Интенсивность ошибок коррекции (ECC (память с коррекцией ошибок; англ. Error-Correcting Code)) памяти	IPMI, BMC	Более 50 исправимых ошибок ECC в час на модуль, либо любая неисправимая ошибка	Пр. ФСТЭК №239, п. 13.3.е	CUSUM — контроль устойчивого сдвига
1.3	Температура процессора / чипсета	IPMI, SNMP, датчики iDRAC	$T > (T_{max} - 10°C)$ в течение ≥ 15 мин	Пр. ФСТЭК №31 (ОЦЛ.1, ЗТС Прил.2)	Экспоненц. сглаживание (EWMA)
1.4	Деградация производительности дисков (латентность I/O)	SMART, iostat, агент мониторинга	P95-латентность I/O выросла более чем в 2 раза от базового значения в	ФЗ-187 (устойчивое функционирование)	ARIMA + правило 3σ

			течение ≥ 1 часа		
1.5	Состояние блока питания (PSU fault events)	IPMI, Redfish (современный интерфейс управления серверным оборудованием), BMC-лог	Любое событие PSU_FAULT или потеря резервирования питания	Пр. ФСТЭК №239, п. 13.3.е	Детерм. правило + сигнализация
1.6	Целостность прошивки BMC/BIOS (хэш-контроль)	TPM (доверенный платформенный модуль; англ. Trusted Platform Module), лог Secure Boot (безопасная загрузка), SIEM	Хэш прошивки BMC/BIOS не совпадает с эталонным значением в TPM	Пр. ФСТЭК №31, меры ОЦЛ.1, ОЦЛ.2 Прил.2	Сигнатурный анализ (детерм.)
1.7	Износ SSD (твердотельный накопитель; англ. Solid State Drive) (Wear Leveling Count)	SMART атрибут 177/233	Атрибут Wear Leveling Count опустился ниже 10% от начального значения	ФЗ-187; Пр. №239, п. 13.3.е	Регрессионная модель тренда

II. Сетевой уровень (Уровень 2) — Основа для обнаружения компрометации

Назначение: Анализирует трафик и сетевую активность внутри периметра АИС КИИ и на его границах. Основная задача — обнаружение IoC (индикаторы компрометации; англ. Indicators of Compromise) и IoB (индикаторы поведения; англ. Indicators of Behavior) в высокоскоростных и высокоразмерных потоках данных в режиме реального времени.

Угрозы: Горизонтальное сканирование и разведка, C2-коммуникации вредоносного ПО (периодическую отправку маяков (beaconing)), DGA-

активность (генерация доменных имён по алгоритму; англ. Domain Generation Algorithm) ботнетов, туннелирование данных через DNS/ICMP (система доменных имён / протокол управляющих сообщений; англ. Domain Name System / Internet Control Message Protocol), утечка данных через нетипичные маршруты.

Нормативное основание: Приказ ФСТЭК №31, меры ЗИС.2 (защита периметра), ЗИС.4 (сегментирование), ЗИС.19 (защита при передаче) Приложения 2; Приказ ФСБ №378 (мониторинг трафика при подключении к сети Интернет).

Методы анализа: ML без учителя: Isolation Forest, One-Class SVM (метод опорных векторов для одноклассовой классификации аномалий; англ. One-Class Support Vector Machine) для многомерных потоков; статистический анализ распределения Пуассона для всплесков; энтропийный анализ.

Таблица 2. Иерархия метрик сетевого уровня

№	Метрика	Источник данных	Порог аномалии	Норм. ссылка	Метод анализа
2.1	Энтропия DNS-запросов хоста (DGA-детекция)	сенсоры NTA/NDR (анализ сетевого трафика / обнаружение и реагирование на угрозы в сети; англ. Network Traffic Analysis / Network Detection and Response), лог DNS-сервера	Энтропия Шеннона DNS-запросов хоста выросла более чем на 3σ от базового профиля в течение ≥ 5 мин	Пр. ФСТЭК №31	Isolation Forest / One-Class SVM

2.2	Кардинальность исходящих подключений (уник. IP:порт)	NetFlow/IPFIX (протоколы передачи данных о сетевых потоках; англ. NetFlow / IP Flow Information Export), EDR-агенты	Более 500 уникальных исходящих подключений в час для рабочей станции; более 2000 — для сервера приложений	Пр. ФСТЭК №31	Пуассон-анализ всплесков
2.3	Объём исходящего трафика в нетипичные геолокации	NetFlow, NTA, Firewall-лог	Объём исходящего трафика в нетипичные геолокации вырос более чем на 3σ от 30-дневного базового профиля	Пр. ФСБ №378; Пр. ФСТЭК №31	ARIMA + Isolation Forest
2.4	Частота аномальных ARP/ICMP-пакетов (сканирование)	IDS/IPS (системы обнаружения и предотвращения вторжений; англ. Intrusion Detection System / Intrusion Prevention System), межсетевые экраны, NDR	Более 1000 ARP-запросов в минуту с одного хоста, либо широковещательный шторм	Пр. ФСТЭК №31	Пуассон + детерминированное правило
2.5	Использование нестандартных портов для HTTPS/HTTP	Firewall, DPI (глубокая инспекция пакетов; англ. Deep Packet Inspection), NetFlow	Более 10 SSL/TLS-соединений в час на порту, отличном от 443 и 80	Пр. ФСБ №378 (мониторинг тр-ка)	One-Class SVM + анализ TLS-метаданных

2.6	Латеральные NetBIOS/SMB (сетевой базовый интерфейс ввода-вывода / протокол совместного использования файлов и ресурсов; англ. Network Basic Input/Output System / Server Message Block)-подключения внутри сегмента	EDR, NetFlow, SIEM	Обращение к более чем 5 уникальным хостам в минуту по SMB от одной учётной записи	Пр. ФСТЭК №239 (ИНЦ)	Графовые модели аномальных путей
2.7	Детектирование туннелирования (DNS/ICMP tunneling)	NDR, DNS-лог, NTA	DNS-пакеты размером более 512 байт в сочетании с нетипичным TTL (время жизни пакета; англ. Time To Live) и высокой энтропией содержимого	Пр. ФСТЭК №31; ФЗ-187	ML-классификатор + энтропийный анализ

III. Программный/Хостовой уровень (Уровень 3) — Основа для детектирования вредоносной активности

Назначение: Сосредоточен на телеметрии процессов, файловой системы и вызовов API непосредственно на хосте. Выявляет эксплуатацию уязвимостей, техники использования штатных инструментов ОС в

злоумышленных целях (Living-off-the-Land) техники, инъекции кода и несанкционированные изменения конфигурации.

Угрозы: Эксплуатация уязвимостей инфраструктурных компонентов и конфигурации, инъекция кода в легитимные процессы, закрепление в системе через автозагрузку, отключение средств защиты.

Нормативное основание: Приказ ФСТЭК №239 (ИНЦ) (меры по обнаружению компьютерных инцидентов); требования ФСТЭК к управлению обновлениями.

Методы анализа: Комбинация детерминированных правил (сигнатуры, белые списки процессов) с поведенческим анализом на основе телеметрии EDR и Sysmon; Isolation Forest на деревьях процессов.

Таблица 3. Иерархия метрик программного уровня

№	Метрика	Источник данных	Порог аномалии	Норм. ссылка	Метод анализа
3.1	Время жизни критической уязвимости (Time-to-Patch)	SIEM (WSUS/SCCM (служба обновления Windows / система управления конфигурацией; англ. Windows Server Update Services / System Center Configuration Manager) + БД уязвимостей)	Критическая уязвимость (CVSS (система оценки уязвимостей; англ. Common Vulnerability Scoring System) ≥ 9.0) не устранена в течение более 72 часов; уязвимость с CVSS 7.0–8.9 — более 30 дней	Требования ФСТЭК к обновлениям	Детерм. правило + оценка риска (CVSS × экспозиция)
3.2	Частота аномальных вызовов API (инъекция кода)	EDR-агенты, Sysmon (Event 8)	Более 3 уникальных процессов в минуту на одном хосте вызывают	Пр. ФСТЭК №239 (ИНЦ)	Сигнатуры (белые списки) +

			CreateRemoteThread в чужие процессы		подсчёт частот
3.3	Изменения в автозагрузке и планировщике задач	Sysmon (Event 12/13), EDR, SIEM	Любое изменение ключей Run/RunOnce или создание новой задачи в планировщике вне процесса управления изменениями	Пр. ФСТЭК №239, п. 13.3.е	Детерм. правило + контроль целостности
3.4	Аномальное порождение процессов (Process Tree)	EDR (Sysmon Event 1), SIEM	Цепочка порождения: Office/браузер → cmd/PowerShell → сетевой процесс	Пр. ФСТЭК №239 (ИНЦ)	Isolation Forest на деревьях процессов
3.5	Изменения привилегированных групп AD (AdminSDHolder)	SIEM (логи AD, Event 4728/4732)	Любое добавление учётной записи в группу Domain Admins вне утверждённого процесса IAM	Пр. ФСТЭК №31 (УПД Прил.2); №239	Детерм. правило + уведомление SOAR
3.6	Несанкционированный запуск интерпретаторов (Living-off-the-Land)	EDR, Sysmon Event 1/11, SIEM	Запуск PowerShell с флагом -enc, wscript или mshta из пользовательского процесса	Пр. ФСТЭК №239 (ИНЦ)	Сигнатурный анализ + TF-IDF (метод взвешивания частоты слова; англ. Term Frequency — Inverse Document Frequency) командных строк
3.7	Отключение или изменение	EDR (антивирус),	Любое событие отключения антивируса или	Пр. ФСТЭК	Детерм. правило +

	настроек средств защиты	лог СЗИ, SIEM	изменения политики СЗИ	№239, п. 13.3.е	эскалация инцидента

IV. Пользовательский уровень (Уровень 4) — Основа для обнаружения APT и инсайдерских угроз

Назначение: Строит индивидуальные поведенческие профили пользователей и анализирует отклонения в их активности: нетипичное время работы, скорость латерального перемещения, массовый доступ к данным. Требует долгосрочного накопления базового профиля (90+ дней).

Угрозы: Латеральное перемещение скомпрометированных учётных записей, инсайдерские угрозы (кража/утечка данных), атаки на привилегированных пользователей, использование скомпрометированных сервисных учётных записей.

Нормативное основание: Приказ ФСТЭК №31 (контроль доступа); Пр. ФСТЭК №117, п. 48 (управление привилег. доступом); Пр. ФСТЭК №239 (ИНЦ).

Методы анализа: UEBA (анализ поведения пользователей и объектов; англ. User and Entity Behavior Analytics): One-Class SVM, Гауссовы смеси (GMM (модель гауссовой смеси; англ. Gaussian Mixture Model)) для моделирования индивидуальной нормы; графовые модели для анализа аномальных путей доступа; LSTM на временных рядах активности.

Таблица 4. Иерархия метрик пользовательского уровня

№	Метрика	Источник данных	Порог аномалии	Норм. ссылка	Метод анализа

4.1	Скорость латерального перемещения учётной записи	SIEM (логи AD, Kerberos, Event 4624)	Доступ к 3 и более различным сетевым сегментам за 10 минут при нетипичном профиле пользователя	Пр. ФСТЭК №31; №239 (ИНЦ)	Графовые модели аном. путей в сети доступа
4.2	Аномальность времени активности пользователя	Логи IAM-систем, AD (Event 4624)	Время сессии отклонилось более чем на 2.5σ от персонального 90-дневного поведенческого профиля	Пр. ФСТЭК №31 (контроль доступа)	One-Class SVM / Гауссовы смеси (GMM)
4.3	Массовый доступ к файловым ресурсам (подготовки данных к exfiltration (Data Staging))	SIEM (аудит FS, DLP, EDR)	Более 500 уникальных файлов в минуту, либо объём скопированных данных превысил 1 ГБ за 5 минут	Пр. ФСБ №489 (защита ПДн); ФЗ-187	LSTM на временных рядах активности + порог
4.4	Нетипичное использование привилегированных учётных записей	PAM-система, SIEM	Вход привилегированной учётной записи в нерабочее время или с нового хоста	Пр. ФСТЭК №117, п.48; Пр. ФСТЭК №239	UEBA-профиль + One-Class SVM
4.5	Многократные неудачные аутентификации (Brute Force / Spray)	SIEM (Event 4625, 4771), AD	Более 5 неудачных попыток в минуту с разных IP, либо попытки перебора по более чем 20 учётным записям	Пр. ФСТЭК №239, п. 13.3.е	Детерм. правило + кластеризация по IP/времени
4.6	Изменение паролей сервисных учётных записей вне расписания	IAM, PAM, SIEM (Event 4723/4724)	Любое изменение пароля сервисной учётной записи вне утверждённого окна обслуживания	Пр. ФСТЭК №117, п.48; Пр. ФСТЭК №31	Детерм. правило + корреляция с CR-системой
4.7	Использование устаревших протоколов	SIEM, NDR (детектор	Любой NTLMv1 или WDigest-запрос в	Пр. ФСТЭК №31	Детерм. сигнатура +

	аутентификации (NTLMv1 (устаревший протокол аутентификации Windows версии 1; англ. NT LAN Manager v1), WDigest (устаревший провайдер проверки подлинности Windows))	протоколов)	продуктивной среде	(ЗИС.20 Прил.2)	обогащение из TI

V. Контекстный уровень угроз (Уровень 5) — Основа для проактивного обнаружения и оценки инцидентов

Назначение: Интегрирует данные внешней киберразведки (Threat Intelligence — разведка киберугроз: бюллетени ГосСОПКА, платформа MISP (открытая платформа обмена индикаторами угроз; англ. Malware Information Sharing Platform) и коммерческие TIP (платформа анализа киберугроз; англ. Threat Intelligence Platform)-источники) с внутренней телеметрией всех нижележащих уровней. Позволяет сопоставлять события с известными IoC и профилями APT-группировок (группировок постоянных целенаправленных угроз; англ. Advanced Persistent Threat).

Угрозы: Целевые кибератаки известных APT-группировок, C2-инфраструктура (инфраструктура управления и контроля вредоносного ПО; англ. Command and Control), активные эксплойты для незакрытых уязвимостей, Supply Chain-атаки через скомпрометированные обновления ПО.

Нормативное основание: Приказ ФСТЭК №239 (ИНЦ) (взаимодействие с ГосСОПКА); ФЗ-187, ст. 9 (информирование о компьютерных инцидентах).

Методы анализа: Детерминированное сопоставление (сигнатурный анализ IoC); корреляция событий с картами MITRE ATT&CK; графовые модели знаний для выявления скрытых связей между внутренними активами и внешними рискованными объектами.

Таблица 5. Иерархия метрик контекстного уровня

№	Метрика	Источник данных	Порог аномалии	Норм. ссылка	Метод анализа
5.1	Совпадение IoC с внутренней активностью (хэш/IP/домен)	SIEM + TIP (ГосСОПКА, MISP)	Любое совпадение внутренней активности с IoC (хэш, IP-адрес, домен) из доверенного TI-источника	Пр. ФСТЭК №239 (ИНЦ); ФЗ-187	Сигнатурный анализ + обогащение контекстом TTП
5.2	Анализ репутации и геолокации внешних хостов	TIP, VirusTotal (онлайн-сервис проверки файлов и URL), AbuseIPDB (база данных репутации IP-адресов), NetFlow	Установление соединения с хостом с репутацией ниже 20 из 100, либо расположенным в геолокации, нетипичной для бизнеса организации	Пр. ФСТЭК №31; ФЗ-187	Корреляция NetFlow + дин. списки репутации
5.3	Совпадение поведенческих паттернов с TTП APT (MITRE ATT&CK)	SIEM, EDR, TIP (профили группировок)	Обнаружение 3 и более техник из одной APT-кампании в течение 24 часов	Пр. ФСТЭК №239 (ИНЦ); ФЗ-187	Граф знаний ATT&CK + корреляция событий SIEM
5.4	Обнаружение C2-коммуникаций (Beaconing)	NDR, NTA, прокси-логи	Периодичность исходящих соединений с коэффициентом вариации CV < 0.1 при более чем 10	Пр. ФСБ №378; Пр. ФСТЭК №31	Статистика интервалов + Isolation Forest

			попытках подряд		
5.5	Корреляция уязвимостей системы с активными эксплойтами в TI	SIEM (WSUS/SCCM) + TIP (ExploitDB (база данных эксплойтов), NVD (национальная база данных уязвимостей США; англ. National Vulnerability Database))	Наличие известного активного эксплойта для уязвимости, которая не устранена на защищаемом хосте	Требования ФСТЭК к обновлениям; ФЗ-187	Детерм. матчинг CVE (банк общеизвестных уязвимостей; англ. Common Vulnerabilities and Exposures) × активность эксплойта
5.6	Детектирование Supply Chain IoC (хэши подозр. обновлений ПО)	TIP, EDR (хэши файлов), SIEM	Хэш полученного обновления ПО совпадает с известными Supply Chain IoC из TI-источников	ФЗ-187; Пр. ФСТЭК №239, п. 13.3.е	Сигнатурный + целостностный контроль
5.7	Аномалии в потоках ГосСОПКА (время реакции на Бюллетень)	SIEM, система тикетов, НПА-трекер	Отсутствие реакции на бюллетень ГосСОПКА в течение более 24 часов	Пр. ФСТЭК №239 (ИНЦ); ФЗ-187	Детерм. правило + эскалация через SOAR

Рисунок 1. Пятиуровневая иерархия метрик

3. Предполагаемая схема гибридного проактивного контура реагирования на инциденты АИС КИИ

Данный раздел формализует архитектурное решение, связывающее нормативно-правовую базу, систему метрик и математические методы в единый замкнутый контур управления безопасностью. Предлагаемая модель строится на принципе «гибридности», под которым понимается синергетическое совместное использование трёх классов методов: детерминированных моделей на основе правил НПБ и сигнатур — для реагирования на известные угрозы; стохастических и статистических моделей прогнозирования — для выявления трендов и отклонений; а также

моделей машинного обучения — аномалийного и поведенческого — для обнаружения сложных, неизвестных и многошаговых угроз.

Архитектурной основой контура служит цикл НОРД (Наблюдение — Ориентирование — Решение — Действие), встроенный в требования НПБ и использующий формализованные метрики раздела 2. Цикл НОРД применительно к задачам проактивного мониторинга АИС КИИ предполагает четыре последовательных и непрерывно повторяющихся этапа:

1. **Наблюдение (Н) —** непрерывный многослойный сбор телеметрии со всех уровней иерархии метрик — от аппаратных показателей до потоков разведки об угрозах.
2. **Ориентирование (О) —** анализ и интерпретация собранных данных с применением гибридных математических методов: статистического прогнозирования, детерминированной корреляции и моделей машинного обучения.
3. **Решение (Р) —** формирование решения об инциденте: классификация угрозы, определение её стадии по матрице MITRE ATT&CK и выбор сценария реагирования.
4. **Действие (Д) —** автоматизированное оркестрированное реагирование, информирование регулятора через ГосСОПКА и адаптация модели по результатам расследования инцидента.

3.1. Многослойный сбор и обогащение телеметрии (Наблюдение)

Первый этап цикла НОРД реализует непрерывный и структурированный сбор данных в соответствии с пятиуровневой иерархией

метрик. Каждый уровень иерархии соответствует собственному технологическому слою сбора, что обеспечивает полноту покрытия АИС КИИ и возможность межуровневой корреляции событий.

На аппаратном уровне телеметрия собирается посредством протоколов IPMI, Redfish и SNMP, охватывая показатели дисковых массивов, памяти, температурных датчиков и источников питания. Сетевой уровень обеспечивается сенсорами NDR и потоками NetFlow/IPFIX, а также данными межсетевых экранов. Хостовый уровень формируется на основе агентов EDR, журналов Sysmon и системных логов операционных систем. Пользовательский уровень агрегирует данные из IAM-систем (систем управления идентификацией и доступом; англ. Identity and Access Management), Active Directory (служба каталогов Microsoft) и прокси-серверов. Контекстный уровень обогащается потоками из платформ Threat Intelligence — ГосСОПКА, MISP и коммерческих TIP-источников, — которые придают событиям внутренней инфраструктуры контекст внешней угрозы.

Принципиально важным условием является не только полнота сбора, но и единообразие форматов данных. Все СЗИ, интегрируемые в контур мониторинга, должны предоставлять телеметрию в форматах, пригодных для автоматической корреляции и анализа, что прямо закреплено в нормативных требованиях к интеграции средств защиты в единую систему мониторинга и управления безопасностью.

3.2. Анализ и прогноз — ядро гибридной модели (Ориентирование)

Второй этап является ключевым в архитектуре контура: именно здесь применяется комплекс математических методов, преобразующий сырую телеметрию в классифицированные инциденты безопасности. Аналитическое ядро модели состоит из четырёх последовательно применяемых блоков.

Блок 1. Детерминированная корреляция (SIEM). На первом этапе анализа выполняются правила, напрямую соответствующие требованиям НПБ. Данный блок обеспечивает немедленное детектирование известных сценариев компрометации на основе жёстко заданных условий. Например, одновременное наступление событий «изменение привилегий», «внесение в автозагрузку» и «исходящее SSL-соединение» квалифицируется как инцидент согласно мерам ИНЦ.1–ИНЦ.5 Приложения к Приказу №239. Этот блок является обязательным компонентом любой системы мониторинга КИИ и обеспечивает базовое соответствие требованиям НПБ.

Блок 2. Статистико-прогнозный анализ. Второй блок применяет методы, назначенные метрикам уровней 1 и 2: ARIMA, контрольные карты Шухарта (CUSUM), анализ распределения Пуассона. На каждом шаге формируется прогноз нормального состояния системы на шаг t+1, что позволяет выявлять медленно развивающиеся аномалии — деградацию оборудования и постепенный дрейф показателей сетевой активности, — которые не поддаются обнаружению методами сигнатурного анализа.

Блок 3. Гибридная ML-модель для поведенческих аномалий. Ядром аналитического блока является архитектура «LSTM + Isolation Forest», предназначенная для комплексного анализа многомерных временных рядов. Сеть LSTM обучается на исторических данных нормальной работы системы, прогнозируя ожидаемый вектор метрик M_прогноз(t+1) с учётом долгосрочных зависимостей и циклических паттернов активности. Вычисляемый вектор остатков R(t+1) = M_факт(t+1) − M_прогноз(t+1) отражает величину отклонения от нормы. Алгоритм Isolation Forest анализирует этот вектор, выявляя точки, которые «легко изолировать» как аномальные. Двухэтапный подход является более робастным, чем анализ сырых значений метрик, поскольку нейтрализует влияние сезонных и циклических колебаний.

Блок 4. Тактико-технический анализ (MITRE ATT&CK). Завершающий аналитический блок выполняет кластеризацию и классификацию обнаруженных аномалий в тактики и техники матрицы MITRE ATT&CK. Это позволяет не только идентифицировать факт аномалии, но и определить стадию кибератаки — от разведки до воздействия, — что критически важно для приоритизации реагирования и оценки степени компрометации объекта КИИ.

3.3. Принятие решения об инциденте (Решение)

Третий этап цикла НОРД преобразует результаты аналитической модели в формализованное решение об инциденте. На основании совокупного вывода четырёх аналитических блоков для каждого выявленного события определяются его тип и категория в соответствии с таксономией инцидентов, стадия в цепочке кибератаки согласно матрице MITRE ATT&CK, приоритет реагирования, а также конкретный плейбук, подлежащий исполнению на этапе действия.

Принципиальным отличием гибридной модели от традиционных SIEM-подходов является то, что решение формируется не на основе единственного сигнала, а на основе консолидированного вывода всех блоков ориентирования. Это существенно снижает уровень ложноположительных срабатываний: событие квалифицируется как инцидент только при подтверждении аномалии несколькими независимыми методами анализа.

3.4. Реагирование и адаптация (Действие)

Четвёртый этап замыкает цикл НОРД, реализуя конкретные меры по нейтрализации угрозы и адаптации системы защиты. Реагирование осуществляется по трём взаимосвязанным направлениям.

Оркестрированное реагирование реализуется через SOAR-платформу (платформу оркестрации, автоматизации и реагирования на угрозы; англ.

Security Orchestration, Automation and Response), которая автоматически исполняет заранее подготовленные плейбуки на основе решения гибридной модели. Конкретный сценарий реагирования определяется типом и стадией угрозы: при детектировании инъекции кода выполняется изоляция хоста, при обнаружении аномального DNS блокируется соответствующее имя на уровне корпоративного резолвера. Интеграция с отечественными СЗИ и системами управления инфраструктурой является обязательным условием работоспособности контура в среде КИИ.

Информирование регулятора обеспечивается автоматической генерацией сообщений в ГосСОПКА в соответствии с требованиями Приказа ФСБ России от 19.06.2019 № 282 — не позднее 3 часов с момента обнаружения инцидента для значимых объектов КИИ. Автоматизация данного процесса является одним из ключевых практических преимуществ предлагаемой архитектуры.

Адаптация модели осуществляется через механизм обратной связи: результаты расследования завершённых инцидентов используются для дообучения ML-моделей на новых данных, корректировки порогов статистических методов и добавления новых детерминированных правил в SIEM. Таким образом, цикл НОРД является самосовершенствующимся: каждый расследованный инцидент повышает точность детектирования будущих угроз и снижает уровень ложноположительных срабатываний, замыкая контур управления безопасностью АИС КИИ.

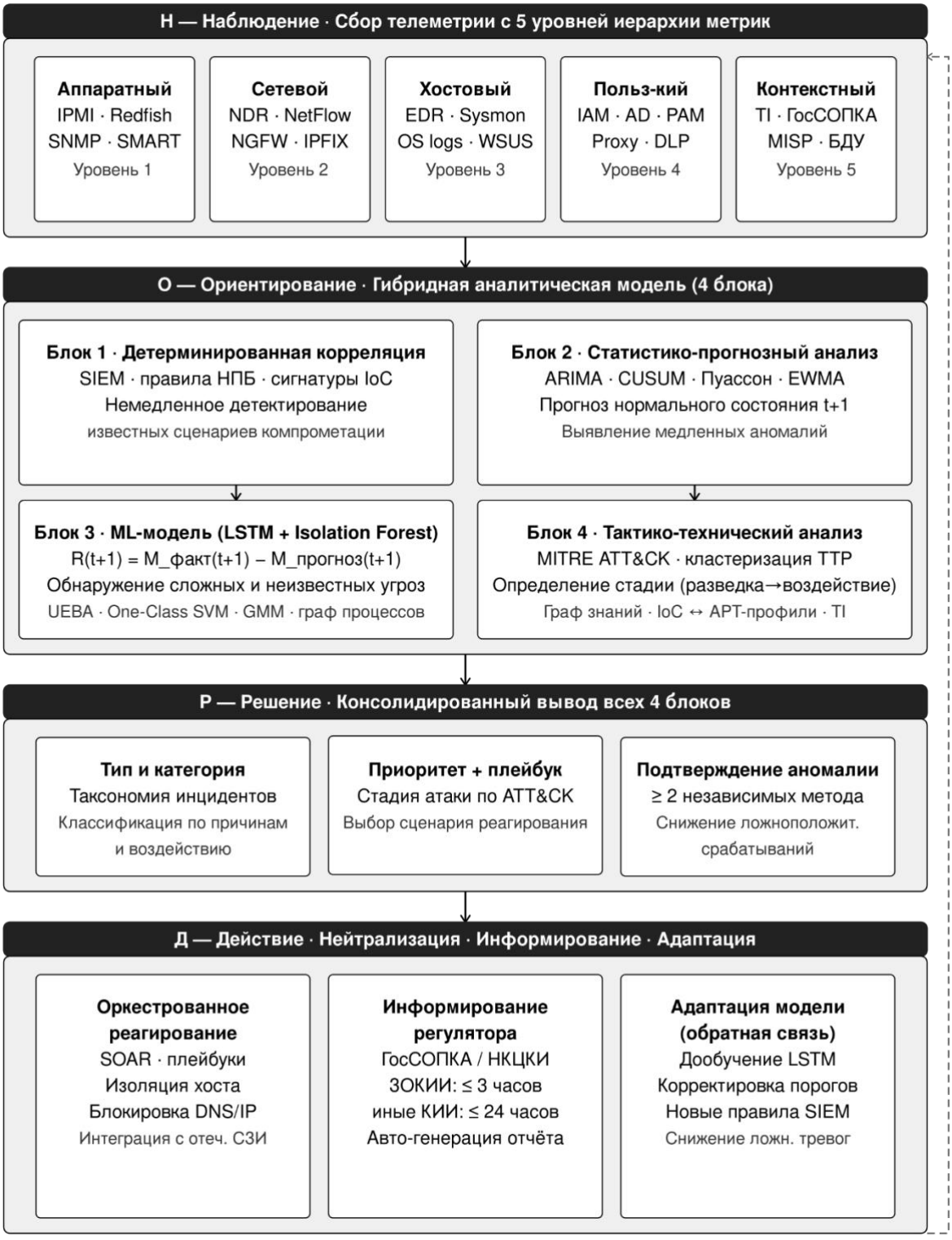

Рисунок 2. Архитектура гибридного проактивного контура НОРД

Заключение и перспективы

Формирование систем проактивного реагирования на инциденты АИС КИИ перестает быть вопросом технологического выбора и становится строгой необходимостью, диктуемой эволюцией нормативно-правовой базы Российской Федерации. Предложенная методология, интегрирующая детальный анализ НПБ, формализованную систему метрик, концептуальную схему и практические инструменты, представляет собой стратегию для интеграции методов проактивного реагирования инцидентов у субъектов КИИ.

Строгая формализация метрик формирует методологическую основу для разработки инструментальных средств систем проактивного реагирования на основе машинного обучения.

Ключевые тезисы:

1. НПБ РФ (ФЗ-187, приказы ФСТЭК) создает юридически обязывающие предпосылки для перехода к проактивной модели через требования к «предупреждению», «обнаружению» и «минимальным срокам реагирования».

2. Эффективная реализация этих требований невозможна без применения продвинутых методов анализа данных (ML, статистическое прогнозирование), что указывает на необходимость развития соответствующих методических рекомендаций ФСТЭК.

3. Технологический стек (SIEM (система управления событиями безопасности), EDR/XDR (обнаружение и реагирование на конечных узлах / расширенное обнаружение и реагирование; англ. Endpoint/Extended Detection and Response), SOAR (оркестрация и автоматизация реагирования), NDR (обнаружение и реагирование на сетевые угрозы; англ. Network Detection and Response)) является не набором отдельных продуктов,

а единой платформой, настраиваемой в соответствии с формализованными метриками и правилами, вытекающими из НПБ и модели угроз.

4. Ключ к успеху — в интеграции аппаратного, сетевого и прикладного мониторинга — включая межсетевые экраны нового поколения (NGFW (межсетевые экраны нового поколения; англ. Next-Generation Firewall)) как источник телеметрии и точку принудительного исполнения политик — с системами оркестрации и аналитики угроз, что позволяет перейти от реагирования на отдельные события к управлению сквозными сценариями кибератак и сбоев.

Перспективными направлениями дальнейших исследований являются: разработка стандартизированных профилей защиты (Protection Profiles (профили защиты — формализованные наборы требований безопасности)) для средств проактивного мониторинга в соответствии с требованиями ФСТЭК, создание отраслевых цифровых двойников АИС КИИ для безопасного тестирования сценариев атак и отработки реагирования, а также развитие национальной экосистемы обмена индикаторами компрометации (CTI (киберразведка на основе данных об угрозах; англ. Cyber Threat Intelligence)) в форматах, пригодных для автоматической загрузки в SIEM/SOAR-платформы.

Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. URL: https://eais.rkn.gov.ru/docs/149.pdf (дата обращения: 06.05.2026).
2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/zakony/federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения: 06.05.2026).
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс]. URL: https://base.garant.ru/12148567/ (дата обращения: 06.05.2026).
4. Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 15.03.2021) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 06.05.2026).
5. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-

dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 06.05.2026).

6. Приказ ФСТЭК России от 21.12.2017 № 235 (ред. от 20.04.2023) «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (дата обращения: 06.05.2026).
7. Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 28.08.2024) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 06.05.2026).
8. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117 (дата обращения: 06.05.2026).
9. Приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31.08.2010 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-31-avgusta-2010-g-n-489 (дата обращения: 06.05.2026).

10. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [Электронный ресурс]. URL: https://base.garant.ru/70727118/ (дата обращения: 06.05.2026).
11. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер [Электронный ресурс]. URL: https://itglobal.com/wp-content/uploads/2021/05/gost-57580.1-1.pdf (дата обращения: 06.05.2026).
12. Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: утв. ФСТЭК России 02.05.2024, актуализирована 11.11.2025 [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/item/3213 (дата обращения: 06.05.2026).
13. Банк данных угроз безопасности информации ФСТЭК России (БДУ ФСТЭК). Обновление: декабрь 2025 г. [Электронный ресурс]. URL: https://bdu.fstec.ru (дата обращения: 06.05.2026).
14. NIST Cybersecurity Framework (CSF) 2.0 [Электронный ресурс]. URL: https://www.nist.gov/cyberframework (дата обращения: 06.05.2026).

15. MITRE ATT&CK Enterprise Matrix [Электронный ресурс]. URL: https://attack.mitre.org (дата обращения: 06.05.2026).

16. Positive Technologies. CODE RED 2026: актуальные киберугрозы для российских организаций: аналитический отчет / PT Expert Security Center [Электронный ресурс]. URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/ (дата обращения: 18.04.2026).

17. Буркацкий К.А., Чаркин В.К., Сатановская Е.А. Обзор подходов проактивного реагирования на инциденты в сетевом оборудовании с применением искусственного интеллекта // Научно-практический электронный журнал «Аллея Науки». 2025. № 10(109) [Электронный ресурс]. URL: https://alley-science.ru/domains_data/files/Oct25/OBZOR-PODHODOV-PROaKTIVNOGO-REaGIROVaNIYa-Na-INTSIDENTI-V-SETEVOM-OBORUDOVaNII-S-PRIMENENIEM-ISKUSSTVENNOGO-INTELLEKTa.pdf (дата обращения: 19.04.2026).