НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2026 Том 26 № 3 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2026 Vol. 26 No 3 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2026-26-3-486-494
УДК 004.056; 004.89

# Большие данные в процессах обеспечения безопасности объектов критической информационной инфраструктуры

**Марина Юрьевна Толстых[1]✉, Павел Дмитриевич Коратаев[2]**

[1] Московский ордена Почета университет МВД России им. В.Я. Кикотя, Москва, 117997, Российская Федерация
[1] Московский государственный лингвистический университет, Москва, 119034, Российская Федерация
[2] Военно-учебный научный центр Военно-воздушных сил «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина», Воронеж, 394064, Российская Федерация

[1] marina_lion@mail.ru✉, https://orcid.org/0009-0001-2223-7709
[2] korataev2015@mail.ru, https://orcid.org/0009-0000-3634-2772

**Аннотация**

**Введение.** Исследована роль технологии больших данных в процессах обеспечения безопасности объектов критической информационной инфраструктуры (КИИ) Российской Федерации в условиях роста кибератак и цифровой трансформации. Актуализируется задача перехода от реактивной к проактивной модели защиты. Представлена разработка оригинальных направлений интеграции больших данных в системы безопасности КИИ: моделирования каскадных киберфизических инцидентов на графах межсистемных зависимостей, анализа «темных данных» промышленного оборудования как источника индикаторов компрометации, гибридной архитектуры федеративного обучения для межотраслевой кооперации субъектов КИИ без передачи конфиденциальных данных за периметр организации. **Метод.** Предложен математический аппарат построения resilient-систем безопасности, основанный на представлении киберфизической инфраструктуры в виде динамического взвешенного ориентированного временного мультиграфа с байесовским обновлением весов в реальном времени. Динамика распространения воздействий моделируется непрерывными цепями Маркова с поглощением, а оптимизация размещения средств защиты формализуется как стохастическая игра «защитник–атакующий» с поиском ε-приближенного равновесия Нэша методами обучения с подкреплением. Разработан двухэтапный итеративно-уточняющий алгоритм максимизации устойчивости при бюджетных, ресурсных и нормативных ограничениях. **Основные результаты.** Сформирован замкнутый data-driven контур проактивного управления безопасностью объектов КИИ, в котором потоки больших данных обеспечивают непрерывное обновление параметров модели и адаптацию защитных механизмов. Верификация подходов выполнена на цифровом двойнике фрагмента распределительной электросети с точностью классификации инцидентов 94,3 %. **Обсуждение.** В отличие от традиционных решений Security Information and Event Management и User and Entity Behavior Analytics, ориентированных на корреляцию известных событий, предложенный подход обеспечивает предиктивное моделирование киберфизических последствий атак с учетом межслойных зависимостей. Архитектура федеративного обучения позволяет формировать межотраслевые модели угроз без нарушения требований законодательства о защите информации. Перспективы применения разработанного подхода связаны с нормативным закреплением разработанных механизмов в качестве обязательных элементов систем безопасности на значимых объектах КИИ и созданием национальной платформы обмена обезличенными моделями угроз.

**Ключевые слова**

большие данные, критическая информационная инфраструктура, кибербезопасность, цифровая трансформация, resilient-системы

**Ссылка для цитирования:** Толстых М.Ю., Коратаев П.Д. Большие данные в процессах обеспечения безопасности объектов критической информационной инфраструктуры // Научно-технический вестник информационных технологий, механики и оптики. 2026. Т. 26, № 3. С. 486–494. doi: 10.17586/2226-1494-2026-26-3-486-494

# Big data in the processes of ensuring the security of critical information infrastructure facilities

**Marina Yu. Tolstykh[1]✉, Pavel D. Korataev[2]**

[1] Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, 117997, Russian Federation
[1] Moscow State Linguistic University, Moscow, 119034, Russian Federation
[2] Military Educational and Scientific Centre of the Air Force N.E. Zhukovsky and Y.A. Gagarin Air Force Academy, Voronezh, 394064, Russian Federation

[1] marina_lion@mail.ru✉, https://orcid.org/0009-0001-2223-7709
[2] korataev2015@mail.ru, https://orcid.org/0009-0000-3634-2772

**Abstract**

The role of big data technology in the processes of ensuring the security of objects of the critical information infrastructure (CII) of the Russian Federation in the context of increasing cyber-attacks and digital transformation is investigated. The task of moving from a reactive to a proactive protection model is being actualized. The scientific novelty of the research lies in the development of original directions for integrating Big Data into CII security systems: modeling cascading cyber-physical incidents on intersystem dependency graphs, analyzing the "dark data" of industrial equipment as a source of compromise indicators, and a hybrid architecture of federated learning for interdisciplinary cooperation of CII subjects without transferring confidential data beyond the organization perimeter. A mathematical apparatus for constructing resilient security systems is proposed, based on the representation of a cyber-physical infrastructure in the form of a dynamic weighted oriented time multigraph with Bayesian updating of weights in real time. The dynamics of impact propagation is modeled by continuous Markov chains with absorption, and optimization of the placement of protective equipment is formalized as a stochastic defender–attacker game with the search for an e-approximate Nash equilibrium using reinforcement learning methods. A two-stage iteratively refining algorithm for maximizing sustainability under budgetary, resource, and regulatory constraints has been developed. A closed data-driven loop of proactive security management of CII facilities has been formed, in which big data flows ensure continuous updating of model parameters and adaptation of protective mechanisms. Approach verification on a distribution grid digital twin demonstrated 94.3 % incident classification accuracy. Unlike traditional Security Information and Event Management and User and Entity Behavior Analytics solutions focused on the correlation of known events, the proposed approach provides predictive modeling of the cyber-physical consequences of attacks, taking into account interlayer dependencies. The architecture of federated learning allows for the formation of cross-industry threat models without violating the requirements of information protection legislation. The prospects for application are related to the regulatory consolidation of the developed mechanisms as mandatory elements of security systems at significant CII facilities and the creation of a national platform for the exchange of impersonal threat models.

**Keywords**

Big Data, critical information infrastructure, cybersecurity, digital transformation, resilient systems

**For citation:** Tolstykh M.Yu., Korataev P.D. Big data in the processes of ensuring the security of critical information infrastructure facilities. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2026, vol. 26, no. 3, pp. 486–494 (in Russian). doi: 10.17586/2226-1494-2026-26-3-486-494

## Введение

В текущих условиях геополитической обстановки особое внимание уделяется защите критической информационной инфраструктуры (КИИ) Российской Федерации (РФ), поскольку атаки на нее оказывают непосредственное влияние на национальную безопасность и интересы государства в ключевых отраслях. По данным пресс-службы Совета безопасности РФ[1] в 2025 году количество кибератак на КИИ увеличилось в четыре раза[2], по результатам анализа ландшафта киберугроз от компании «Positive Technologies» (Россия) и их прогнозов на 2026 год[3], стремительная цифровая трансформация входит в 5 ключевых драйверов кибератак на российские организации. Действительно, цифровизация, подразумевающая интеграцию передовых технологий, таких как искусственный интеллект, машинное обучение, сети пятого поколения, интернет вещей (Internet of Things, IoT) радикально трансформирует функционирование объектов КИИ, в том числе с точки зрения обеспечения их безопасности. С одной стороны, указанные технологии расширяют поверхность атак, усиливая уязвимости систем и сетей, с другой — предоставляют мощные инструменты для проактивной защиты, включая предиктивную аналитику, которая основывается на не менее значимой технологии цифровизации — больших данных.

В контексте обеспечения безопасности объектов КИИ больших данных может использоваться как инструмент обработки и анализа больших объемов разнородных данных, генерируемых в реальном времени. Технология позволяет не только аккумулировать сведения из различных источников (лог-файлы информационных и автоматизированных систем, в том числе автоматизированных систем управления технологическим процессом (АСУ ТП), информация с датчиков IoT-устройств, данные сетевого трафика), но и извлекать

[1] Атаки на КИИ выросли в четыре раза // RSpectr. URL: https://rspectr.com/novosti/ataka-na-kii-vyrosli-v-chetyre-raza (дата обращения: 11.12.2025).

[2] Хакерские атаки на критическую инфраструктуру в России участились в 4 раза // CISOCLUB. URL: https://cisoclub.ru/hakerskie-ataki-na-kriticheskuju-infrastrukturu-v-rossii-uchastilis-v-4-raza/ (дата обращения: 11.12.2025).

[3] CODE RED 2026: Актуальные киберугрозы для российских организаций / Positive Technologies. М., 2025. 149 с. URL: https://pt-corp.storage.yandexcloud.net/CODE_RED_2026_9685772206.pdf (дата обращения: 11.12.2025).

из них ценную информацию для выявления аномалий, прогнозирования угроз, выработки стратегий эффективной защиты объектов.

Целью настоящей работы является анализ роли больших данных как технологии цифровизации в процессах обеспечения безопасности объектов КИИ, а также разработка оригинальных решений для оптимизации указанных процессов. Актуальность исследования заключается в необходимости разработки инновационных подходов к цифровизации, позволяющих балансировать между уязвимостями и защитными возможностями цифрового инструментария, в том числе в условиях импортозамещения [1]. Исследование предлагает оригинальные оптимизационные стратегии и математические модели, отсутствующие в существующих отечественных научных и технических источниках, что способствует развитию объектов КИИ как resilient-систем[1] [2] в ключевых отраслях в соответствии с законом о безопасности КИИ. Исследование опирается на анализ отечественных нормативных и инструктивных документов, материалов российских разработчиков защитных решений, а также международных организаций, научных публикаций, что обеспечивает его объективность и определенную научную новизну.

## Некоторые векторы интеграции больших данных в процессы обеспечения безопасности объектов КИИ

Эффективность применения технологий больших данных в обеспечении безопасности объектов КИИ во многом определяется глубиной их интеграции в операционные процессы обнаружения, анализа и реагирования на инциденты, а также наличием оптимизационных механизмов, позволяющих минимизировать затраты и риски при сохранении требуемой производительности и соответствия нормативным требованиям. В дополнение к традиционным сценариям использования больших данных в целях обеспечения защиты объектов КИИ возможны менее очевидные подходы.

**Моделирование каскадных киберфизических инцидентов на графах межсистемных зависимостей (Cyber-Physical Dependency Graphs, CPDG) [3].** В отличие от традиционных статических карт топологии сети или схем АСУ ТП, графы киберфизических зависимостей представляют собой многослойные ориентированные графы с временной размерностью, в которых вершинами выступают не только сетевые устройства и хосты, но и технологические параметры, исполнительные механизмы, физические процессы и элементы внешней среды (например, температура окружающей среды, давление в магистрали и т. д.). Ребра графа отражают причинно-следственные, логические и временные зависимости между ними. В режиме близком к реальному времени поступают такие потоки данных, как: технологическая телеметрия Supervisory Control And Data Acquisition (SCADA) и АСУ ТП; события промышленных контроллеров; сетевой трафик промышленного сегмента; логи корпоративных систем, в том числе систем защиты информации (СЗИ); данные систем физической безопасности (контроля и управления доступом, видеонаблюдения, охранных и пожарных).

Типовая архитектура системы прогностического моделирования и упреждающего обнаружения каскадных киберфизических инцидентов на основе CPDG включает в себя следующие компоненты: слой сбора и первичной нормализации разнородных потоков данных; корпоративное озеро больших данных (Data Lake), содержащее «горячий» и «холодный» уровни [4]; графовая платформа временных мультиграфов; слой обработки и машинного обучения; инструменты оркестрации и оперативного принятия решений; слой визуализации и интерфейс оператора.

На построенном графе могут решаться следующие задачи в реальном времени. С помощью модифицированных алгоритмов поиска в ширину с весами критичности ребер возможно моделировать пути атаки от первоначальной точки до критичных технологических узлов. При поступлении сигнала о любом инциденте может запускаться симуляция распространения физических последствий с учетом текущих значений технологических параметров. При появлении новой записи в реестре данных общеизвестных уязвимостей информационной безопасности автоматически перестраиваются веса ребер графа и выдается список объектов, где данная уязвимость может привести к каскадному отказу с заданной вероятностью, таким образом реализуется анализ «Что-если» [5] новых уязвимостей.

Применение технологий больших данных для построения и оперативного анализа CPDG выводит защиту объектов КИИ на качественно новый уровень: от реактивного обнаружения инцидентов к проактивному прогнозированию и предотвращению каскадных киберфизических отказов.

**Анализ «темных данных» систем как источника индикаторов компрометации [6].** Под «темными данными» в контексте КИИ понимается информация диагностического и отладочного содержания, которую генерируют устройства систем автоматизации (контроллеры, устройства удаленного управления, интеллектуальные электронные устройства и прочее оборудование), и которая не попадает в СЗИ, соответственно, не проходит анализ в реальном времени. К разновидностям таких данных относятся: полные дампы памяти при перезагрузке; пакеты трассировки стека при сбоях; лог-файлы веб-сервера, встроенного в интеллектуальные электронные устройства; диагностические кольцевые буферы контроллеров и др.

Архитектура системы анализа «темных данных» может состоять из следующих блоков и процессов: агенты для автоматического сбора диагностических и отладочных данных; хранилище — многоуровневое Data

[1] Resilient-системы — информационные, технические, организационные системы, обладающие способностью адаптироваться и быстро восстанавливаться после различных инцидентов (кибератаки; сбои, вызванные техническими неисправностями или перегрузками; чрезвычайные ситуации природного и геополитического характеров). В концепции работы систем полагается, что инциденты неизбежны, поэтому акцент ставится на процессы адаптации и восстановления.

Lake, где они содержатся в исходном бинарном виде, а также в табличном (их нормализованная часть) [7]; парсеры и нормализаторы для разбора проприетарных диагностических протоколов, поиска сигнатур известных эксплойтов; ML-компонент для детекции аномалий в диагностических дампах и корреляции с обычными событиями информационной безопасности.

Так, обнаруженные в «темных данных» индикаторы автоматически сопоставляются с событиями из СЗИ по точным временным меткам и уникальным идентификаторам устройств. Анализ «темных данных» превращает оборудование объектов КИИ из «черного ящика» в один из информативных источников индикаторов компрометации.

**Гибридная ансамблевая модель «большие данные и федеративное обучение» для межотраслевой кооперации субъектов КИИ (Federated Threat Intelligence Ensemble, FTIE) [8].** В отличие от централизованных систем обмена индикаторами компрометации, требующих передачи сырых или обезличенных данных в единый контур, предлагаемая архитектура полностью исключает выгрузку конфиденциальных данных за периметр организации. Каждый субъект КИИ обучает локальную модель обнаружения аномалий и классификации угроз исключительно на собственных потоках данных (логи АСУ ТП, сетевой трафик, события СЗИ, телеметрия SCADA и IoT-устройств). В центральный агрегатор — доверенный узел Национального координационного центра по компьютерным инцидентам (НКЦКИ) или отраслевой центр государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) — передаются только обезличенные градиенты или дифференциально-приватные обновления весов модели.

Типовая архитектура FTIE включает следующие компоненты: локальные узлы федеративного обучения на базе отечественных платформ; защищенный канал передачи обновлений модели с использованием протоколов криптографической защиты по ГОСТ; центральный оркестратор-агрегатор (реализованный в контуре НКЦКИ или отраслевого центра ГосСОПКА), выполняющий безопасное усреднение параметров и формирование глобальной модели; слой обратной дистрибуции улучшенной глобальной модели обратно участникам.

Вместе с тем архитектура федеративного обучения подвержена специфическим угрозам безопасности [9]. К основным относятся атаки отравления модели, при которых скомпрометированный участник передает вредоносные градиенты; атаки вывода членства, позволяющие восстановить факт присутствия записи в обучающей выборке; атаки реконструкции данных по градиентам. Для противодействия указанным угрозам архитектура FTIE предусматривает применение дифференциальной приватности при формировании локальных обновлений; верификацию градиентов на центральном агрегаторе методами robust aggregation (например, trimmed mean); криптографическую защиту канала передачи; аудит аномальных обновлений с использованием статистических тестов. Указанные механизмы минимизируют риски компрометации как локальных данных участников, так и глобальной модели.

Применение архитектуры FTIE позволит создавать высокоточные межотраслевые модели обнаружения новых и ранее неизвестных угроз без нарушения законодательства, снизить нагрузку на каналы связи, а также обеспечить технологический суверенитет и возможность работы в полностью изолированных сегментах КИИ.

Представленные направления уже вышли за рамки научных прототипов и находятся в стадиях пилотного и опытно-промышленного внедрений на объектах КИИ [10]. Их совместное применение позволяет перейти от реактивной модели обнаружения инцидентов к проактивной и предиктивной защите, существенно повышая устойчивость КИИ к сложным целенаправленным атакам и минимизируя риски каскадных киберфизических отказов. В ближайшие годы данные технологии с высокой вероятностью будут нормативно закреплены в качестве обязательных элементов систем безопасности значимых объектов КИИ.

Апробация предложенных подходов проведена на цифровом двойнике фрагмента распределительной электросети напряжением 10/0,4 кВ, развернутом на базе программно-аппаратного комплекса с использованием отечественной платформы имитационного моделирования (SimInTech). Цифровой двойник интегрирован с реальными потоками телеметрии SCADA посредством Open Platform Communications Unified Architecture шлюза, обеспечивающего поступление данных с периодом опроса 1 с.

Граф CPDG включал 847 вершин, распределенных по трем слоям: кибернетический (312 вершин: серверы SCADA, автоматизированные рабочие места диспетчеров, коммутационное оборудование, удаленные терминальные блоки), физический (418 вершин: выключатели, разъединители, трансформаторы, линии, датчики тока и напряжения), внешний (117 вершин: температура окружающей среды, нагрузка потребителей, состояние смежных фидеров). Количество межслойных ребер составило 2340, внутрислойных — 4120. Веса ребер инициализированы на основе экспертных оценок в соответствии с методикой оценки рисков нарушения электроснабжения[1] и статистики технологических нарушений за предшествующий пятилетний период[2].

Верификация выполнена на трех классах атак: компрометация RTU с последующей инъекцией ложных команд управления коммутационным оборудованием; атака «человек посередине» на канал связи SCADA с подменой телеметрических данных; ransomware-атака

[1] Приказ Минэнерго России от 29.11.2016 № 1256 «Об утверждении Методических указаний по расчету уровня надежности и качества поставляемых товаров и оказываемых услуг для организации по управлению единой национальной (общероссийской) электрической сетью и территориальных сетевых организаций».

[2] Отчет о функционировании ЕЭС России в 2025 году / АО «СО ЕЭС». М., 2026. URL: https://www.so-ups.ru/functioning/tech-disc/tech-disc2026/tech-disc2026ups/ (дата обращения: 22.02.2026).

на сервер SCADA с блокировкой функций мониторинга. Для каждого класса сгенерировано по 50 сценариев с вариацией точки входа, времени суток и уровня нагрузки сети.

Детально исследован сценарий «компрометация RTU — ложная команда на выключатель — перегрузка смежного фидера — срабатывание защиты — отключение потребителей». Система CPDG обеспечила обнаружение аномального паттерна за 1,2 с до физического срабатывания защиты (среднее по 50 итерациям — 1,18 с, среднеквадратическое отклонение — 0,23 с), что подтверждает возможность упреждающего реагирования и блокировки развития каскада на ранней стадии.

Результаты классификации инцидентов по всей выборке (150 сценариев): Accuracy 95,1 %; Precision 93,8 %; Recall 94,7 %; F1-score 94,3 %; False Positive Rate 1,9 %; среднее время обнаружения 0,87 с.

Сравнение с базовым решением Security Information and Event Management (SIEM) (без модуля CPDG) показало повышение Recall на 18,4 % и сокращение времени до первичного алерта в 3,2 раза.

Эксперименты проводились на сервере с двумя процессорами Intel Xeon Gold 6248R, 512 ГБ ОЗУ и GPU NVIDIA A100. Байесовское обновление весов графа и симуляция марковских цепей выполнялись с использованием GPU-ускорения, что обеспечило обработку потока до 1,2 млн событий в секунду при латентности аналитического конвейера не более 150 мс. Верификация проведена на модели распределительной сети; масштабирование на магистральные сети и другие отрасли КИИ требует адаптации графа зависимостей и дополнительной валидации. Использование зарубежного аппаратного обеспечения обусловлено требованиями к вычислительной производительности; переход на отечественные GPU-ускорители (например, перспективные разработки на базе архитектуры «Эльбрус» или «Байкал») является направлением дальнейших исследований.

Проведенный эксперимент подтвердил практическую реализуемость предложенной архитектуры и ее превосходство над традиционными подходами к обнаружению инцидентов на объектах КИИ энергетического сектора.

Таким образом, технологии больших данных способны не только радикально повысить эффективность обнаружения атак и реагирования на инциденты безопасности, но и обеспечить качественно новый уровень устойчивости объектов КИИ к сложным целенаправленным атакам. Для формализации и практической реализации resilient-систем необходим единый математический аппарат, позволяющий интегрировать разнородные потоки данных в режиме реального времени, количественно оценивать риски каскадных отказов и оптимально распределять защитные ресурсы в условиях неопределенности и ограничений, заданных в том числе нормативными требованиями.

## Математический аппарат построения resilient-систем обеспечения безопасности объектов КИИ на основе технологий больших данных

Формализация указанных систем может быть выполнена путем представления всей киберфизической инфраструктуры субъекта КИИ в виде динамического взвешенного ориентированного временного мультиграфа [11, 12][1]:

$$G(t) = (V, E(t), w(t), \tau),$$

где $V = V_{\text{киберн}} \cup V_{\text{физич}} \cup V_{\text{внешн}}$ — объединенное множество вершин кибернетического, физического и внешнего слоев (хосты, контроллеры АСУ ТП, исполнительные механизмы, технологические параметры, факторы окружающей среды); $E(t)$ — множество ориентированных ребер в момент времени $t$, отражающих причинно-следственные, логические и временные зависимости; $w(e, t) \in [0, 1]$ — динамический вес ребра, интерпретируемый как условная вероятность передачи воздействия; $\tau(e) > 0$ — задержка распространения воздействия по ребру $e$.

Веса $w(e, t)$ и задержки $\tau(e)$ обновляются в реальном времени байесовским фильтром по поступающим потокам больших данных:

$$w(e, t) = P\,(\textit{последствие}|\textit{причина}, \textit{данные}),$$

где *данные* — информация от логов и телеметрии на момент времени $t$.

Количественная оценка устойчивости системы в момент $t$ определяется как:

$$R(t) = 1 - \max P\,(\textit{отказ}|\textit{компрометация } s, G(t)),$$

где $s$ — множество возможных точек входа атакующего.

Вероятность отказа (критического) вычисляется как максимальный поток в графе $G(t)$ от стартовой вершины к множеству критичных узлов с учетом весов $w(e, t)$ и задержек $\tau(e)$.

Динамика распространения киберфизического воздействия моделируется непрерывной цепью Маркова с поглощением [13]. Интенсивности переходов формируются из графа зависимостей, что приводит к системе прямых дифференциальных уравнений Колмогорова [13]:

$$\frac{dp_i(t)}{dt} = \sum_{j \neq i} \lambda_{ji}(t) p_j(t) - \sum_{j \neq i} \lambda_{ji}(t) p_i(t),\ i = 1, \ldots, N,$$

где $p_i(t)$ — вероятность нахождения системы в состоянии $i$ в момент $t$.

Решение системы в реальном времени осуществляется методами стохастической симуляции на GPU-ускоренных аналитических платформах [14], что

[1] Термин «динамический» означает, что структура графа (множество ребер, веса ребер, временные задержки распространения непрерывно обновляются в реальном или близком к реальному времени на основе поступающих потоков разнородных данных из корпоративного Data Lake.

обеспечивает прогноз развития каскадного отказа с горизонтом до нескольких часов при нагрузке в сотни миллионов событий в секунду.

Оптимизация размещения и настройки средств защиты формализуется как стохастическая игра с неполной информацией «защитник–атакующий» [15] на графе $G(t)$. Точное равновесие Нэша [16] аналитически неразрешимо, поэтому в реальном времени ищется ε-приближенное равновесие с помощью онлайн-алгоритмов обучения с подкреплением семейства актор-критик [17].

Итоговая задача максимизации устойчивости $\max R(t)$ формулируется следующим образом. Требуется максимизировать $R(t)$ при следующих ограничениях:

1) суммарная стоимость внедрения и эксплуатации выбранных защитных мероприятий не превышает выделенного бюджета:

$$\sum c_k x_k \le B,$$

где $c_k$ — стоимость $k$-го защитного мероприятия (приобретение, внедрение, аттестация, эксплуатация); $x_k$ — переменная решения: $x_k = 1$, если $k$-е мероприятие включается в план защиты, $x_k = 0$, если не включается (для дискретного случая), либо $x_k \in [0, 1]$ — доля ресурса, выделяемого на $k$-е мероприятие (для непрерывного случая); $B$ — утвержденный бюджет на обеспечение безопасности объекта КИИ на расчетный период;
2) суммарное потребление вычислительных, энергетических и сетевых ресурсов не нарушает установленных лимитов производительности и устойчивости объекта КИИ;
3) конфигурация и режимы работы средств защиты полностью соответствуют требованиям законодательства и приказов регуляторов.

Далее применяется двухэтапный итеративно-уточняющий алгоритм. На первом этапе формируется начальное решение путем итеративного расчета обобщенной меры центральности вершин во взвешенном временном графе $G(t)$. Расчет сводится к классической задаче нахождения стационарного распределения в марковском процессе с поглощением [18] и решается модифицированным степенным методом [19] для доминирующего собственного вектора матрицы переходных вероятностей. На втором этапе полученное решение уточняется комбинацией точных и эвристических методов глобальной оптимизации смешанно-целевой задачи: ветви и границы, генетические алгоритмы, метод отжига для дискретных переменных [20]; градиентные методы с барьерными функциями [16] — для непрерывных компонент вектора распределения ресурса защиты. Итеративное чередование этапов гарантирует сходимость к решению, близкому к глобальному оптимуму, при сохранении приемлемого времени вычислений в условиях реального времени и жестких нормативных ограничений.

Предложенный математический аппарат обеспечивает строгое формализованное описание и количественную оценку устойчивости объектов КИИ в условиях непрерывно эволюционирующих киберфизических угроз, при этом технологии больших данных выступают связующим элементом всего вычислительного контура.

Потоки больших данных (технологическая телеметрия, логи СЗИ, события промышленных контроллеров и т. д.) в реальном времени обеспечивают обновление весов и задержек динамического мультиграфа, формируют интенсивности переходов и служат входными данными для онлайн-обучения при поиске ε-приближенного равновесия Нэша, таким образом, создают адаптирующуюся предиктивную систему безопасности объекта КИИ.

Разработанные модели и алгоритмы формируют замкнутый data-driven контур проактивного управления устойчивостью и, как следствие, безопасностью, в котором технологии больших данных играют роль одновременно сенсорного, аналитического и исполнительного слоя.

## Обсуждение

Предложенные подходы к интеграции технологий больших данных в процессы обеспечения безопасности объектов КИИ существенно расширяют возможности традиционных систем защиты. В отличие от решений класса SIEM и User and Entity Behavior Analytics, ориентированных на корреляцию событий в информационном слое инфраструктуры, подход CPDG обеспечивает комплексное моделирование распространения воздействий через кибернетический, физический слои и слой внешней среды. Архитектура федеративного обучения FTIE, в отличие от централизованных платформ обмена информацией об угрозах, исключает передачу сырых данных за периметр организации, обеспечивая формирование межотраслевых моделей обнаружения угроз за счет обмена исключительно обезличенными градиентами. Анализ «темных данных» промышленного оборудования представляет новое направление, превращающее диагностическую информацию контроллеров АСУ ТП в источник индикаторов компрометации.

Предложенные решения непосредственно соотносятся с действующими нормативными требованиями. Приказы федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности КИИ РФ[1,2] определяют обязательные меры защиты значимых объектов КИИ, включая мониторинг событий безопасности, управление инцидентами и обеспечение устойчивости функционирования. Графы CPDG и математический аппарат оценки устойчивости $R(t)$ позволяют формализовать выполнение требований к анализу угроз безопасности информации и моделиро-

[1] Приказ ФСТЭК России от 25.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

[2] Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

ванию нарушителя. Архитектура FTIE соответствует положениям федерального законодательства[1] о взаимодействии субъектов КИИ с ГосСОПКА и обеспечивает выполнение требований о защите информации ограниченного доступа при межотраслевом обмене. Бюджетное ограничение в оптимизационной задаче учитывает экономическое обоснование мер защиты, предусмотренное методическими документами ФСТЭК России, а также национального стандарта[2].

Практическая реализация разработанных решений сопряжена с рядом ограничений: построение графов CPDG требует глубокой экспертизы и существенных трудозатрат на картирование межсистемных зависимостей; анализ «темных данных» предполагает разработку парсеров для проприетарных протоколов; архитектура федеративного обучения требует согласования моделей между участниками. Вычислительная сложность математического аппарата предъявляет высокие требования к аппаратному обеспечению, однако современные GPU-ускоренные платформы [14] позволяют достигать требуемой производительности.

Сравнительный анализ с промышленными решениями показывает следующее. Платформы класса SIEM (MaxPatrol SIEM, Kaspersky Unified Monitoring and Analysis Platform) обеспечивают корреляцию событий информационного слоя, однако не моделируют киберфизические зависимости и каскадные последствия. Решения ICS/SCADA-мониторинга (Claroty, Nozomi Networks, PT ISIM) детектируют аномалии в промышленных протоколах, но ограничены технологическим сегментом без интеграции с физическими процессами. Предложенный подход CPDG объединяет оба контура и дополняет их слоем внешней среды. Платформы Threat Intelligence (Malware Information Sharing Platform, OpenCTI) реализуют централизованный обмен индикаторами, требующий передачи данных, тогда как FTIE исключает выгрузку информации конфиденциального характера. Таким образом, разработанные решения не заменяют, а расширяют возможности существующих промышленных систем, формируя надстройку предиктивного уровня.

Разработанные подходы применимы к объектам КИИ во всех сферах, определенных соответствующим законодательством, при этом особую ценность представляют для значимых объектов первой и второй категорий. Графы CPDG наиболее эффективны для объектов с развитой технологической инфраструктурой (электростанции, нефтеперерабатывающие заводы), анализ «темных данных» актуален для объектов с большим парком оборудования предыдущих поколений, где традиционные средства мониторинга не обеспечивают достаточной глубины наблюдаемости, федеративное обучение применимо на уровне отраслевых центров ГосСОПКА.

Дальнейшее развитие предполагает разработку методических рекомендаций по построению типовых графов CPDG, создание библиотеки парсеров диагностических протоколов и нормативное закрепление разработанных механизмов в требованиях регуляторов. Особое значение имеет перспектива создания национальной платформы федеративного обмена моделями угроз под эгидой НКЦКИ, а интеграция с технологиями доверенного искусственного интеллекта и квантово-устойчивой криптографии обеспечит долгосрочную актуальность решений.

## Заключение

В условиях нарастающего количества и сложности целенаправленных атак на объекты критической информационной инфраструктуры обеспечение национальной безопасности возможно только при глубокой и системной цифровизации процессов защиты и обороны. Именно цифровизация на основе технологий больших данных позволяет не просто реагировать на уже произошедшие инциденты, а предвидеть, предотвращать и минимизировать последствия киберфизических угроз, обеспечивая непрерывность функционирования ключевых социоэкономических отраслей и сохраняя технологический и государственный суверенитеты России.

Проведенное исследование показало, что технологии больших данных выступают не просто вспомогательным инструментом цифровизации, они являются системообразующим элементом построения нового поколения систем обеспечения безопасности объектов критической информационной инфраструктуры. Интеграция больших данных в процессы мониторинга, анализа и реагирования на инциденты безопасности позволяет перейти от реактивной к проактивной и предиктивной моделям защиты. Нетривиальные направления применения больших данных выходят за рамки традиционных решений Security Information and Event Management и User and Entity Behavior Analytics и обеспечивают качественно новый уровень прогнозирования и предотвращения каскадных киберфизических рисков.

Верификация предложенных подходов на цифровом двойнике фрагмента распределительной электросети подтвердила их практическую реализуемость и эффективность: точность классификации инцидентов составила 94,3 %, время упреждающего обнаружения — 1,2 с до физического срабатывания защиты. Сравнительный анализ показал, что разработанные решения не конкурируют, а органично дополняют существующие промышленные системы защиты, формируя предиктивный уровень, отсутствующий в традиционных решениях Security Information and Event Management и Internet Connection Sharing.

Таким образом, предложен системный подход к созданию национальной экосистемы устойчивых киберфизических систем на основе технологий больших данных. Дальнейшее развитие полученных результатов может быть направлено на их нормативном закрепле-

[1] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[2] Национальный стандарт РФ ГОСТ Р 59503-2021/ISO/IEC TR 27016:2014 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации».

нии в качестве обязательных элементов систем безопасности значимых объектов критической информационной инфраструктуры нового поколения и в создании межотраслевой платформы обмена обезличенными моделями угроз на принципах федеративного обучения.

**Литература**


1. Якушев Н.О., Устинова К.А., Кочнев А.А. Импортозамещение как фактор развития отечественных цифровых технологий // Экономические и социальные перемены: факты, тенденции, прогноз. 2024. Т. 17. № 3. С. 82–101. doi: 10.15838/esc.2024.3.93.5
2. Davies Ph., Fritzsche A., Parry G., Wood Z. Data, resilience, and identity in the digital age // Strategic Change. 2023. V. 32. N 6. P. 169–174. doi: 10.1002/jsc.2560
3. Dedousis P., Stergiopoulos G., Arampatzis G., Gritzalis D. A security-aware framework for designing industrial engineering processes // IEEE Access. 2021. V. 9. P. 163065–163085. doi: 10.1109/access.2021.3134759
4. Zarochentsev A., Espinal X., Kiryanov A., Schovancova J. Federated data storage evolution in HENP: data lakes and beyond // Journal of Physics: Conference Series. 2020. V. 1525. P. 012071. doi: 10.1088/1742-6596/1525/1/012071
5. Nguyen Q.V.H., Zheng K., Weidlich M., Zheng B.L., Yin H., Nguyen T.T., Stantic B. What-if analysis with conflicting goals: recommending data ranges for exploration // Proc. of the IEEE 34th International Conference on Data Engineering (ICDE). 2018. P. 89–100. doi: 10.1109/icde.2018.00018
6. Косов Н.А., Гельфанд А.М., Лаптев А.А. Анализ темных данных для обеспечения устойчивости информационных систем от нарушения конфиденциальности или несанкционированных действий // Colloquium-Journal. 2019. № 13-2 (37). С. 100–103.
7. Ренсков Д.А. Исследование методов разработки систем управления данными, включая базы данных, хранилища данных и озера данных // Научные исследования и технологический суверенитет в современном мире: сборник статей всероссийской (национальной) научной конференции. СПб.: НАЦРАЗВИТИЕ, 2025. С. 59–64.
8. Tom A.K., Khraisat A., Jan T., Whaiduzzaman M., Nguyen T.D., Alazab A. Survey of federated learning for cyber threat intelligence in industrial IoT: techniques, applications and deployment models // Future Internet. 2025. V. 17. N 9. P. 409. doi.org/10.3390/fi17090409
9. Костенко В.А., Селезнева А.Е. Виды атак на федеративные нейросети и способы защиты // Труды Института системного программирования РАН. 2024. Т. 36. № 1. С. 35–44. doi: 10.15514/ISPRAS-2024-36(1)-3
10. Боровков А.И., Рябов Ю.А., Щербина Л.А., Мартынец Е.А., Корчевская А.А. Цифровые двойники в высокотехнологичной промышленности. СПб.: ПОЛИТЕХ-ПРЕСС, 2022. 492 с.
11. Кишкович Ю.П. Дискретная математика и элементы анализа сетей на языке R. М.: КноРус, 2023. 242 с.
12. Zhou H., Chen X., Yuan Y. A novel Extended-Kalman-Filter-Incorporated Latent Feature model on dynamic weighted directed graphs // Proc. of the IEEE International Conference on Systems, Man, and Cybernetics (SMC). 2024. P. 191–196. doi: 10.1109/smc54092.2024.10832044
13. Буре В.М., Парилина Е.М. Теория вероятностей и математическая статистика: Учебник для вузов. СПб.: Лань, 2025. 416 с.
14. Kang P. Evaluation of GPU-Accelerated edge platforms for stochastic simulations: performance and energy efficiency analysis // Mathematics. 2025. V. 13. N 20. P. 3305. doi: 10.3390/math13203305
15. Miao L., Li S. Cyber security based on mean field game model of the defender: Attacker strategies // International Journal of Distributed Sensor Networks. 2017. V. 13. N 10. P. 1–10. doi: 10.1177/1550147717737908
16. Кохендерфер М., Уинлер Т., Рэй К. Алгоритмы принятия решений: Учебник. М.: ДМК Пресс, 2023. 684 с.
17. Moghimi M., Ku H. Risk-sensitive actor-critic with static spectral risk measures for online and offline reinforcement learning // arXiv. 2025. arXiv:2507.03900. doi: 10.48550/arXiv.2507.03900
18. Зеленцов Б.П. Укрупнение состояний при моделировании надежности технических систем марковскими процессами // Надежность и качество сложных систем. 2021. № 2 (34). С. 36–52. doi: 10.21685/2307-4205-2021-2-4


**References**


1. Yakushev N.O., Ustinova K.A., Kochnev A.A. Import substitution as a factor in the development of domestic digital technology. *Economic and Social Changes: Facts, Trends, Forecast*, 2024, vol. 17, no. 3, pp. 82–101. (in Russian). doi: 10.15838/esc.2024.3.93.5
2. Davies Ph., Fritzsche A., Parry G., Wood Z. Data, resilience, and identity in the digital age. *Strategic Change*, 2023, vol. 32, no. 6, pp. 169–174. doi: 10.1002/jsc.2560
3. Dedousis P., Stergiopoulos G., Arampatzis G., Gritzalis D. A security-aware framework for designing industrial engineering processes. *IEEE Access*, 2021, vol. 9, pp. 163065–163085. doi: 10.1109/access.2021.3134759
4. Zarochentsev A., Espinal X., Kiryanov A., Schovancova J. Federated data storage evolution in HENP: data lakes and beyond. *Journal of Physics: Conference Series*, 2020, vol. 1525, pp. 012071. doi: 10.1088/1742-6596/1525/1/012071
5. Nguyen Q.V.H., Zheng K., Weidlich M., Zheng B.L., Yin H., Nguyen T.T., Stantic B. What-if analysis with conflicting goals: recommending data ranges for exploration. *Proc. of the IEEE 34th International Conference on Data Engineering (ICDE)*, 2018, pp. 89–100. doi: 10.1109/icde.2018.00018
6. Kosov N.A., Gelfand A.M., Laptev A.A. Analysis of dark data to ensure sustainability information systems from breach of privacy or unauthorized actions. *Colloquium-Journal*, 2019, no. 13-2 (37), pp. 100–103. (in Russian)
7. Renskov D.A. Research of methods of development of data management systems, including databases, data warehouses and data lakes. *Proc. of the Scientific Research and Technological Sovereignty in the Modern World*, 2025, pp. 59–64. (in Russian)
8. Tom A.K., Khraisat A., Jan T., Whaiduzzaman M., Nguyen T.D., Alazab A. Survey of federated learning for cyber threat intelligence in industrial IoT: techniques, applications and deployment models. *Future Internet*, 2025, vol. 17, no. 9, pp. 409. doi: 10.3390/fi17090409
9. Kostenko V.A., Selezneva A.E. Types of attacks on federated neural networks and methods of protection. *Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS)*, 2024, vol. 36, no.1, pp. 35–44. (in Russian). doi: 10.15514/ISPRAS-2024-36(1)-3
10. Borovkov A.I., Ryabov Yu.A., Shcherbina L.A., Martynets E.A., Korchevskaya A.A. *Digital Twins in the High-Technology Manufacturing Industry*. St. Petersburg, POLITEKH-PRESS Publ., 2022, 492 p. (in Russian)
11. Kishkovich Yu.P. Discrete *Mathematics and Elements of Network Analysis in R Language*. Moscow, KnoRus Publ., 2023, 24 p. (in Russian)
12. Zhou H., Chen X., Yuan Y. A novel Extended-Kalman-Filter-Incorporated Latent Feature model on dynamic weighted directed graphs. *Proc. of the IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2024, pp. 191–196. doi: 10.1109/smc54092.2024.10832044
13. Bure V.M., Parilina E.M. *Probability Theory and Mathematical Statistics*. St. Petersburg, Lan' Publ., 2025, 416 p. (in Russian)
14. Kang P. Evaluation of GPU-Accelerated edge platforms for stochastic simulations: performance and energy efficiency analysis. *Mathematics*, 2025, vol. 13, no. 20, pp. 3305. doi: 10.3390/math13203305
15. Miao L., Li S. Cyber security based on mean field game model of the defender: Attacker strategies. *International Journal of Distributed Sensor Networks*, 2017, vol. 13, no. 10, pp. 1–10. doi: 10.1177/1550147717737908
16. Kochenderfer M.J., Wheeler T.A., Wray K.H. *Algorithms for Decision Making*. The MIT Press, 2022, 700 p.
17. Moghimi M., Ku H. Risk-sensitive actor-critic with static spectral risk measures for online and offline reinforcement learning. *arXiv*, 2025. arXiv:2507.03900. doi: 10.48550/arXiv.2507.03900
18. Zelentsov B.P. Aggregation of states of Markov processes by modeling reliability of technical systems. *Reliability & Quality of*

19. Гасников А.В. Современные численные методы оптимизации. Метод универсального градиентного спуска: учебное пособие. М.: МФТИ, 2018. 286 с.
20. Гитман И.Б. Введение в стохастическую оптимизацию: учебное пособие. Пермь: ПНИПУ, 2014. 104 с.

*Complex Systems*, 2021, no. 2 (34), pp. 36–52. (in Russian). doi: 10.21685/2307-4205-2021-2-4
19. Gasnikov A.V. Modern Numerical Optimization Methods. *Universal Gradient*. Moscow, MIPT Publ., 2018, 286 p. (in Russian)
20. Gitman I.B. *Introduction to Stochastic Optimization*. Perm, PNIPU Publ., 2014, 104 p. (in Russian)

## Авторы

**Толстых Марина Юрьевна** — кандидат технических наук, доцент, доцент, Московский ордена Почета университет МВД России им. В.Я. Кикотя, Москва, 117997, Российская Федерация; доцент, Московский государственный лингвистический университет, Москва, 119034, Российская Федерация, https://orcid.org/0009-0001-2223-7709, marina_lion@mail.ru

**Коратаев Павел Дмитриевич** — кандидат технических наук, старший преподаватель, Военно-учебный научный центр Военно-воздушных сил «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина», Воронеж, 394064, Российская Федерация, https://orcid.org/0009-0000-3634-2772, korataev2015@mail.ru

## Authors

**Marina Yu. Tolstykh** — PhD, Associate Professor, Associate Professor, Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, 117997, Russian Federation; Associate Professor, Moscow State Linguistic University, Moscow, 119034, Russian Federation, https://orcid.org/0009-0001-2223-7709, marina_lion@mail.ru

**Pavel D. Korataev** – PhD, Senior Lecturer, Military Educational and Scientific Centre of the Air Force N.E. Zhukovsky and Y.A. Gagarin Air Force Academy, Voronezh, 394064, Russian Federation, https://orcid.org/0009-0000-3634-2772, korataev2015@mail.ru

*Статья поступила в редакцию 29.02.2026*
*Одобрена после рецензирования 18.03.2026*
*Принята к печати 18.05.2026*

*Received 29.02.2026*
*Approved after reviewing 18.03.2026*
*Accepted 18.05.2026*