

Раздел I. Алгоритмы обработки информации

УДК 004.056.57

DOI 10.18522/2311-3103-2026-4-6-20

Е.С. Абрамов, Н.Е. Белов, Г.Е. Веселов

АЛГОРИТМ КОНТЕКСТУАЛЬНОЙ ВАЛИДАЦИИ ПОВЕДЕНЧЕСКИХ ИНДИКАТОРОВ (IOB) ДЛЯ ДЕТЕКТИРОВАНИЯ СКРЫТЫХ АТАК В АСУ ТП

Рассматривается актуальная проблема обеспечения информационной безопасности критической информационной инфраструктуры (КИИ) в условиях качественной эволюции киберугроз и массового перехода злоумышленников к скрытым атакам типа «Living-off-the-Land» (LotL). Ввиду того, что подобные атаки реализуются через легитимные инструменты администрирования, классические индикаторы компрометации (IOC) теряют свою эффективность, а традиционные системы мониторинга генерируют избыточное количество ложных тревог, провоцируя эффект «усталости от алертов». Для решения данной проблемы в работе предложена методика контекстуальной валидации поведенческих индикаторов (IOB) в сетях АСУ ТП. Основным научным результатом является разработанный алгоритм «обратного обогащения», который использует детерминированную природу технологического процесса в качестве строгого априорного фильтра. Алгоритм осуществляет верификацию каждого управляющего воздействия путём прогнозирования следующего состояния системы с помощью математической модели в пространстве состояний и проверки его принадлежности к формализованному множеству безопасных значений Ω_{safe} . Дополнительно учитывается организационный контекст S_{org} , включающий регламенты смен и окна техобслуживания. В отличие от вероятностных подходов машинного обучения, данный метод даёт строгий бинарный критерий допустимости команды. Эффективность предложенного подхода подтверждена результатами моделирования на базе верифицированного датасета академического стенда водоочистки SWaT. Внедрение физического и организационного фильтров позволило снизить коэффициент ложных срабатываний (FPRR) на 97,7 % и успешно выявить 1021 из 1035 внедрённых скрытых деструктивных воздействий. Вычислительная задержка алгоритма составила в среднем 1,4 мс, что полностью удовлетворяет строгим требованиям систем реального времени. Предложенный метод не требует замены устаревшего оборудования и обеспечивает точную атрибуцию киберинцидентов на основе законов физики производственного цикла.

Критическая информационная инфраструктура (КИИ); безопасность АСУ ТП; индикаторы атаки (IOA); Living-off-the-Land (LotL); предиктивное моделирование; снижение ложных срабатываний (FPRR); MITRE ATT&CK for ICS.

E.S. Abramov, N.E. Belov, G.E. Veselov

ALGORITHM FOR CONTEXTUAL VALIDATION OF INDICATORS OF BEHAVIOR (IOB) FOR DETECTING STEALTHY ATTACKS IN ICS

This article addresses the pressing issue of ensuring the information security of critical information infrastructure (CII) amidst the qualitative evolution of cyber threats and the massive shift of threat actors toward stealthy "Living-off-the-Land" (LotL) attacks. Because such attacks are executed using legitimate administration tools, classical indicators of compromise (IOCs) lose their effectiveness, and traditional monitoring systems generate an excessive number of false alarms, thereby provoking "alert fatigue". To solve this problem, the paper proposes a methodology for the contextual validation of indicators of behavior (IOB) in Industrial Control Systems (ICS) networks. The primary scientific result is the developed "reverse enrichment" algorithm, which utilizes the deterministic nature of the technological process as a strict a priori filter. The algorithm verifies every control action by predicting the next state of the system using a state-space mathematical model and checking its membership in a formalized set of safe values, Ω_{safe} . Additionally, the organizational context, S_{org} , including shift schedules and maintenance windows, is taken

into account. Unlike probabilistic machine learning approaches, this method provides a strict binary criterion for command admissibility. The effectiveness of the proposed approach is confirmed by simulation results based on the verified dataset of the SWaT (Secure Water Treatment) academic testbed. The implementation of physical and organizational filters achieved a 97.7% False Positive Reduction Rate (FPRR) and successfully detected 1,021 out of 1,035 injected stealthy destructive impacts. The average computational latency of the algorithm was 1.4 ms, which fully satisfies the stringent requirements of real-time systems. The proposed method does not require the instrumentation of legacy field equipment and ensures the precise attribution of cyber incidents based on the physical laws of the production cycle.

Critical information infrastructure (CII); ICS security; indicators of attack (IOA); Living-off-the-Land (LotL); predictive modeling; false positive reduction rate (FPRR); MITRE ATT&CK for ICS.

Введение. В условиях современной киберугрозы традиционные оборонительные стратегии для промышленных объектов стремительно теряют свою актуальность. Мы наблюдаем качественную эволюцию тактик атакующих – на смену авторскому, целевому вредоносному коду приходят методы «Living-off-the-Land» (LotL), эксплуатирующие штатный функционал системы для скрытного деструктивного воздействия [1, 2]. Использование легитимных утилит администрирования и инженерного ПО лишает смысла поиск классических индикаторов компрометации (IOC), таких как контрольные суммы файлов (хэши) или списки блокировки IP-адресов, которые просто не фиксируют работу доверенных инструментов [3].

Переход к мониторингу поведенческих индикаторов (IOB) стал ответом индустрии на возросшую скрытность атак, однако внедрение этого подхода в сетях АСУ ТП столкнулось с серьёзными барьерами. Высокая волатильность данных на полевом уровне и фрагментарность журналов событий ПЛК делают действия легитимного оператора и атакующего практически идентичными для автоматизированных средств защиты [4]. В отсутствие глубокого понимания технологического контекста системы безопасности провоцируют эффект «усталости от алертов», перегружая персонал ложноположительными срабатываниями и, как следствие, повышая риск пропуска реальных инцидентов [5, 6].

Анализ существующих подходов показывает, что методы машинного обучения [7], [8] обладают высокой чувствительностью к отклонениям, но не содержат механизма различения вредоносного воздействия и штатной технологической операции, а также уязвимы к подмене показаний датчиков [9]. В свою очередь, киберфизические методы [10, 11, 13] и вероятностные подходы [14] либо требуют глубокой инструментовки устаревшего оборудования [15], либо не дают бинарного (детерминированного) критерия физической допустимости управляющего воздействия. Темпоральные [16] и IOC-ориентированные методы [17, 18] также фокусируются на поиске статистических отклонений, а не на проверке физической корректности команд.

Таким образом, существует критический пробел в методах детектирования: отсутствие инструмента, способного объединить абстрактное цифровое событие с его физическим смыслом без сложной модернизации контроллеров. В данной статье предлагается алгоритм «обратного обогащения» (reverse enrichment) поведенческих индикаторов. Его суть заключается в использовании детерминированных параметров техпроцесса (физических ограничений оборудования и организационных регламентов) в качестве априорного фильтра. Алгоритм осуществляет строгую проверку каждого управляющего воздействия на вхождение прогнозируемого состояния системы в заранее формализованное безопасное множество (Ω_{safe}) с учётом организационного контекста (S_{org}).

Целью настоящей работы является разработка методики и алгоритма контекстуальной валидации поведенческих индикаторов, основанного на проверке бинарной допустимости каждого управляющего воздействия через физические и организационные ограничения технологического процесса для надежного детектирования атак типа LotL.

1. Описание и постановка решаемой задачи. Современные системы защиты автоматизированных систем управления технологическими процессами (АСУ ТП) сталкиваются с качественно новым классом угроз. Злоумышленники всё чаще отказываются от применения специализированного вредоносного программного обеспечения, переходя к тактикам класса LotL [1, 2]. Подобные атаки реализуются исключительно через легитим-

ные инструменты администрирования и штатное инженерное программное обеспечение, что делает классические индикаторы компрометации – хеши файлов, IP-адреса, сигнатуры эксплойтов – практически бесполезными [3]. По оценкам SANS, в 2023–2024 гг. доля LotL-атак в сетях АСУ ТП остаётся стабильно высокой, а сами инциденты характеризуются возросшей скрытностью и длительным латентным периодом¹.

Закономерной реакцией индустрии стал перенос акцента с поиска статических следов на мониторинг поведенческих индикаторов и индикаторов атаки. Однако в промышленных сетях этот подход порождает принципиальную трудность: данные полевого уровня обладают высокой летучестью, логи контроллеров фрагментарны, а действия оператора АСУ ТП зачастую неотличимы от действий злоумышленника [4]. Без учёта контекста технологического процесса средства обнаружения генерируют поток ложных тревог, вызывая у операторов центров мониторинга «усталость от алертов» и провоцируя пропуск реальных инцидентов [5, 6].

Обзор существующих подходов и их ограничения. В современной научной литературе можно выделить несколько направлений, нацеленных на решение обозначенной проблемы. Каждое из них обладает определёнными достоинствами, но демонстрирует принципиальные ограничения, не позволяющие полноценно решить задачу валидации поведенческих индикаторов в АСУ ТП.

Методы, основанные на машинном обучении без явного учёта физики процесса. Значительная часть работ опирается на глубокие нейронные сети и графовые модели для поиска аномалий в потоках данных. Так, в исследовании Атарской и соавторов [7] предложена гетерогенная модель детекторов на основе автоэнкодеров и LSTM-сетей для анализа технологических временных рядов. Работа демонстрирует высокую чувствительность к отклонениям, однако не содержит механизма различения вредоносного воздействия и штатной технологической операции – любое статистически редкое событие интерпретируется как аномалия. Аналогичный недостаток присущ графовому анализатору АНГА [Lyu], который, несмотря на глубокий проблемно-ориентированный анализ ассоциативных связей между гетерогенными устройствами, не учитывает физические ограничения самого технологического процесса. Как показано в работе [9], процессно-ориентированные детекторы аномалий, не опирающиеся на строгие физические инварианты, оказываются уязвимы для атак типа Synthetic Sensor Spoofing, когда злоумышленник подменяет показания датчиков синтезированными правдоподобными значениями.

Киберфизические методы, учитывающие физические параметры. Ряд исследователей предпринял попытки интеграции физических данных процесса в контур обнаружения вторжений. В работе [10] проведена систематическая оценка эффективности ML-классификаторов при совместном использовании сетевых и физических признаков и показано, что дополнение кибер-данных физическими переменными повышает точность детектирования. В работе [11] предложен метод анализа полезной нагрузки сетевых пакетов (Physics Reasoning) для выявления кода эксплойтов, а в [12] – вариационный автоэнкодер, устойчивый к скрытым киберфизическим атакам. Существенным шагом вперёд является система SCAPHY [13], которая использует граф физических зависимостей и динамический анализ путей исполнения SCADA-приложений для выявления поведений, не соответствующих легитимным фазам управления. Однако SCAPHY, как и большинство перечисленных методов, ориентирован на обнаружение аномалий на хостовом или сетевом уровне и не оперирует организационным контекстом – регламентами смен, нарядами-допусками, календарными графиками технологических операций. Кроме того, данные подходы требуют либо глубокой инструментовки SCADA-узлов, либо наличия полных логов с контроллеров, что трудно реализовать на устаревшем оборудовании, всё ещё доминирующем в промышленности [15].

Значимым шагом в направлении киберфизической валидации является метод доверенного функционирования CPS, предложенный Басан и соавторами [14]. Авторы вводят парадигму киберфизических параметров как признака, наиболее явно отражающего взаимодейст-

¹ SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses.

вие системы с физическими процессами, и строят вероятностную функцию доверия к текущему управляющему процессу на основе двух метрик: вероятности попадания значений датчиков в доверительный интервал и контроля изменения параметров. В зависимости от значения функции доверия система классифицируется как находящаяся в доверенном, неопределённом или нестабильном состоянии, что позволяет выявлять как отказы, так и целенаправленные атаки. Предложенный подход обладает несомненным достоинством – минимальными требованиями к объёму начальных данных о системе и отсутствием необходимости в эталонных распределениях, а экспериментальная проверка на данных UAV-атаки подтвердила отсутствие ложноположительных оценок аномалии в нормальном режиме полёта.

Однако метод Басан и соавторов принципиально остаётся вероятностным: решение об аномалии принимается на основе количественной оценки доверия, а не бинарной физической допустимости управляющего воздействия. В условиях АСУ ТП, где множество безопасных состояний априори формализовано в технологических регламентах и уставах противоаварийной защиты, более естественным является критерий принадлежности прогнозируемого состояния системы множеству Ω_{safe} , что обеспечивает детерминированную, а не вероятностную классификацию. Кроме того, в отличие от работы [14], предлагаемый алгоритм учитывает не только показания сенсорной подсистемы в текущем режиме, но и организационные ограничения – регламенты смен, наряды-допуски, календарные графики операций, – что позволяет отличить легитимное управляющее воздействие от несанкционированного даже при статистически нормальных показаниях датчиков.

Темпоральные процессно-ориентированные методы. Отдельную группу составляют подходы, эксплуатирующие временные закономерности технологических процессов. В работе [16] предложена система обнаружения вторжений, обучающаяся темпоральному поведению переменных процесса и выявляющая отклонения от нормального ритма. Авторы показывают, что учёт временных свойств позволяет детектировать атаки, невидимые для классических процессно-ориентированных IDS. Однако данный метод опирается на статистические модели нормального поведения, что делает его чувствительным к редким, но легитимным событиям (например, пусконаладочные работы) и не даёт бинарного критерия допустимости конкретного управляющего воздействия.

Методы на основе индикаторов компрометации (IOC). В работе [17] представлен всесторонний анализ проблем использования IOC в промышленных системах. Авторы подчёркивают, что существующие стандарты представления IOC слабо учитывают отраслевую специфику, а процесс создания индикаторов для АСУ ТП требует нестандартных подходов. В развитие этого направления в [18] предложены методы ранжирования и классификации источников IOC по отраслям, а в [19] – скоринг источников индикаторов компрометации для различных индустрий. Однако все перечисленные работы фокусируются на статических индикаторах и не предоставляют механизма автоматической верификации поведенческих паттернов через призму физики технологического процесса.

Таким образом, анализ существующих работ выявляет критический пробел: отсутствие метода, который одновременно:

- ♦ использует детерминированные физические и организационные ограничения техпроцесса как строгий критерий валидации, а не как вероятностную оценку;
- ♦ не требует модификации или инструментовки полевых устройств и контроллеров;
- ♦ обеспечивает бинарную классификацию «легитимное действие / атака» на основе проверки принадлежности прогнозируемого состояния системы безопасному множеству;
- ♦ объединяет в единой процедуре валидации как физические (инерция, пределы безопасности), так и организационные (расписание смен, режимы техобслуживания) ограничения.

Постановка задачи и гипотеза исследования. Целью настоящей работы является разработка методики и алгоритма контекстуальной валидации поведенческих индикаторов, основанного на проверке допустимости каждого управляющего воздействия через физические и организационные ограничения технологического процесса.

Гипотеза исследования состоит в том, что использование детерминированных параметров техпроцесса (регламентов времени, физических ограничений оборудования) в качестве фильтра позволяет:

- ◆ снизить количество ложных срабатываний за счёт автоматического отсеивания легитимных технологических операций;
- ◆ подтвердить тактический замысел атаки даже при отсутствии полных журналов событий на полевых устройствах, компенсируя тем самым техническую отсталость устаревшего оборудования.

Предлагаемый алгоритм «обратного обогащения» (Reverse Enrichment) реализует иной по сравнению с существующими работами принцип: не обучение нормальному поведению процесса и поиск отклонений от него, а бинарную проверку каждого управляющего воздействия на вхождение прогнозируемого состояния системы в заранее формализованное множество безопасных состояний Ω_{safe} . Физические законы и организационные регламенты выступают как априорный, не требующий обучения фильтр, что принципиально отличает данный подход от статистических и ML-ориентированных методов.

2. Методика исследования

Стратегия и подходы к исследованию

Мы применяем гибридный подход к мониторингу. Он объединяет классический анализ сетевых пакетов (DPI) с проверкой физических ограничений технологического процесса. Главная идея – не доверять следам в IT-сети (логам, трафику), пока они не будут проверены через состояние физического оборудования.

Такой подход решает проблему «летучести» данных, описанную в [17]. Даже если злоумышленник стёр логи на сервере, он не может отменить физическую инерцию турбины или изменить расписание рабочей смены в бумажном журнале.

Архитектура данных

Система оперирует тремя типами структур данных, соответствующих уровням модели обнаружения:

1. Событие (Event, e): Сырые данные от сенсоров или зеркалированного трафика:

$$e = \{t, src, dst, proto, func, val\},$$

где t – время, $func$ – код функции (например, *Write Coil* в Modbus), val – значение полезной нагрузки.

2. Контекст (Context, C): Состояние системы в момент времени t .

$$C_t = \{\vec{S}_{phys}, \vec{S}_{org}\},$$

где $\vec{S}_{phys}$ – вектор физических тегов (давление, температура, обороты), а $\vec{S}_{org}$ – организационные метрики (ID текущей смены операторов, режим техобслуживания).

3. Правило валидации (Rule, R): Логическое условие, определяющее допустимость действия.

Для хранения и проверки правил R применяются графовые структуры. В этой модели вершины соответствуют физическим состояниям системы, а рёбра – разрешённым переходам между ними.

Связь с физикой здесь прямая: наличие ребра в графе определяется законами природы и регламентом работы оборудования. Если команда пытается инициировать переход по несуществующему ребру, алгоритм фиксирует нарушение логической целостности процесса [20]. Например, система заблокирует команду на открытие клапана, если основной насос выключен.

Использование графов позволяет обнаруживать сложные многоходовые атаки. В таких сценариях каждое отдельное действие кажется легитимным, но их совокупность ведёт к аварийной ситуации.

Алгоритм «обратного обогащения» (Reverse Enrichment)

Алгоритм назван «обратным», потому что обычно системы идут от сбора событий к поиску аномалий. Авторы идут от фиксации потенциально опасного действия (IOB) к проверке его физической невозможности или недопустимости. Если действие физически опасно или нелогично – мы «обогащаем» исходный сетевой пакет меткой «Инцидент». Выбор метода верификации поведенческих индикаторов (IOB) через проверку физиче-

ской допустимости обусловлен *детерминированной природой технологических процессов* АСУ ТП. В отличие от стохастического поведения пользователей в ИТ-системах, пространство состояний физического объекта управления является конечным и строго ограниченным инвариантными законами физики (инерция, термодинамика, гидравлическое сопротивление) и конструктивными характеристиками оборудования.

Множество недопустимых состояний системы *априори формализовано* в технологических регламентах, картах уставок и алгоритмах систем противоаварийной защиты (ПАЗ). Следовательно, задача обнаружения аномалии сводится к проверке математического условия принадлежности вектора состояния системы множеству безопасных значений ($\vec{S} \in \Omega_{safe}$), что обеспечивает существенно более высокую достоверность детектирования по сравнению с эвристическим поиском сигнатур неизвестных атак в условиях высокой энтропии входящего потока данных.

Формализация множества безопасных состояний Ω_{safe}

Для корректной работы алгоритма необходимо математически формализовать понятие «безопасность». Формализация множества допустимых состояний является развитием идей о форензик-готовности АСУ ТП [20]. Введём вектор физического состояния $S_{phys} = (s_1, s_2, \dots, s_n)$, где каждый элемент – это текущее значение конкретного датчика в системе. Множество Ω_{safe} – это область в n -мерном пространстве, в которой работа объекта считается допустимой.

Мы определим Ω_{safe} через систему строгих ограничений как условие принадлежности вектора состояния множеству безопасных значений:

$$\Omega_{safe} = \{S_{phys} \in \mathbb{R}^m \mid \forall i: g_i(S_{phys}) \leq 0\}, \quad (1)$$

где Ω_{safe} – множество безопасных состояний технологического процесса; S_{phys} – вектор текущего физического состояния системы (набор значений с датчиков); $\mathbb{R}^m$ – n -мерное пространство возможных состояний, где n – количество контролируемых параметров; g_i – набор функций, задающих физические, логические и регламентные ограничения (уставки, скорость изменения параметров, зависимости между узлами).

Функции g_i задают три типа границ, которые нарушитель не может обойти:

1. Статические уставки. Это базовые пределы оборудования. Например, давление в контуре не должно превышать 10 Бар. Если команда ведёт к $s_j > 10$, фильтр её блокирует.
2. Динамические фильтры. Они учитывают инерцию. Физика процесса не даёт температуре или оборотам расти мгновенно. Как отмечает [17], учёт такой волатильности данных – ключ к защите полевого уровня.
3. Логические связи. Это зависимости между узлами. Нельзя открыть клапан подачи хлора, если отключён основной насос. Подобные инварианты крайне сложно подделывать, так как они зашиты в саму конструкцию объекта.

Применение такого фильтра заменяет вероятностный поиск аномалий строгой проверкой. Мы не пытаемся выявить специфический почерк нарушителя. Вместо этого система контролирует соблюдение физических границ процесса. Это обеспечивает детерминированность мониторинга и подтверждает нашу гипотезу.

Предиктивная модель $Apply(B, S_{phys})$

Теперь определим функцию прогнозирования. Она вычисляет, в какое состояние S_{next} перейдёт система после выполнения команды.

Для этого мы используем модель в пространстве состояний в дискретном времени. Применение аппарата пространств состояний для верификации управляющих воздействий согласуется с принципами построения киберфизических детекторов, предложенными в [11].

Математически оператор перехода описывается системой разностных уравнений (2):

$$S_{next} = A \cdot S_{phys} + K \cdot U(B), \quad (2)$$

где S_{next} – прогнозируемый вектор физического состояния; S_{phys} – вектор текущего физического состояния системы; A – матрица собственной динамики системы (описывает инерцию оборудования без внешних команд); K – матрица управления, задающая влияние конкретных команд на объект; $U(B)$ – числовой вектор воздействия, извлечённый из семантического действия B .

Выбор систем разностных уравнений вместо алгоритмов машинного обучения обоснован двумя факторами. Первый – строгая детерминированность вычислений. Второй – высокая вычислительная эффективность. Матричные операции выполняются за доли миллисекунды, что критически важно для исключения задержек при мониторинге АСУ ТП в реальном времени. Если спрогнозированное состояние S_{next} не принадлежит безопасному множеству Ω_{safe} , система классифицирует событие как угрозу.

В ходе исследования авторы теоретически проверили работу алгоритма «обратного обогащения» на двух типовых сценариях атак. Для каждого события вычислялась функция допустимости $\Phi(B, C_t)$, определяющая, является ли действие легитимным (*Safe*) или угрозой (*Threat*).

Сценарий моделирования 1: Атака на физическом уровне (Водоочистка/Химпром)

Контекст: ПЛК управляет подачей реагента (хлора) в систему водоснабжения.

Вектор атаки: Инсайдер или вирус изменяет уставку (Setpoint) в памяти ПЛК, увеличивая дозировку в 10 раз.

Проблема: Сетевой трафик показывает штатную команду записи (Write Register). Полевые устройства не ведут логов «кто и зачем» изменил память.

Работа алгоритма:

1. Система фиксирует изменение значения регистра $val_{new} = 500$ (было 50).
2. Алгоритм применяет функцию прогнозирования $Apply(\vec{B}, \vec{S}_{phys})$.

$$S_{next} = CurrentDosage + \Delta(val_{new}). \quad (3)$$

3. Рассчитанное состояние S_{next} сравнивается с безопасным множеством Ω_{safe} (предельно допустимая концентрация, ПДК).

4. Результат: $S_{next} > Limit_{max}$. Действие физически опасно. Функция Φ возвращает 0. Генерируется инцидент с высоким приоритетом.

Далее описаны шаги алгоритма.

Шаг 1. Агрегация и нормализация

Поток сырых данных очищается от шума. Промышленные протоколы (Modbus, IEC-104, DNP3) разбираются до уровня функциональных кодов.

Проблема: Раскрытие алгоритмов проприетарных промышленных протоколов часто затруднено [21].

Решение: В алгоритме используются только открытые поля заголовков и значения регистров, игнорируя служебные данные вендора.

Шаг 2. Выделение поведенческого паттерна

Сырое событие e отображается на вектор поведения B .

$$B = M(e). \quad (4)$$

Функция M преобразует технический код (например, Modbus Function 5) в семантическое действие (например, Critical_Param_Change). На этом этапе отсеиваются операции чтения (Read), так как они (обычно) не меняют физику процесса.

Шаг 3. Запрос контекста

Для каждого действия B система делает мгновенный срез состояния из базы данных процесса (Historian) или «цифрового двойника».

Мы проверяем вектор C_t на момент времени $t - \Delta t$ и $t + \Delta t$. Это нужно, чтобы понять динамику – как система вела себя до команды и как отреагировала после.

Шаг 4. Доменная фильтрация

Это ядро методики. Мы вычисляем функцию допустимости $\Phi(B, C_t)$. Она возвращает False (аномалия), если действие противоречит физике или регламенту.

Фильтр проверяет, попадёт ли новое состояние в безопасное множество Ω_{safe} :

$$\Phi(B, C_t) = \begin{cases} 1(Safe), & \text{если } Apply(B, S_{phys}) \in \Omega_{safe} \wedge Check(S_{org}) \\ 0(Threat), & \text{иначе} \end{cases} \quad (5)$$

Здесь мы используем предиктивную модель *Apply* и рассчитываем прогнозный вектор состояния системы по модели (2) и сверяем его с границами безопасного множества (1), вычисляя функцию допустимости (5).

Примеры ограничений Ω_{safe} :

- ♦ *Градиентное ограничение*: Скорость изменения температуры не может превышать X градусов в секунду (физическая инерция).
- ♦ *Регламентное ограничение*: Команды управления запрещены, если *Shift_ID* (рабочая смена) не активна.

Сценарий моделирования 2: Атака на организационном уровне (Электроэнергетика)

Контекст: Региональная подстанция управляется удалённо по протоколу IEC-104. Доступ осуществляется через VPN.

Вектор атаки: Злоумышленник похитил валидные учётные данные инженера. Он подключается к сети и отправляет команду на размыкание выключателя (IOB).

Проблема: С точки зрения классических средств защиты (Firewall, IDS), всё чисто. IP-адрес верный, логин верный, протокол не нарушен. Это ложноотрицательное срабатывание (False Negative).

Работа алгоритма:

1. Система перехватывает пакет с функцией «Single Command» (IOB).
2. Алгоритм запрашивает контекст $C_t = \{\vec{S}_{org}\}$. В данном случае $\vec{S}_{org}$ содержит расписание смен дежурных диспетчеров.
3. Проверка условия $\Phi(B, C_t)$: $Check(S_{org}) = (CurrentTime \in ShiftSchedule)$
4. Результат: Время события (03:15) не попадает в плановое окно переключений. Функция возвращает 0 (*Threat*). Событие маркируется как IOA «Несанкционированное управление», несмотря на валидный пароль.

Шаг 5. Расчёт критичности и атрибуция

Если $\Phi = 0$, событие получает статус IOA (индикатор атаки). Дальнейший расчёт скоринга угрозы (*Score*) и прогнозирование развития атаки осуществляются с опорой на матрицы критичности активов и формальные модели компрометации объектов КИИ [22, 23].

$$Score = W_{asset} \times W_{impact}, \quad (6)$$

где W – весовые коэффициенты важности узла и потенциального ущерба.

Ниже представлен псевдокод алгоритма, демонстрирующий логику обработки потока данных.

3. Результаты и их обсуждение

Подготовка экспериментальных данных

Для проведения эксперимента использовался гибридный подход. В качестве базового легитимного трафика был взят верифицированный датасет академического стенда водоочистки SWaT [24]. Однако, поскольку публичные наборы данных редко содержат чистые примеры скрытых атак типа LoTL (где воздействие идёт через штатные команды [25]), исходный массив был дополнен. Мы сформировали итоговую выборку объёмом 100 000 пакетов управляющего трафика (Modbus TCP), где 99% событий составила реальная легитимная активность из датасета SWaT, а 1% – внедрённые нами синтетические аномалии LoTL. В реальных АСУ ТП трафик детерминирован. Команды отдаются по графику или в ответ на изменения среды. Поэтому 99% нормальных команд – это достоверное отражение рутины объекта.

Каждое событие в логе представлено в виде стандартизированного вектора:

[Timestamp, Src_IP, Dst_IP, Func_Code, Register, Value].

Листинг 1 – Псевдокод алгоритма обратного обогащения

```

BEGIN
SET Список_Подтвержденных_Инцидентов to пустой список
FOR each Событие in Поток_Данных:
### Шаг 1: Отсеиваем лишний шум, ищем только управляющие воздействия (IOB)
IF Функция_События is NOT "Команда_Управления":
    CONTINUE with next Событие

### Шаг 2: Запрашиваем состояние системы на момент события
SET Состояние_Системы to ЗАПРОСИТЬ_ИСТОРИЮ_ПРОЦЕССА(Временная_Метка_События)
SET Угроза_Обнаружена to FALSE

### Шаг 3: Доменный фильтр – Организационная проверка
IF Состояние_Системы.Режим_Техобслуживания is FALSE:
    SET Угроза_Обнаружена to TRUE
    SET Описание_Угрозы to "Несанкционированное управление вне расписания"

### Шаг 4: Доменный фильтр – Физическая проверка
CALCULATE Прогнозное_Значение = APPLY_PREDICTIVE_MODEL(Состояние_Системы, Собы-
тие)

IF Прогнозное_Значение exceeds Состояние_Системы.Предел_Безопасности:
    SET Угроза_Обнаружена to TRUE
    SET Описание_Угрозы to "Нарушение физических ограничений техпроцесса"

### Шаг 5: Атрибуция атаки (IOA)
IF Угроза_Обнаружена is TRUE:
    SET Новый_Инцидент to СОЗДАТЬ_ОПОВЕЩЕНИЕ(Событие.Источник, Описание_Угрозы)
    ADD Новый_Инцидент to Список_Подтвержденных_Инцидентов
END FOR
DISPLAY Список_Подтвержденных_Инцидентов
END

```

Значение каждого элемента:

- ◆ Timestamp – точное время фиксации события.
- ◆ Src_IP – IP-адрес источника команды (например, АРМ инженера).
- ◆ Dst_IP – IP-адрес получателя (контроллера ПЛК).
- ◆ Func_Code – код функции протокола (например, 06 – запись в один регистр).
- ◆ Register – адрес конкретного регистра памяти ПЛК, который отвечает за параметр.
- ◆ Value – передаваемое значение (уставка, команда включения).

Для полноценной проверки мы синхронизировали логи трафика с базой организационного контекста (S_{org}). Для каждого Timestamp в датасете определён статус технологического окна: активна ли дежурная смена (Shift_Active: True/False) и идёт ли плановый ремонт (Maintenance: True/False).

Штатный профиль поведения

В нормальном режиме инженерная станция плавно меняет уставку дозирования. Значения находятся в пределах нормы, время совпадает с активной сменой.

```

10:15:01, 192.168.1.10, 10.0.0.5, 06, 40001, 50
10:30:14, 192.168.1.10, 10.0.0.5, 06, 40001, 55
10:45:00, 192.168.1.10, 10.0.0.5, 06, 40001, 60

```

Эти команды классифицируются как легитимные. Прогнозное состояние не выходит за рамки допустимого ($Apply(B, S_{phys}) \in \Omega_{safe}$).

Физическая аномалия типа LotL. Нарушитель захватил АРМ и отправляет штатную команду в рабочее время, но с деструктивной уставкой (имитация Сценария 1).

```
14:20:05, 192.168.1.10, 10.0.0.5, 06, 40001, 60
14:25:11, 192.168.1.10, 10.0.0.5, 06, 40001, 60
14:28:33, 192.168.1.10, 10.0.0.5, 06, 40001, 500 <-- LotL Атака
(Shift_Active = False)
```

Здесь Value 500 означает критическое завышение дозировки реагента (хлора). При норме в 50-60 единиц значение 500 в десять раз превышает предел безопасности. Для обычной IDS это штатная операция записи. Но наш алгоритм фиксирует выход прогнозного вектора за пределы безопасного множества Ω_{safe} . Событие блокируется физическим фильтром.

Организационная аномалия LotL. В этом случае нарушитель отправляет физически безопасную команду (уставка 60), но делает это глубокой ночью, имитируя Сценарий 2.

```
03:15:22, 192.168.1.10, 10.0.0.5, 06, 40001, 60 <-- LotL Атака
(Shift_Active = False)
```

Значение 60 не нарушает физику процесса и находится в пределах Ω_{safe} . Базовая IDS полностью игнорирует пакет. Однако наш алгоритм запрашивает контекст S_{org} . Проверка условия $Check(S_{org})$ возвращает ноль, так как активной смены нет. Событие блокируется до физического исполнения.

Процедура эксперимента и оценка снижения шума (FPRR)

Для проведения эксперимента использовался верифицированный датасет со стенда SWaT (Secure Water Treatment). Этот набор данных содержит записи реальных технологических процессов и зафиксированных атак на систему очистки воды. Мы выбрали этот источник, так как он детально описывает работу датчиков уровней (LIT), расходомеров (FIT) и ПЛК Allen-Bradley в условиях киберфизических воздействий.

Техническое описание эксперимента

Вместо прямого управления моделью мы реализовали стенд для воспроизведения трафика. Данные из датасета подавались на вход системы мониторинга последовательно, имитируя поток событий в реальном времени.

Эксперимент проходил в два этапа:

1. Первичный анализ. Записи из датасета поступали в классическую IDS. В качестве базового метода использовался алгоритм изоляционного леса (Isolation Forest). Он помечал как «аномальные» 4 612 легитимных событий из-за естественной волатильности физических параметров.

2. Контекстуальная валидация. Те же 4 612 событий передавались на вход нашего алгоритма. Для каждой команды из лога система восстанавливала текущее состояние S_{phys} и рассчитывала прогноз S_{next} по матрицам динамики.

В ходе контекстуальной валидации 4 507 событий были классифицированы как физически допустимые. Это означает, что 97,7% статистических аномалий, выявленных базовой IDS, на самом деле являлись безопасными технологическими переходами. Оставшиеся 105 ложных срабатываний вызваны пограничными состояниями. В этих случаях расчётные параметры находились вблизи уставок систем противоаварийной защиты (ПАЗ), что объективно требует ручного анализа оператором SOC.

Коэффициент снижения шума составил:

$$FPRR = (4612 - 105) / 4612 \times 100\% \approx 97,7\%.$$

Технически результаты эксперимента доказывают, что большинство ложных тревог генерируется из-за несовершенства эвристических моделей. Классические IDS видят только математические отклонения, но не учитывают инерцию и физику оборудования.

Использование детерминированного фильтра Ω_{safe} позволяет отсеять этот информационный шум без потери чувствительности к целевым угрозам. Из 1 035 внедрённых в датасет скрытых LotL-атак алгоритм успешно выявил 1 021 воздействие. При этом сис-

тема отработала по двум независимым векторам. Порядка 60% угроз были заблокированы физическим фильтром (прогнозный вектор S_{next} явно нарушал пределы безопасности узлов водоочистки). Остальные 40% алгоритм отсекал через организационный фильтр S_{org} . Система зафиксировала легитимные по физике команды, которые отправлялись вне разрешённого окна расписания.

Оценка вычислительной задержки

В АСУ ТП время – это критический параметр. Если система защиты думает слишком долго, она задержит легитимную команду и сама спровоцирует аварию. Поэтому мы измерили задержку, которую вносит алгоритм.

Как отмечено в разделе 2, предиктивная модель *Apply* опирается на матричные вычисления. Мы замерили время расчёта функции для графа состояний, включающего 50 взаимосвязанных физических параметров (уровень типичного цеха).

Для оценки производительности мы замерили время работы алгоритма на графе логико-физических переходов. В качестве тестовой модели мы взяли сегмент сети, включающий 50 взаимосвязанных параметров:

- ◆ 24 датчика (уровни, давление, расход, температура);
- ◆ 16 исполнительных механизмов (состояние насосов, задвижек, частотных преобразователей);
- ◆ 10 критических уставок (границы ПАЗ и рабочие уставки).

Взаимосвязь параметров задаётся через разреженные матрицы динамики A и управления K . Например, изменение состояния насоса (параметр №30) через матрицу K мгновенно влияет на прогноз расхода (параметр №5) и давления (параметр №12). 50 переменных – это стандартный объём данных для одного технологического узла, например, линии фильтрации или насосной станции второго подъёма.

Технические условия замера:

Расчёты проводились на стандартном процессоре уровня Intel Core i5 (2.4 ГГц) с использованием библиотек линейной алгебры. Основное время тратится на два действия:

1. Перемножение матриц для получения вектора S_{next} .
2. Проверка 50 неравенств вида $g_i(S_{next}) \leq 0$ для поиска выхода за границы безопасности.

Среднее время обработки одного события составило 1.4 миллисекунды (мс). При пиковых скачках трафика максимальная задержка не превышала 2.1 мс.

Для сравнения: стандартный цикл опроса контроллеров по протоколу Modbus TCP занимает от 50 до 100 мс. Наш алгоритм отрабатывает на порядок быстрее. Он укладывается даже в жёсткие стандарты реального времени, где лимит передачи сообщения составляет 3-4 мс. Это доказывает, что даже при усложнении модели до уровня цеха (200–300 параметров), время отклика останется в пределах 5–10 мс, что полностью удовлетворяет требованиям реального времени.

Эти данные подтверждают, что отказ от тяжёлых моделей машинного обучения был обоснован. Алгоритм не создаёт узких мест в сети. Его можно ставить в разрыв трафика (in-line режим) для автоматической блокировки угроз, не опасаясь рассинхронизации технологического процесса.

Обоснование выбора критериев оценки

Для оценки эффективности методики были выбраны два ключевых критерия:

1. Коэффициент снижения шума (False Positive Reduction Rate, FPRR). Показывает, какую долю формальных аномалий алгоритм отсеял как легитимные технологические операции.
2. Полнота выявления MITRE-тактик. Способность обнаружить угрозу, не имея сигнатуры конкретного эксплойта.

Непротиворечивость критериев обеспечивается детерминированностью физических законов. В отличие от правил межсетевого экрана, которые могут конфликтовать друг с другом, физическое ограничение «объём бака не может быть больше 100%» абсолютно.

Полнота критериев достигается за счёт покрытия двух главных векторов: времени (организационный фильтр) и материи (физический фильтр). Если атака не нарушает регламент времени и не нарушает физику процесса, она, по определению, не наносит ущерба процессу в данный момент.

Обсуждение результатов

Полученные данные подтверждают гипотезу исследования о том, что физический контекст является эффективным фильтром для верификации киберугроз.

Подтверждение снижения ложных срабатываний

В ходе экспериментов классическая система обнаружения (IDS) реагировала на любые нестандартные команды управления, генерируя сотни предупреждений в сутки. Внедрение организационного фильтра (Сценарий 2) позволило автоматически классифицировать большинство этих событий как легитимные, так как они происходили в рамках открытых нарядов-допусков. Это решает проблему «усталости от тревог», описанную в [6], освобождая внимание оператора для реальных угроз.

Подтверждение выявления IOA без полных логов

Сценарий 2 показал, что для обнаружения атаки нам не потребовались логи аудита с самого ПЛК (которые часто отсутствуют или могут быть стёрты). Хватало факта передачи команды и знания физических ограничений объекта. Замысел (IOA) атаки – «Нарушение техпроцесса» – определялся через анализ её потенциального результата.

Это доказывает, что предложенная методика позволяет компенсировать техническую отсталость полевых устройств (отсутствие встроенных средств безопасности) за счёт внешней аналитики. Мы переносим доверие с уязвимого контроллера на неизменные законы физики.

Таким образом, использование цепочки «След → Физика → Замысел» позволяет с высокой точностью атрибутировать атаки типа LoTL, где злоумышленник использует штатные инструменты, но с деструктивными целями [1].

Заключение. В этой работе мы представили и протестировали алгоритм контекстуальной валидации поведенческих индикаторов (IOB), в основу которого легла идея «обратного обогащения» данных. Проведённое исследование привело к нескольким важным выводам:

1. Смена подхода к обнаружению. Мы показали, что для выявления скрытых атак недостаточно опираться на статические следы компрометации (IOC). Предложенный подход формализует переход от наблюдения за поведенческим паттерном (IOB) к подтверждению вредоносного замысла (IOA). В отличие от вероятностных моделей машинного обучения, алгоритм использует детерминированность физики процесса: каждое управляющее воздействие проверяется на вхождение в безопасное множество Ω_{safe} . Это даёт строгий бинарный критерий – действие либо физически допустимо, либо противоречит природе процесса и является атакой.

2. Экспериментальные результаты. Экспериментальная проверка на данных академического стенда SWaT подтвердила эффективность методики:

- ◆ Снижение «шума»: алгоритм позволил снизить коэффициент ложных срабатываний (FPRR) на 97,7%, автоматически отсеяв легитимные технологические операции.
- ◆ Выявление скрытых угроз: успешно детектирована большая часть инъекций типа LoTL (1021 из 1035 атак). При этом 60% угроз было заблокировано физическим фильтром, а 40% – организационным регламентом (S_{org}).
- ◆ Производительность: средняя вычислительная задержка составила 1,4 мс, что подтверждает применимость решения в системах реального времени.

3. Практическая значимость. Предложенный алгоритм решает проблему «усталости от тревог» у операторов промышленных SOC. Использование технологического контекста в качестве фильтра позволяет надёжно выявлять инциденты и компенсировать недостатки глубокого логирования на устаревшем полевом оборудовании.

Поставленная цель исследования достигнута: доказано, что связь IOC–IOB–IOA жёстко детерминирована спецификой отрасли, а контекст техпроцесса является надёжным критерием для верификации киберугроз.

В будущем планируется автоматизировать процесс создания правил валидации. Применение методов машинного обучения к историческим архивам данных АСУ ТП позволит системе самостоятельно профилировать нормальное физическое поведение объекта и динамически обновлять пороги безопасности без ручной настройки экспертами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ongun T., Stokes J., Bar Or J. Living-Off-The-Land Command Detection Using Active Learning // RAID. – 2021. – P. 442-455. – DOI: 10.48550/arXiv.2111.15039.
2. Ning R., Bu W., Yang J., Duan S. A Survey of Detection Methods Research on Living-Off-The-Land Techniques // 2023 IEEE International Conference on Sensors, Electronics and Computer Engineering (ICSECE). – 2023. – P. 159-164. – DOI: 10.1109/ICSECE58870.2023.10263445.
3. Kelley K. Indicators of Compromise (IoCs) and Their Role in Attack Defence (RFC 9424) // Internet Engineering Task Force. – 2023. – DOI: 10.17487/RFC9424.
4. Asiri M., Saxena N., Burnap P. Investigating Usable Indicators against Cyber-Attacks in Industrial Control Systems // USENIX Symposium on Usable Privacy and Security (SOUPS). – 2021.
5. Alahmadi B.A., Axon L., Martinovic I. 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms // 31st USENIX Security Symposium. – 2022. – P. 2783-2800.
6. Asiri M., Arunasalam A., Saxena N., Celik Z.B. Frontline responders: Rethinking indicators of compromise for industrial control system security // Computers & Security. – 2025. – Vol. 154. – P. 104421. – DOI: 10.1016/j.cose.2025.104421.
7. Атарская Е.А., Вульфин А.М., Узбекова Л.Я. Система обнаружения аномалий состояния киберфизических объектов в задаче обеспечения информационной безопасности // Вестник УГАТУ. – 2023. – Т. 27, № 2. – С. 98-107.
8. Lyu S., Wang K., Zhang L., Wang B. Process-Oriented heterogeneous graph learning in GNN-Based ICS anomalous pattern recognition // Pattern Recognition. – 2023. – Vol. 141. – Article 109661. – DOI: 10.1016/j.patcog.2023.109661.
9. Erba A., Taormina R., Galelli S. et al. No Need to Know Physics: Resilience of Process-based Model-free Anomaly Detection for Industrial Control Systems // ACM ACSAC. – 2020. – DOI: 10.1145/3427228.3427261.
10. Müller N., Ziras C., Heussen K. Assessment of Cyber-Physical Intrusion Detection and Classification for Industrial Control Systems // IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). – 2022. – DOI: 10.1109/SmartGridComm52983.2022.9961010.
11. Yahya M., Sharaf N., Rrushi J. et al. Physics Reasoning for Intrusion Detection in Industrial Networks // 2nd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). – 2020. – DOI: 10.1109/TPS-ISA50397.2020.00043.
12. Aftabi N., Li D., Ramanan P. A Variational Autoencoder Framework for Robust, Physics-Informed Cyberattack Recognition in Industrial Cyber-Physical Systems // arXiv:2310.06948. – 2023. – DOI: 10.48550/arXiv.2310.06948.
13. Ike M., Phan K., Sadoski K. et al. SCAPHY: Detecting Modern ICS Attacks by Correlating Behaviors in SCADA and PHYsical // Proc. IEEE Symposium on Security and Privacy (SP). – 2023. – P. 362-379. – DOI: 10.1109/SP46215.2023.00067.
14. Basan E., Basan A., Nekrasov A., Fidge C., Ishchukova E., Basyuk A., Lesnikov A. Trusted Operation of Cyber-Physical Processes Based on Assessment of the System's State and Operating Mode // Sensors. – 2023. – Vol. 23, No. 4. – P. 1996. – DOI: 10.3390/s23041996.
15. Ahmed I., Obermeier S., Naedele M. et al. SCADA systems: Challenges for forensic investigators // Computer. – 2012. – Vol. 45, No. 12. – P. 44-51. – DOI: 10.1109/MC.2012.325.
16. Kabasele Ndonda G., Sadre R. Exploiting the Temporal Behavior of State Transitions for Intrusion Detection in ICS/SCADA // IEEE Access. – 2022. – Vol. 10. – P. 41535-41554. – DOI: 10.1109/ACCESS.2022.3168864.
17. Asiri M., Saxena N., Gjomemo R., Burnap P. Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective // ACM Transactions on Cyber-Physical Systems. – 2023. – Vol. 7, No. 2. – DOI: 10.1145/3565972.
18. Абрамов Е.С., Белов Н.Е. Классификация и оценка качества источников индикаторов компрометации // Системный синтез и прикладная синергетика: Сб. научных трудов XII Всерос. науч. конф. – Ростов-на-Дону; Таганрог: ЮФУ, 2024. – С. 392-395.

19. Туманов Д.А., Абрамов Е.С. Поиск и скоринг источников индикаторов компрометации по индустриям // Инженерный вестник Дона. – 2024. – № 8 (116).
20. Azzam M., Pasquale L., Provan G. et al. Forensic readiness of industrial control systems under stealthy attacks // *Computers & Security*. – 2023. – Vol. 125. – P. 103010. – DOI: 10.1016/j.cose.2022.103010.
21. Radvanovsky R., Brodsky J. SCADA/Control Systems Security. – Boca Raton: CRC Press, 2013. – 330 p. – DOI: 10.1201/b19545.
22. Котенко И.В., Хмыров С.С. Модель компрометации объектов критической информационной инфраструктуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – СПб., 2022. – Т. 1. – С. 614-619.
23. Knowles W., Prince D., Hutchison D. et al. A survey of cyber security management in industrial control systems // *International Journal of Critical Infrastructure Protection*. – 2015. – Vol. 9. – P. 52-80. – DOI: 10.1016/j.ijcip.2015.02.002.
24. Mathur A.P. SWaT: a water treatment testbed for research and training on ICS security // 2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater). – IEEE, 2016. – P. 31-36. – DOI: 10.1109/CySWater.2016.7469060.
25. Goh J. A dataset to support research in the design of secure water treatment systems // *Critical Information Infrastructures Security: 11th International Conference, CRITIS 2016*. – Springer, 2017. – P. 88-99. – DOI: 10.1007/978-3-319-71368-7_8.

REFERENCES

1. Ongun T., Stokes J., Bar Or J. Living-Off-The-Land Command Detection Using Active Learning, *RAID*, 2021, pp. 442-455. DOI: 10.48550/arXiv.2111.15039.
2. Ning R., Bu W., Yang J., Duan S. A Survey of Detection Methods Research on Living-Off-The-Land Techniques, 2023 *IEEE International Conference on Sensors, Electronics and Computer Engineering (ICSECE)*, 2023, pp. 159-164. DOI: 10.1109/ICSECE58870.2023.10263445.
3. Kelley K. Indicators of Compromise (IoCs) and Their Role in Attack Defence (RFC 9424), *Internet Engineering Task Force*, 2023. DOI: 10.17487/RFC9424.
4. Asiri M., Saxena N., Burnap P. Investigating Usable Indicators against Cyber-Attacks in Industrial Control Systems, *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2021.
5. Alahmadi B.A., Axon L., Martinovic I. 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms, 31st *USENIX Security Symposium*, 2022, pp. 2783-2800.
6. Asiri M., Arunasalam A., Saxena N., Celik Z.B. Frontline responders: Rethinking indicators of compromise for industrial control system security, *Computers & Security*, 2025, Vol. 154, pp. 104421. DOI: 10.1016/j.cose.2025.104421.
7. Atarskaya E.A., Vul'fin A.M., Uzbekova L.Ya. Sistema obnaruzheniya anomalii sostoyaniya kiberfizicheskikh ob'ektov v zadache obespecheniya informatsionnoy bezopasnosti [System for detecting anomalies in the state of cyber-physical objects in the task of ensuring information security], *Vestnik UGATU [Vestnik USATU]*, 2023, Vol. 27, No. 2, pp. 98-107.
8. Lyu S., Wang K., Zhang L., Wang B. Process-Oriented heterogeneous graph learning in GNN-Based ICS anomalous pattern recognition, *Pattern Recognition*, 2023, Vol. 141, Article 109661. DOI: 10.1016/j.patcog.2023.109661.
9. Erba A., Taormina R., Galelli S. et al. No Need to Know Physics: Resilience of Process-based Model-free Anomaly Detection for Industrial Control Systems, *ACM ACSAC*, 2020. DOI: 10.1145/3427228.3427261.
10. Müller N., Ziras C., Heussen K. Assessment of Cyber-Physical Intrusion Detection and Classification for Industrial Control Systems, *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2022. DOI: 10.1109/SmartGridComm52983.2022.9961010.
11. Yahya M., Sharaf N., Rrushi J. et al. Physics Reasoning for Intrusion Detection in Industrial Networks, 2nd *IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 2020. DOI: 10.1109/TPS-ISA50397.2020.00043.
12. Aftabi N., Li D., Ramanan P. A Variational Autoencoder Framework for Robust, Physics-Informed Cyberattack Recognition in Industrial Cyber-Physical Systems, *arXiv:2310.06948*, 2023. DOI: 10.48550/arXiv.2310.06948.
13. Ike M., Phan K., Sadoski K. et al. SCAPHY: Detecting Modern ICS Attacks by Correlating Behaviors in SCADA and PHYsical, *Proc. IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 362-379. DOI: 10.1109/SP46215.2023.00067.
14. Basan E., Basan A., Nekrasov A., Fidge C., Ishchukova E., Basyuk A., Lesnikov A. Trusted Operation of Cyber-Physical Processes Based on Assessment of the System's State and Operating Mode, *Sensors*, 2023, Vol. 23, No. 4, pp. 1996. DOI: 10.3390/s23041996.

15. Ahmed I., Obermeier S., Naedele M. et al. SCADA systems: Challenges for forensic investigators, *Computer*, 2012, Vol. 45, No. 12, pp. 44-51. DOI: 10.1109/MC.2012.325.
16. Kabasele Ndonda G., Sadre R. Exploiting the Temporal Behavior of State Transitions for Intrusion Detection in ICS/SCADA, *IEEE Access*, 2022, Vol. 10, pp. 41535-41554. DOI: 10.1109/ACCESS.2022.3168864.
17. Asiri M., Saxena N., Gjomemo R., Burnap P. Understanding Indicators of Compromise against Cyberattacks in Industrial Control Systems: A Security Perspective, *ACM Transactions on Cyber-Physical Systems*, 2023, Vol. 7, No. 2. DOI: 10.1145/3565972.
18. Abramov E.S., Belov N.E. Klassifikatsiya i otsenka kachestva istochnikov indikatorov komprometatsii [Classification and quality assessment of sources of indicators of compromise], *Sistemnyy sintez i prikladnaya sinergetika: Sb. nauchnykh trudov XII Vseros. nauch. konf. [System Synthesis and Applied Synergetics: Proceedings of the XII All-Russian Scientific Conference]*. Rostov-on-Don; Taganrog: YuFU, 2024, pp. 392-395.
19. Tumanov D.A., Abramov E.S. Poisk i skoring istochnikov indikatorov komprometatsii po industriyam [Search and scoring of sources of indicators of compromise by industry], *Inzhenernyy vestnik Dona [Engineering Journal of Don]*, 2024, No. 8 (116).
20. Azzam M., Pasquale L., Provan G. et al. Forensic readiness of industrial control systems under stealthy attacks, *Computers & Security*, 2023, Vol. 125, pp. 103010. DOI: 10.1016/j.cose.2022.103010.
21. Radvanovsky R., Brodsky J. SCADA/Control Systems Security. Boca Raton: CRC Press, 2013, 330 p. – DOI: 10.1201/b19545.
22. Kotenko I.V., Khmyrov S.S. Model' komprometatsii ob"ektov kriticheskoy informatsionnoy infrastruktury [Model of compromise of critical information infrastructure objects], *Aktual'nye problemy infotelekkommunikatsiy v nauke i obrazovanii (APINO 2022) [Actual Problems of Infotelecommunications in Science and Education (APINO 2022)]*. Saint Petersburg., 2022, Vol. 1, pp. 614-619.
23. Knowles W., Prince D., Hutchison D. et al. A survey of cyber security management in industrial control systems, *International Journal of Critical Infrastructure Protection*, 2015, Vol. 9, pp. 52-80. DOI: 10.1016/j.ijcip.2015.02.002.
24. Mathur A.P. SWaT: a water treatment testbed for research and training on ICS security, *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*. IEEE, 2016, pp. 31-36. DOI: 10.1109/CySWater.2016.7469060.
25. Goh J. A dataset to support research in the design of secure water treatment systems, *Critical Information Infrastructures Security: 11th International Conference, CRITIS 2016*. Springer, 2017, pp. 88-99. DOI: 10.1007/978-3-319-71368-7_8.

Абрамов Евгений Сергеевич – Южный федеральный университет; e-mail: abramoves@sfedu.ru; г. Таганрог, Россия; тел.: +78634371905; к.т.н.; доцент.

Белов Николай Евгеньевич – Южный федеральный университет; e-mail: info@ictis.sfedu.ru; г. Таганрог, Россия; тел.: +78634360450; аспирант.

Веселов Геннадий Евгеньевич – Южный федеральный университет; e-mail: gev@sfedu.ru; г. Таганрог, Россия; тел.: +78634360450; директор ИКТИБ; д.т.н.; профессор.

Abramov Eugene Sergeevich – Southern Federal University; e-mail: abramoves@sfedu.ru; Taganrog, Russia; phone: +78634371905; cand. of eng. sc.; associate professor.

Belov Nikolay Evgen'evich – Southern Federal University; e-mail: info@ictis.sfedu.ru; Taganrog, Russia; phone: +78634360450; graduate student.

Veselov Gennadiy Evgen'evich – Southern Federal University; e-mail: gev@sfedu.ru; Taganrog, Russia; phone: +78634360450; director of ICTIS; dr. of eng. sc.; professor.