

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ, КОМПЛЕКСОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ/MATHEMATICAL SOFTWARE FOR COMPUTERS, COMPLEXES AND COMPUTER NETWORKS

DOI: https://doi.org/10.60797/IRJ.2026.171.27 EDN: WZPSHV

ИНФОРМАЦИОННО-ЭНТРОПИЙНЫЙ ПОДХОД К ОЦЕНКЕ УСТОЙЧИВОСТИ IIOT-СЕТЕЙ: МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДЕГРАДАЦИИ КИБЕРФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

Научная статья

Поборуева М.С.[1, *], Бодров О.А.[2]
[2] ORCID : 0009-0005-7225-6704;
[1, 2] Рязанский государственный радиотехнический университет имени В. Ф. Уткина, Рязань, Российская Федерация

* Корреспондирующий автор (imerm01[at]yandex.ru)

Предложена: 13.05.2026; Принята: 01.09.2026; Опубликована: 17.09.2026

Аннотация

Постановка проблемы. В настоящее время возникла необходимость количественной оценки устойчивости сетей промышленного интернета вещей (IIoT) к киберфизическим воздействиям. Классические методы теории надёжности и информационной безопасности не учитывают неопределённость поведения распределённых устройств, каскадные эффекты и прямую связь между искажением данных и потерей управляемости физическим процессом, что приводит к неспособности прогнозировать деградацию киберфизической безопасности.

Цель. Разработать математическую модель деградации киберфизической безопасности IIoT-сетей на основе информационно-энтропийного подхода, позволяющую количественно оценивать устойчивость системы как степень сохранения определённости состояния управляемого процесса.

Результаты. Предложен интегральный показатель энтропийной устойчивости, отражающий дезорганизацию информационных, вычислительных и физических процессов. Получены аналитические зависимости для оценки скорости деградации защищённости и предельных состояний сети. Выявлены три характерные фазы деградации: начальная адаптация, накопление неопределённости и квази-насыщение, при котором система теряет прогностическую управляемость даже при физической исправности оборудования.

Практическая значимость. Разработанная модель позволяет выявлять критические узлы, прогнозировать допустимое время безопасной эксплуатации IIoT-инфраструктуры и обосновывать стратегии адаптивной киберзащиты. Метод применим для обнаружения низкоинтенсивных «медленных» атак, не выявляемых традиционным мониторингом, и может служить основой для построения систем управления уровнем системной неопределённости в цифровом производстве.

Ключевые слова: IIoT, киберфизическая безопасность, информационная энтропия, устойчивость сетей, деградация систем, стохастические модели, риск-ориентированная защита.

AN INFORMATION-ENTROPY APPROACH TO ASSESSING THE RESILIENCE OF IIOT NETWORKS: A MATHEMATICAL MODEL OF CYBERPHYSICAL SECURITY DEGRADATION

Research article

Poborueva M.S.[1, *], Bodrov O.A.[2]
[2] ORCID : 0009-0005-7225-6704;
[1, 2] V.F. Utkin Ryazan State Radio Engineering University, Ryazan, Russian Federation

* Corresponding author (imerm01[at]yandex.ru)

Suggested: 13.05.2026; Accepted: 01.09.2026; Published: 17.09.2026

Abstract

Statement of the problem. There is now a need to quantitatively evaluate the resilience of Industrial Internet of Things (IIoT) networks to cyberphysical threats. Traditional methods of reliability theory and information security do not account for the uncertainty in the behaviour of distributed devices, cascading effects, or the direct link between data corruption and the loss of control over physical processes, which results in an inability to predict the degradation of cyberphysical security.

Objective. To develop a mathematical model of the degradation of cyberphysical security in IIoT networks based on an information-entropy approach, allowing for a quantitative assessment of the system's resilience as the degree to which the determinism of the controlled process's state is preserved.

Results. An integrated measure of entropy stability has been suggested, reflecting the disorganisation of information, computational and physical processes. Analytical relationships have been derived for assessing the rate of degradation of security and the limiting states of the network. Three characteristic phases of degradation have been identified: initial adaptation, accumulation of uncertainty and quasi-saturation, during which the system loses predictive controllability even when the equipment is physically sound.

Practical significance. The developed model makes it possible to identify critical nodes, predict the permissible duration of safe operation of IIoT infrastructure, and justify adaptive cyber defence strategies. The method is applicable for detecting low-

intensity ‘slow’ attacks that are not detected by traditional monitoring, and can serve as a basis for developing systems to manage the level of systemic uncertainty in digital manufacturing.

Keywords: IIoT, cyberphysical security, information entropy, network resilience, system degradation, stochastic models, risk-based protection.

Введение

Сети промышленного интернета вещей (Industrial Internet of Things, IIoT) являются ключевым компонентом цифровых промышленных экосистем, обеспечивающим интеграцию распределённых сенсорных и исполнительных устройств в единую киберфизическую среду. Современные IIoT-системы решают задачи сбора, обработки и передачи данных, а также непосредственного управления технологическими процессами в реальном времени. Для проектирования и обеспечения устойчивости таких систем необходима априорная информация не только о надёжности оборудования, но и о степени дезорганизации информационных, вычислительных и физических процессов под влиянием целенаправленных кибератак и каскадных отказов. Применение информационно-энтропийных мер для оценки состояния сложных динамических систем получило широкое распространение в таких задачах, как анализ сетевой живучести, прогнозирование отказов, управление рисками и обеспечение кибербезопасности. Наиболее эффективно задача количественной оценки устойчивости IIoT-сетей может быть решена методами математического моделирования деградации доверия к узлам системы.

Ввиду вышесказанного является актуальной задача разработки математической модели деградации киберфизической безопасности IIoT-сетей, основанной на информационной энтропии как универсальной мере неопределённости и потери управляемости. Первым шагом для построения такой модели является введение вероятностной метрики состояния каждого узла и описания динамики её изменения под действием атак и защитных механизмов.

Цель работы — разработать информационно-энтропийную математическую модель оценки устойчивости IIoT-сетей, позволяющую количественно описывать процесс деградации киберфизической безопасности.

В статье рассматривается задача оценки устойчивости IIoT-сети как стохастической динамической системы с распределёнными источниками неопределённости. В отличие от классических методов теории надёжности, ориентированных на отказ оборудования, в данной работе предложено использовать информационную энтропию для интегральной характеристики степени согласованности между реальным состоянием технологического процесса и его цифровым представлением, формируемым сетью. Такой подход позволяет учитывать целенаправленный характер кибератак, каскадные эффекты и динамическую перестройку топологии IIoT, что не обеспечивается традиционными показателями доступности, живучести или риска.

Основные результаты и обсуждение

2.1. Проблема оценки устойчивости IIoT как киберфизической системы

В рамках теоретических исследований решается задача разработки адаптивных математических моделей и алгоритмов, направленных на обеспечение киберфизической безопасности и оптимизацию взаимодействия интеллектуальных объектов в сетях IIoT. В традиционных телекоммуникационных и ИТ-системах устойчивость трактуется как способность сети сохранять связность и допустимые показатели QoS при отказах элементов. Однако для промышленного интернета вещей такая постановка оказывается недостаточной, поскольку IIoT представляет собой не информационную, а киберфизическую систему (Cyber-Physical System, CPS), в которой: данные влияют на алгоритмы управления, алгоритмы изменяют физические процессы, физические процессы формируют новые данные.

Таким образом, нарушение информационной безопасности вызывает не только потерю данных, но и физическую деградацию управляемого объекта.

Ключевая проблема заключается в том, что: классические показатели надёжности (доступность, надежность, отказоустойчивость) не отражают степень потери управляемости технологической системой.

Переосмысление устойчивости CPS активно обсуждается в международных стандартах и исследовательских программах цифровой промышленности [1], [2].

В методологических документах NIST устойчивость CPS связывается с понятием живучести, включающим способность системы предвидеть, выдерживать, адаптироваться и восстанавливаться, а не просто функционировать.

В стандартах промышленной автоматизации IEC подчёркивается, что для индустриальных сетей критично учитывать системные эффекты распространения ошибок управления, а не только сетевые инциденты.

Анализ научных публикаций последних лет показывает три выявленные группы противоречий [3], [4].

Таблица 1 - Результаты анализа публикаций

DOI: https://doi.org/10.60797/IRJ.2026.171.27.1

№	Выявленное противоречие	Следствие
1	Метрики ИБ оценивают защиту данных, а не корректность физического управления	«Безопасная» сеть может разрушать процесс
2	Теория надёжности предполагает случайные отказы, а кибератаки целенаправленные	Нарушается статистическая применимость моделей
3	Сетевые модели не учитывают	Ошибки малой мощности

№	Выявленное противоречие	Следствие
	семантику технологических данных	вызывают катастрофические эффекты

Иными словами, в IIoT возникает разрыв между информационной и физической интерпретацией устойчивости.

Рассмотрим три наиболее распространённых метода оценки.

1. Вероятностная надёжность. Описывает систему через вероятность безотказной работы:

$$R(t) = P\{T > t\} \quad (1)$$

где T — время до отказа.

Недостатком подхода является то, что он не различает отказ оборудования и подмену данных, при этом не учитывает эффект накопление недостоверности измерений.

2. Риск-ориентированные модели информационной безопасности

Оценка строится через ожидаемый ущерб:

$$\text{Risk} = \sum_k P_k \cdot \text{Damage}_k \quad (2)$$

Недостатком является статический характер оценки, которая не отражает динамику разрушения процессов управления.

3. Метрики сетевой живучести. Основаны на связности графа:

$$S = \frac{|V_{\text{active}}|}{|V|} \quad (3)$$

Недостатком является то, что сеть может оставаться связной, но передавать ложные данные в то время как физический объект уже вышел из допустимого режима работы.

Для киберфизической системы устойчивость должна определяться как: способность сохранять допустимую степень определённости состояния управляемого процесса. То есть ключевым становится не факт работы элементов, а уровень неопределённости в знаниях о системе. Это приводит к переходу от энергетической (структурной) метрики к информационной метрике устойчивости.

Если рассматривать IIoT как систему формирования знаний о физическом объекте, то атака есть процесс внесения неопределённости. Тогда естественной мерой деградации становится информационная энтропия.

Пусть:

X(t) — вектор истинных состояний технологического процесса,

X̂(t) — наблюдаемое системой состояние,

ε(t)=X(t)-X̂(t) – ошибка киберфизического восприятия.

Тогда устойчивость определяется не отказами, а ростом распределения ошибки p(ε,t). Энтропия этого распределения:

$$H(t) = -\int p(\varepsilon, t) \ln p(\varepsilon, t) d\varepsilon \quad (4)$$

характеризует степень «потери понимания» системой собственного состояния.

Представим IIoT-сеть графом G=(V,E), где каждый узел имеет состояние доверия P_i (t).

Под действием атак и защитных механизмов:

$$\frac{dP_i}{dt} = -\lambda_i(t) P_i(t) + \mu_i(t)\left(1 - P_i(t)\right) \quad (5)$$

где: $\lambda_i(t)$ — интенсивность деградационных воздействий,

$\mu_i(t)$ — интенсивность механизмов защиты и восстановления.

Таким образом, проблема оценки устойчивости IIoT заключается в необходимости следующих шагов.

1. Перейти от метрик отказов к метрикам неопределённости.
2. Учитывать направленный характер кибератак как источник отрицательной информации.
3. Моделировать безопасность как динамический процесс деградации знания о системе.
4. Связать информационные нарушения с физической потерей управляемости через энтропийные показатели.

Существующие методы анализа надёжности, риска и живучести не позволяют корректно оценивать устойчивость IIoT, поскольку игнорируют информационную природу киберфизической деградации. Решение заключается во введении информационно-энтропийной метрики, описывающей безопасность как процесс роста неопределённости состояния системы, что создаёт основу для построения прогностических моделей киберфизической устойчивости.

2.2. Информационно-энтропийная мера состояния безопасности

Для оптимизации маршрутизации в гетерогенных сетях IIoT разработана адаптивная математическая модель, использующая графовые нейронные сети (GNN). Модель учитывает топологию сети, динамические изменения и киберугрозы, такие как атаки типа «чёрная дыра».

В киберфизических системах промышленного интернета вещей нарушение функционирования проявляется прежде всего как искажение информационного представления о физическом процессе, а не как физическое разрушение инфраструктуры. Даже при полностью работоспособных каналах связи и оборудовании система может находиться в опасном состоянии вследствие: подмены телеметрии, задержек синхронизации, внедрения ложных управляющих команд, деградации доверия между узлами.

Следовательно, устойчивость IIoT-сети должна оцениваться через степень согласованности между: X(t) — реальным состоянием объекта управления и X̂(t) — оценкой состояния, формируемой цифровой системой.

Чем больше расхождение между X(t) и X̂(t), тем выше вероятность принятия ошибочных управляющих решений. Это расхождение носит вероятностный характер и естественным образом описывается через информационную энтропию.

Рассмотрим IIoT-сеть, содержащую N взаимодействующих устройств (датчиков, контроллеров, шлюзов, исполнительных механизмов) [5], [6]. Для каждого узла введём вероятность корректного функционирования:

$$P_i(t) = P\{\text{данные и функции узла i достоверны в момент t}\} \quad (6)$$

Эта величина отражает уровень доверия к узлу и агрегирует: вероятность отсутствия компрометации, корректность измерений, целостность программного состояния, синхронность с технологическим процессом.

Тогда состояние всей сети описывается вектором:

$$P(t) = P_1(t), P_2(t), \ldots, P_N(t) \quad (7)$$

Для количественной оценки неопределённости введём информационную энтропию сети [7], [8]:

$$H(t) = -\sum_{i=1}^{N} P_i(t) \ln P_i(t). \quad (8)$$

Данная величина характеризует степень потери определённости в знаниях системы о собственной работоспособности.

Физический смысл показателя H(t):

H(t) → 0 — система полностью наблюдаема и управляема;

умеренный рост H(t) — появление локальных недостоверностей;

резкий рост H(t) — начало каскадной киберфизической деградации;

H(t) → H_{max} = lnN — состояние функциональной дезорганизации.

В настоящем исследовании в качестве меры неопределённости используется энтропия Шеннона. Выбор обусловлен тем, что целью работы является количественная оценка общей степени потери определённости состояния IIoT-сети при постепенной деградации доверия к её узлам.

По сравнению с альтернативными энтропийными мерами энтропия Шеннона обладает рядом преимуществ.

Во-первых, она имеет непосредственную вероятностную интерпретацию и характеризует средний объём неопределённости случайной системы.

Во-вторых, она аддитивна для независимых компонентов, что позволяет естественным образом агрегировать вклад отдельных узлов сети.

В-третьих, она широко применяется в задачах анализа информационных процессов, кибербезопасности и оценки сложных технических систем, благодаря чему результаты исследования сопоставимы с существующими публикациями.

Альтернативные меры, такие как энтропия Реньи или энтропия Цаллиса, ориентированы на описание мультифрактальных распределений, тяжёлых хвостов или нелинейных статистических эффектов. Их использование целесообразно при исследовании сетей со сложной коррелированной динамикой и может рассматриваться как направление дальнейшего развития предложенной модели.

В работе энтропия вычисляется как сумма вкладов отдельных узлов, что соответствует предположению о статистической независимости их состояний.

Такое допущение является оправданным для первого этапа моделирования, когда вероятность компрометации каждого элемента определяется локальными процессами защиты и атаки и не зависит непосредственно от состояния соседних устройств.

При наличии выраженных каскадных эффектов более адекватной является модель, основанная на совместном распределении вероятностей состояний узлов $H(X_1,\ldots,X_N)$ или на графовой энтропии сети.

Использование подобных моделей позволяет учитывать корреляции между компонентами IIoT-инфраструктуры и представляет собой дальнейшее развитие предлагаемого подхода.

Для сопоставимости систем различного масштаба используем нормированную энтропию:

$$H_n(t) = H(t)/lnN, 0 \le H_n(t) \le 1 \quad (9)$$

Пусть ошибка наблюдения технологического состояния имеет распределение плотности p(ε,t). Тогда энтропия может быть записана в непрерывной форме (формула 4).

Рост этой величины означает увеличение диапазона возможных интерпретаций состояния объекта, то есть снижение достоверности управления.

Таким образом, энтропия выступает интегральной мерой киберфизического риска, объединяющей: информационные искажения, сетевые задержки, отказоустойчивость, последствия атак.

Изменение вероятности P_i (t) определяется конкуренцией двух процессов: дестабилизирующего воздействия (атаки, сбои, ошибки) и компенсирующего воздействия (обнаружение, фильтрация, восстановление). Тогда уравнение динамического баланса вычисляется по формуле 5.

Решение уравнения:

$$P_i(t) = \mu_i/(\lambda_i + \mu_i) + (P_i(0) - \mu_i/(\lambda_i + \mu_i))e^{(-(\lambda_i+\mu_i)^t)} \quad (10)$$

Это выражение показывает, что даже при сохранении физической работоспособности узел со временем переходит в состояние пониженного доверия, если $\lambda_i > \mu_i$.

Дифференцируя H(t), получим скорость потери организованности:

$$\frac{dH(t)}{dt} = -\sum_{(i=1)}^{N} \frac{dP_i}{dt(1+lnP_i(t))} \quad (11)$$

Подставляя динамику P_i (t):

$$\frac{dH(t)}{dt} = \sum_{(i=1)}^{N} [\lambda_i P_i - \mu_i(1-P_i)](1+lnP_i) \quad (12)$$

Данное выражение демонстрирует нелинейный характер деградации: на ранних стадиях рост энтропии медленный, при достижении критической массы недостоверных узлов возникает лавинообразный эффект, защита наиболее эффективна при воздействии на узлы с высоким вкладом в энтропию.

Для практической оценки введём интегральный показатель устойчивости на интервале наблюдения T:

$$S = 1 - \frac{1}{T}\int_0^T H_n(t)dt \quad (13)$$

Интерпретация критерия:

$S \geq 0{,}8$ — система устойчива к киберфизическим воздействиям;

$0{,}5 \leq S < 0{,}8$ — зона скрытой деградации;

$S < 0{,}5$ — потеря гарантированной управляемости;

$S \to 0$ — критическое состояние технологической безопасности.

Информационно-энтропийная метрика позволяет описать безопасность IIoT-сети как динамический процесс изменения уровня доверия к её элементам. В отличие от традиционных показателей надёжности, предложенный подход учитывает неопределённость данных, направленный характер кибератак и их влияние на физическое управление, что делает возможным количественное прогнозирование деградации киберфизической устойчивости.

Предлагаемая модель основана на следующих предположениях:

– вероятность компрометации каждого узла определяется локальными процессами атаки и восстановления;

– интенсивности процессов на рассматриваемом интервале считаются квазипостоянными;

– состояния узлов рассматриваются как статистически независимые.

Последнее предположение справедливо для распределённых IIoT-систем, в которых обмен данными между устройствами не приводит к непосредственному распространению компрометации.

В системах с высокой связанностью, общими программными компонентами или каскадным распространением атак данное допущение может нарушаться.

В этом случае модель может быть расширена посредством введения корреляционной матрицы взаимодействий либо использования совместной энтропии сети.

Для демонстрации применимости предложенной модели рассмотрим фрагмент IIoT-сети, состоящий из N=5 узлов (датчики, ПЛК, шлюз, исполнительный модуль и сервер аналитики) [9], [10].

Каждый узел характеризуется: интенсивностью кибервоздействий λ_i, интенсивностью восстановления (детектирование, фильтрация, перезапуск) μ_i, начальным уровнем доверия P_i (0).

Таблица 2 - Исходные параметры модели

DOI: https://doi.org/10.60797/IRJ.2026.171.27.2

Узел	λ_i (атаки)	μ_i (восстановление)	P_i (0)
1	0,06	0,09	0,95
2	0,05	0,08	0,92
3	0,07	0,10	0,96
4	0,04	0,07	0,90
5	0,08	0,09	0,94

Здесь $\lambda_i < \mu_i$, что соответствует наличию механизмов защиты, однако их эффективность различна.

Для каждого элемента используется полученное ранее решение (формула 10).

Предельное значение доверия для узла 1: $P_i^* = \frac{\mu_i}{(\lambda_i+\mu_i)} = \frac{0.09}{(0.06+0.09)} = 0.60$.

Даже при работающей защите доверие со временем снижается с 0,95 до 0,60, что отражает накопление неопределённости — характерное свойство киберфизических атак «малой интенсивности».

Энтропия сети в каждый момент времени:

$$H(t) = -\sum_{i=1}^{5} P_i(t)\ln P_i(t) \quad (14)$$

Нормированное значение:

$$H_n(t) = \frac{H(t)}{ln_5} \quad (15)$$

Этот показатель интерпретируется как доля утраченной определённости состояния системы.

На интервале наблюдения T устойчивость определяется по формуле 13. Численное интегрирование для рассматриваемого примера даёт значение S ≈ 0,32.

Полученное значение соответствует зоне скрытой киберфизической деградации: физическое оборудование продолжает функционировать, классические метрики доступности показывают норму, однако энтропия быстро растёт ($H_n(t) \to 1$), система теряет достоверность представления о процессе.

Это означает, что управление технологическим объектом становится статистически ненадёжным задолго до возникновения отказов.

На представленном графике (рис. 1) показано изменение нормированной энтропии H_n (t) во времени.

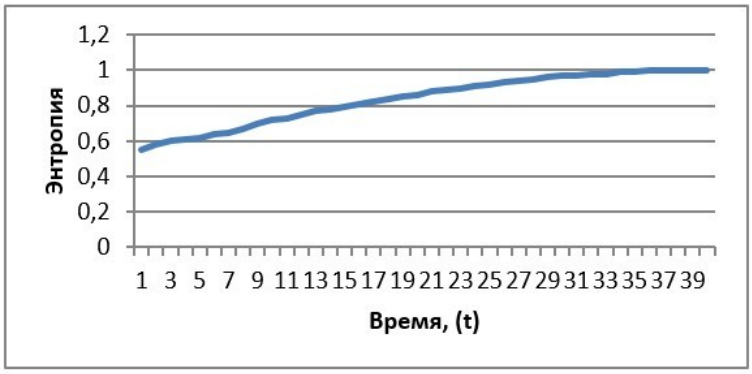

Рисунок 1 - Энтропийная деградация киберфизической стабильности
DOI: https://doi.org/10.60797/IRJ.2026.171.27.3

Наблюдаются три характерные фазы:

1. Начальная фаза адаптации (0–5 ед. времени). Незначительное увеличение энтропии — система компенсирует атаки штатными механизмами.

Фаза накопления неопределённости (5–20). Происходит экспоненциальный рост H_n (t), связанный с постепенной утратой доверия к данным.

Фаза квази-насыщения (после 20). Система входит в состояние высокой дезорганизации: $H_n(t) \approx 0{,}95$, что соответствует потере прогностической управляемости.

Даже при отсутствии катастрофических атак IIoT-сеть может деградировать за счёт длительных низкоинтенсивных воздействий, что: не выявляется традиционным мониторингом, но фиксируется через рост информационной энтропии.

Следовательно, предложенная модель позволяет: обнаруживать «медленные» атаки, оценивать допустимое время безопасной эксплуатации, обосновывать требования к скорости реагирования μ_i, выявлять узлы, дающие наибольший вклад в системную энтропию.

Для предварительной проверки адекватности предложенной модели использовался сценарный анализ поведения тестового фрагмента IIoT-сети.

Полученные зависимости соответствуют известным закономерностям функционирования киберфизических систем, описанным в современных исследованиях устойчивости CPS: увеличение интенсивности атак приводит к снижению уровня доверия узлов, росту информационной неопределённости и сокращению периода безопасной эксплуатации.

Кроме того, модель демонстрирует ожидаемое поведение при изменении отношения λ/μ.

При $\mu \gg \lambda$ энтропия стремится к низким значениям. При $\lambda \approx \mu$ наблюдается постепенный рост неопределённости.

При $\lambda > \mu$ возникает режим ускоренной деградации.

Качественное соответствие результатов известным закономерностям функционирования киберфизических систем рассматривается как предварительная (концептуальная) верификация разработанной модели. Количественная валидация на экспериментальных данных является предметом дальнейших исследований. Дальнейшая экспериментальная верификация планируется посредством имитационного моделирования IIoT-инфраструктуры в среде OMNeT++, NS-3 либо Cooja с последующим сравнением прогнозируемой энтропии с фактической динамикой компрометации узлов.

2.3. Математическая модель деградации киберфизической безопасности IIoT-сети

Для количественного анализа устойчивости IIoT-сети необходимо описать процесс её функционирования как динамическую стохастическую систему, находящуюся под воздействием дестабилизирующих факторов киберсреды.

В отличие от классических моделей отказов, где состояние элемента бинарно («работает/не работает»), в киберфизической системе узел может: функционировать физически, передавать данные, но находиться в состоянии частичной компрометации.

Поэтому вводится непрерывная переменная состояния доверия $P_i(t)$, отражающая вероятность корректности функционирования узла i.

Состояние IIoT-сети в момент времени t задаётся вектором:

$$X(t) = P_1(t), P_2(t), \dots, P_N(t)$$

где N — число взаимодействующих устройств.

Каждая компонента P_i (t)∈[0,1] интерпретируется как уровень: информационной достоверности, программной целостности, корректности взаимодействия с физическим процессом.

Таким образом, система развивается в непрерывном фазовом пространстве доверия.

На каждый узел одновременно действуют два противоположных процесса:

Деградация безопасности вызвана атаками, ошибками синхронизации, внедрением ложных данных λ_i.

Компенсация нарушений обеспечивается механизмами защиты: мониторинг, фильтрация, резервирование, самодиагностика μ_i (t).

Изменение доверия описывается уравнением динамического равновесия по формуле 5. Это уравнение аналогично кинетическим моделям необратимых процессов и отражает энтропийную природу деградации.

При квазистационарных воздействиях (λ_i, μ_i = const) решение имеет вид:

$$P_i(t) = P_i^* + (P_i(0) - P_i^*)e^{(-(\lambda_i+\mu_i)t)}$$

где стационарное значение:

$$P_i^* = \mu_i/(\lambda_i + \mu_i)$$

Это выражение показывает: система не возвращается к идеальному состоянию, устанавливается новый уровень доверия, зависящий от соотношения атаки и защиты, даже слабые, но постоянные воздействия снижают устойчивость.

Подставляя найденные P_i(t) в выражение энтропии (формула 8) получаем макроскопическое описание деградации всей сети [10].

Скорость изменения энтропии рассчитывается по формуле 12. Данное уравнение отражает ключевое свойство IIoT: безопасность деградирует нелинейно и может демонстрировать каскадные эффекты.

Система считается устойчивой, если энтропия не возрастает со временем: $dH(t)/dt \le 0$.

Отсюда следует критерий устойчивости для каждого узла: $\mu_i \ge \lambda_i$.

То есть скорость обнаружения и компенсации нарушений должна превосходить интенсивность атакующих воздействий.

При выполнении условия $\sum_{(i=1)}^{N}[\lambda_i \gg \sum_{(i=1)}^{N}\mu_i]$ система переходит в режим необратимой деградации $H(t) \to H_{max} = lnN$.

Это состояние соответствует: потере достоверной картины технологического процесса, невозможности корректного управления, риску аварий даже при физической исправности оборудования.

Введём время допустимой эксплуатации T_{safe}, при котором энтропия достигает предельно допустимого значения H_{crit}: $H(T_{safe}) = H_{crit}$

Решая это уравнение, можно прогнозировать момент, когда система утратит требуемый уровень киберфизической устойчивости.

Это даёт возможность: планировать профилактическое вмешательство, адаптировать архитектуру защиты, управлять жизненным циклом IIoT-инфраструктуры.

Разработанная математическая модель описывает безопасность IIoT-сети как динамический процесс конкуренции деградации и восстановления доверия к её элементам. В отличие от традиционных подходов, она позволяет анализировать не только факт нарушения, но и скорость накопления неопределённости, определяющую реальную устойчивость киберфизической системы и время её безопасного функционирования.

Заключение

Разработан информационно-энтропийный метод оценки устойчивости IIoT-сетей, позволяющий описывать безопасность как динамический процесс изменения организованности киберфизической системы. Предложенная математическая модель: формализует деградацию безопасности через рост энтропии, связывает интенсивность атак и эффективность защиты, вводит количественный критерий устойчивости, позволяет прогнозировать критические состояния цифрового производства.

Метод может служить основой для построения адаптивных систем киберзащиты следующего поколения, ориентированных не на реакцию на инциденты, а на управление уровнем системной неопределённости.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы на английском языке / References in English

1. Zhukabayeva T. Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions / T. Zhukabayeva, L. Zholshiyeva, N. Karabayev [et al.] // Sensors. — 2025. — Vol. 25. — P. 213. — DOI: 10.3390/s25010213.

2. Yang Ze. Complex Network Evolution with Node Strategies Driven by Information Entropy / Ze Yang, Y. Tian, J. Xiong [et al.] // SSRN. — DOI: 10.2139/ssrn.5163067.

3. Su J. A Hybrid Entropy and Blockchain Approach for Network Security Defense in SDN-Based IIoT / J. Su, M. Jiang // Chinese Journal of Electronics. — 2023. — Vol. 32. — P. 531–541. — DOI: 10.23919/cje.2022.00.103.

4. Wu L. Privacy and security trade-off in cyber-physical systems: An information theory-based framework / L. Wu, H. Wang, K. Liu [et al.] // International Journal of Robust and Nonlinear Control. — 2024. — Vol. 34. — P. 5110–5125. — DOI: 10.1002/rnc.7252.

5. Garofalaki Z. A Security Assessment Platform for Stochastic Petri Net (SPN) Modelling in the Internet of Things (IoT) Ecosystem / Z. Garofalaki, D. Kallergis, C. Douligeris. — 2022. — DOI: 10.1007/978-3-030-93547-4_13.

6. Chehade S. Entropy of the Quantum-Classical Interface: A Potential Metric for Security / S. Chehade, J. Dawson, S. Prowell [et al.]. — 2025. — DOI: 10.20944/preprints202502.1598.v1.

7. Kornyo O. Enhancing AMI Network Security with STI Model: A Mathematical Perspective / O. Kornyo, B. Tei Partey, M. Asante [et al.] // Internet of Things. — 2024. — Vol. 27. — P. 101244. — DOI: 10.1016/j.iot.2024.101244.

8. Okunlola O. Cybersecurity Solutions for Industrial Internet of Things-Edge Computing Integration: Challenges, Threats, and Future Directions / O. Okunlola, J. Olaoye, O. Okunlola [et al.] // International Journal of Future Engineering Innovations. — 2025. — Vol. 2. — P. 87–95. — DOI: 10.54660/IJFEI.2025.2.2.87-95.

9. Chataut R. Unleashing the power of IoT: a comprehensive review of IoT applications and prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0 / R. Chataut, A. Phoummalayvane, R. Akl // Sensors (Basel). — 2023. — Vol. 23, № 16. — P. 7194.

10. Chunlei W. An entropy theory based large-scale network survivability measurement model / W. Chunlei, L. Li, C. Guojiu // Proceedings of 2014 4th IEEE International Conference on Network Infrastructure and Digital Content, IEEE IC-NIDC 2014. — 2014. — P. 240–246. — DOI: 10.1109/ICNIDC.2014.7000302.