Кибербезопасность как критический фактор цифровой трансформации энергетической инфраструктуры Индии

Шагап Василий Андреевич,
Соловьёва Юлиана Владимировна,
Российский университет дружбы народов им. Патриса Лумумбы (РУДН)
117198, г. Москва, ул. Миклухо-Маклая, д.6

В статье исследуется критическая роль кибербезопасности в процессе цифровой трансформации энергетической инфраструктуры Индии. Анализируется диалектическое противоречие между повышением операционной эффективности за счет внедрения цифровых технологий (Smart Grid, ВИЭ, IoT) и одновременным расширением поверхности для кибератак. Рассматривается эволюция нормативно-правовой базы и институциональных механизмов Индии в области кибербезопасности, выявляются ключевые вызовы, связанные с импортозависимостью и уязвимостью цепочек поставок. На основе проведенного анализа формулируются рекомендации по разработке комплексного подхода, сочетающего регуляторное давление, развитие национального технологического потенциала и международное сотрудничество.

Ключевые слова*: кибербезопасность, энергетическая инфраструктура, Индия, цифровая трансформация, Smart Grid, критическая информационная инфраструктура (КИИ), CERT-In, нормативное регулирование, импортозависимость.*

JEL*: O33, L94, K24, F52.*

Cybersecurity as a critical factor in the digital transformation of India's energy infrastructure

Shagap Vasiliy Andreevich,
Solovieva Yuliana Vladimirovna,
Peoples' Friendship University of Russia named after Patrice Lumumba (RUDN)
117198, Moscow, Russia, Miklukho-Maklaya st., 6

The article examines the pivotal role of cybersecurity in the digital transformation of India's energy infrastructure. It explores the tension between enhanced operational efficiency through digital technologies (Smart Grid, RES, IoT) and the increased vulnerability to cyberattacks. The study traces the evolution of India's cybersecurity regulatory framework and institutional mechanisms, highlighting challenges posed by import dependence and supply chain risks. Based on this analysis, it proposes a holistic strategy integrating robust regulation, national technological development, and international collaboration.

Keywords*: cybersecurity, energy infrastructure, India, digital transformation, Smart Grid, critical information infrastructure (CII), CERT-In, regulatory regulation, import dependence.*

JEL*: O33, L94, K24, F52.*

Введение

Внедрение интеллектуальных сетей (Smart Grid), распределенной генерации на основе возобновляемых источников энергии (ВИЭ) и интернета вещей (IoT) позволяет повысить эффективность, надежность и устойчивость энергоснабжения. Однако эта же трансформация коренным образом меняет ландшафт киберугроз. Традиционно изолированные операционные технологии (OT) интегрируются с корпоративными IT-сетями и интернетом, создавая расширенную и уязвимую поверхность для атак. Для Индии, переживающей масштабную модернизацию энергетической инфраструктуры и ставящей амбициозные цели по переходу на ВИЭ, обеспечение кибербезопасности становится не просто технической задачей, а критическим фактором национальной безопасности и экономической стабильности. Как показывают данные отчета Cisco Cybersecurity Readiness Index, общий уровень готовности индийских организаций к современным киберугрозам остается низким: лишь 24% компаний были оценены как достигшие «зрелого» уровня. При этом 80% респондентов в Индии уже сталкивались с киберинцидентами в течение 2023 года, а более половины из них понесли убытки свыше 500 тысяч долларов США [8]. Это свидетельствует о том, что киберугрозы носят для Индии не теоретический, а вполне осязаемый экономический характер.

Целью данной работы является комплексный анализ проблемы кибербезопасности как неотъемлемого элемента цифровой трансформации энергетики Индии, оценка принимаемых государством мер и выработка рекомендаций по формированию целостной стратегии.

Методы исследования включают системный анализ научной литературы и официальных документов, разбор нормативной базы, а также обобщение и синтез данных для выявления ключевых тенденций, вызовов и пробелов в современной политике Индии в области кибербезопасности энергетической инфраструктуры.

Обзор литературы

Проблема обеспечения информационной безопасности критической инфраструктуры, в частности энергетического сектора, находится в фокусе внимания международного научного сообщества. Исследования в данной области охватывают широкий спектр вопросов — от анализа нормативно-правовых рамок до разработки технических решений для противодействия сложным киберугрозам.

Эволюции регуляторного ландшафта и институциональных механизмов Индии в сфере информационной безопасности посвящена работа Матюхиной Е.Н. [2]. Вопросы нормативного регулирования и соответствия международным стандартам, включая рамки NIST и ISO/IEC 27019, также затрагиваются в исследованиях Sanders et al. [29].

Как показывают исследования, в условиях «постоянных преобразований мировой экономики, расширения интеграционных составляющих под влиянием геополитических и геоэкономических процессов происходит трансформация мирового энергетического сектора, появляются новые тенденции и особенности развития, возрастает зависимость национальных экономик от уровня собственного энергетического потенциала и от мировых энергетических возможностей в целом» [3, С. 118]. Powell et al. [27] проводят комплексный обзор проблем и тенденций развития Smart Grid, в то время как Hassine et al. [16] акцентируют внимание на уязвимостях импортируемого оборудования, такого как контроллеры электростанций (Power Plant Controller — PPC) [16; 27]. Угрозы целенаправленных атак (Advanced Persistent Threats — APTs) на объекты энергетики, включая печально известные инциденты вроде Stuxnet, детально проанализированы в работе Venkatachary S.K. et al. [33]. Особое место занимает анализ специфических для умных сетей электроснабжения атак, таких как внедрение ложных данных (False Data Injection — FDI). Исследование Habib et al. [15] подробно описывает механизмы FDI-атак, которые позволяют злоумышленникам манипулировать данными измерений, оставаясь необнаруженными традиционными системами, что может привести к

катастрофическим последствиям для стабильности сети. В своей работе Morya и Singh [25] подробно анализируют операционные вызовы, включая кадровый дефицит и низкий уровень готовности организаций.

Несмотря на значительный объем существующих исследований, комплексный анализ, интегрирующий технологические, регуляторные и геоэкономические аспекты кибербезопасности энергетической инфраструктуры Индии, представлен недостаточно. При этом, в соответствии с прогнозами, «лидерами по абсолютному росту энергопотребления станут Индия и Китай, дающие более половины мирового прироста» [3, С. 128]. Новизна данного исследования заключается в синтезе анализа последних нормативных инициатив (таких как проект CEA Cyber Security Regulations 2024 [8]), актуальных данных о киберугрозах (India Cyber Threat Report 2025 [17]) и глубокой оценки рисков цепочек поставок [11] для формирования целостного видения проблемы. Такой многосторонний подход позволяет не только выявить системные противоречия между цифровой трансформацией и кибербезопасностью, но и сформулировать комплексные рекомендации.

Дилемма цифровизации: повышение эффективности и расширение поверхности атаки

Цифровая трансформация энергетической инфраструктуры представляет собой фундаментальный сдвиг, несущий в себе диалектическое противоречие. С одной стороны, она открывает путь к значительному повышению операционной эффективности, надежности и устойчивости энергоснабжения. С другой — коренным образом меняет ландшафт киберугроз, создавая новые, зачастую невидимые уязвимости. Для Индии, осуществляющей масштабную модернизацию своего энергетического сектора, понимание этой дилеммы является критически важным.

Внедрение цифровых технологий приносит ряд неоспоримых преимуществ, ключевыми из которых являются операционная эффективность, интеграция возобновляемых источников и расширенный мониторинг. По данным

Международного энергетического агентства (IEA), цифровизация позволяет оптимизировать управление сетями, снизить эксплуатационные затраты и ускорить интеграцию переменных возобновляемых источников энергии (ВИЭ) [9; 12]. Фундаментом этой трансформации выступают интеллектуальные сети (Smart Grid), обеспечивающие двусторонний поток энергии и данных. Это позволяет оптимизировать управление спросом и предложением и значительно снижать коммерческие и технические потери, уровень которых в некоторых регионах Индии достигает 62% [29]. Интеграция ВИЭ, в свою очередь, требует развертывания сложных систем прогнозирования и управления для компенсации их переменного характера и обеспечения стабильности сети. Кроме того, массовое внедрение технологий Интернета вещей (IoT), таких как интеллектуальные счетчики (AMI), датчики и контроллеры, обеспечивает детальный мониторинг состояния сети в реальном времени. Это создает основу для внедрения гибких тарифов, автоматического обнаружения и локализации повреждений, что в конечном итоге повышает надежность и потребительский опыт.

Параллельно с ростом эффективности каждый элемент цифровизации создает новые векторы для кибератак. Наиболее значительным системным изменением является интеграция традиционно изолированных операционных технологий (OT) с корпоративными IT-сетями и интернетом, что радикально увеличивает поверхность для потенциальных атак. Интеллектуальные сети, будучи масштабными киберфизическими системами, становятся целями для атак на конфиденциальность, целостность и доступность данных (модель CIA) [27]. Компрометация центров управления или ключевых узлов такой сети может привести к каскадным отказам с серьезными последствиями. Дополнительный риск возникает в цепочке поставок для объектов возобновляемой энергетики. Критически важные компоненты ключевого оборудования в данной отрасли часто импортируются и, как отмечается в отчете Национального института преобразования Индии (NITI Aayog), могут содержать преднамеренно или случайно внедренные уязвимости, становясь точками входа в национальную

энергосистему [11]. Наконец, периметр сети расширяется до миллионов подключенных IoT-устройств, многие из которых изначально не проектировались с учетом строгих требований кибербезопасности. Эти устройства, в частности умные счетчики, часто имеют слабые механизмы аутентификации и могут быть использованы злоумышленниками в качестве плацдарма для организации атак на системы управления более высокого уровня, такие как SCADA [12].

Таким образом, ключевая дилемма заключается в неразрывной связи между операционной эффективностью и киберрисками: повышение гибкости и уровня цифровизации системы неминуемо ведет к усложнению ее архитектуры и росту числа уязвимых точек. Этот фундаментальный вопрос требует выработки сбалансированного подхода, особенно в контексте специфических угроз, с которыми сталкивается энергетическая инфраструктура Индии, как будет показано в следующем разделе.

Ландшафт угроз для энергетической инфраструктуры Индии

Энергетическая инфраструктура Индии, находящаяся в процессе активной цифровизации, сталкивается с многоуровневым и эволюционирующим ландшафтом киберугроз. Ключевыми вызовами являются целевые атаки (Advanced Persistent Threats, APT), риски цепочек поставок и уязвимости, порождаемые интеграцией информационных и операционных технологий.

Наблюдается значительная активность групп APT, нацеленных на критически важные объекты энергетического сектора. Например, группа RedEcho ассоциируется с использованием вредоносного загрузчика ShadowPad против индийских диспетчерских центров и электростанций, в то время как группа SideCopy, действующая из Пакистана, применяла фишинг и уязвимости в популярном ПО для атак на оборонные и энергетические структуры региона [1].

Фундаментальную уязвимость создает высокая импортозависимость от критически важного оборудования и программного обеспечения, что порождает

серьезные риски цепочек поставок. Исследование NITI Aayog [11] прямо указывает на опасности, связанные с доминированием иностранных, в частности китайских, OEM-производителей на рынке компонентов для ветроэнергетики. Эта зависимость создает риски внедрения аппаратных и программных закладок (backdoors) на этапе проектирования и производства, которые практически невозможно обнаружить на национальном уровне из-за отсутствия лабораторий, способных проводить тестирование на уровне чипов.

Интеграция операционных (OT) и информационных технологий (IT), необходимая для повышения эффективности, одновременно создает новые векторы атак. Использование устаревших протоколов, отсутствие шифрования данных и слабые механизмы аутентификации в сегментах OT делают их уязвимыми при подключении к корпоративным сетям. Особую озабоченность вызывают атаки путём внедрения ложных данных (False Data Injection, FDI), при которых манипуляция показаниями измерительных устройств может оставаться необнаруженной традиционными системами и приводить к принятию некорректных оперативных решений, нарушению баланса системы и масштабным отключениям электроэнергии [15].

Таким образом, ландшафт угроз характеризуется сочетанием сложных целевых атак и массовых эксплуатаций уязвимостей, усугубляемым структурной зависимостью от импорта и операционными пробелами внутри отрасли. Этот комплексный характер угроз подчеркивает необходимость столь же многоуровневого ответа.

Ответ государства: Эволюция регуляторной рамки

Индия демонстрирует растущее осознание киберрисков, связанных с цифровизацией энергетического сектора, и предпринимает активные шаги по формированию комплексной нормативно-правовой базы. Эволюция системного подхода индийского правительства к защите информации, как подробно изучено в работе Матюхиной Е.Н. [2], прошла несколько ключевых этапов,

характеризующихся переходом от общих законов к узкоотраслевым, детализированным и строгим нормативным актам.

Фундаментальной основой регулирования стал Закон об информационных технологиях (Information Technology Act, 2000), который заложил базовые принципы работы в киберпространстве и был существенно усилен поправками 2008 года. Важным институциональным шагом стало создание в 2004 г. национального центра реагирования на компьютерные инциденты CERT-In (Indian Computer Emergency Response Team). Дальнейшее развитие было связано с принятием Национальной политики кибербезопасности 2013 г., в рамках которой были учреждены Национальный центр защиты критической информационной инфраструктуры (NCIIPC) и Национальный координационный центр по кибербезопасности (NCCC), что ознаменовало переход к целевой защите объектов критической информационной инфраструктуры (КИИ).

Знаковым событием для энергетического сектора стало принятие Центральным управлением по электроэнергии (Central Electricity Authority, CEA) в 2021 г. «Руководящих принципов по кибербезопасности в энергетическом секторе» (Cyber Security Guidelines) [7]. Этот документ установил обязательные для всех субъектов отрасли требования, введя принцип жесткой сегментации операционных (OT) и информационных (IT) технологий, обязав назначать ответственных за информационную безопасность (Chief Information Security Officer, CISO) и проводить регулярные аудиты.

Новейший этап регуляторного ужесточения связан с инициативами 2023-2024 гг. Центральная комиссия по регулированию электроэнергии (CERC) утвердила Кодекс электросетей (IEGC), глава 8 которого описывает надежные рамки кибербезопасности для национальной энергосистемы и создает Форум координации по кибербезопасности (Cyber Security Coordination Forum, CSCF) для обмена информацией об угрозах [26]. Кроме того, в 2024 г. был разработан амбициозный проект «Положений о кибербезопасности в электроэнергетическом секторе» (CEA Cyber Security Regulations Draft 2024),

призванный стать комплексным нормативным актом, усиливающим защиту КИИ и ОТ [8].

Кульминацией этого процесса стало объявление о вступлении в силу со 2 января 2026 г. нового строгого закона о кибербезопасности для энергетического сектора, как сообщает издание EQ International [19]. Новый режим обязывает все компании сектора, включая генерирующие, передающие и распределительные организации, соблюдать строгие стандарты защиты, проводить обязательные аудиты и тестирование на проникновение, а также незамедлительно сообщать в CERT-In о любых инцидентах.

Институциональный механизм

Формирование надежной нормативной базы является необходимым, но недостаточным условием для обеспечения кибербезопасности. Его эффективность напрямую зависит от наличия компетентных институтов, способных реализовывать политику на практике. В ответ на растущие угрозы Индия сформировала многоуровневую институциональную архитектуру, предназначенную для координации, реагирования и управления рисками в киберпространстве.

Ключевым национальным органом, координирующим деятельность в области компьютерной безопасности, выступает CERT-In (Indian Computer Emergency Response Team). Он выполняет функции центрального узла по сбору, анализу и распространению информации о киберинцидентах, а также обеспечивает методическую поддержку. За защиту объектов критической информационной инфраструктуры (КИИ) отвечает NCIIPC (National Critical Information Infrastructure Protection Centre), который определяет и классифицирует такие объекты, разрабатывает профили их защиты и стандарты безопасности.

Для специализированной поддержки энергетического сектора при Центральном управлении по электроэнергии (CEA) в 2023 г. была создана отраслевая группа реагирования на киберинциденты CSIRT-Power [14]. Её дополняют шесть профильных CERT, учрежденных Министерством энергетики

для отраслей тепловой, гидроэнергетики и передачи электроэнергии. Важным элементом координации стал упомянутый выше Форум координации по кибербезопасности (Cyber Security Coordination Forum, CSCF). Он служит платформой для оперативного обмена информацией об угрозах и лучшими практиками между операторами критической инфраструктуры.

Таким образом, Индия демонстрирует прогресс в построении скоординированной и специализированной институциональной системы, соответствующей вызовам цифровой трансформации. Однако, несмотря на эти достижения, эффективность даже самой развитой нормативной и институциональной системы может быть нивелирована внешними факторами. Наиболее значимым из них, создающим фундаментальную уязвимость, остается высокая импортозависимость от критически важного оборудования и программного обеспечения, что будет детально проанализировано в следующем разделе.

Геополитические аспекты кибербезопасности: уязвимости цепочек поставок в индийской энергетике

Несмотря на значительный прогресс в построении нормативно-правовой и институциональной базы, ключевой вызов для кибербезопасности энергетического сектора Индии остается нерешенным. Речь идет о глубокой импортозависимости от критически важного оборудования и программного обеспечения, что создает фундаментальные, системные уязвимости, находящиеся вне зоны прямого действия национальных регуляторов. Даже самые строгие внутренние предписания оказываются бессильны против уязвимостей и преднамеренных закладок, внедренных на этапах проектирования и производства за рубежом.

Ярче всего эта проблема проявляется в ветроэнергетическом секторе, анализ которого был детально проведен NITI Aayog в 2024 г. Доминирование иностранных оригинальных производителей оборудования (OEM), в особенности китайских, которые контролируют до 61% глобальных мощностей

по сборке ветряных турбин, создает прямые риски для национальной безопасности [23]. Эти производители, получая значительные государственные субсидии и экспортные льготы от правительства Китая, доминируют в цепочке поставок критически важных компонентов, таких как контроллеры электростанций (Power Plant Controller — PPC) и связанное с ними программное обеспечение. Данная зависимость от геополитического конкурента создает высокие риски внедрения аппаратных и программных закладок, которые могут быть активированы удаленно для дестабилизации работы энергосистемы.

Проблема усугубляется архитектурой удаленного управления и утечкой данных. Иностранные OEM-производители часто размещают серверы для сбора телеметрии и центры исследований и разработок (НИОКР) за пределами Индии. Эта практика позволяет осуществлять несанкционированный удаленный мониторинг и управление критическими активами, а также приводит к постоянной утечке чувствительных данных о работе национальной энергосистемы в юрисдикции, не подконтрольные индийским властям. Последние инициативы правительства Индии по стимулированию локализации производства, включая включение ветровой энергетики в схему Production Linked Incentive (PLI), направлены на снижение этой зависимости, однако процесс создания полноценной отечественной цепочки поставок займет годы [20].

Киберриски, проистекающие из импортозависимости, не ограничиваются ветровой энергетикой и носят системный характер. Как подчеркивается в анализе Observer Research Foundation (ORF), энергетическая инфраструктура в целом находится на передовой гибридных угроз, где кибератаки становятся инструментом геополитического противостояния [30]. Это подтверждается недавними инцидентами: в июле 2025 г. Bloomberg сообщил, что индийские регуляторы начали расследование в отношении нескольких производителей солнечных инверторов, преимущественно китайских, по подозрению во внедрении вредоносного ПО, которое могло бы позволить удаленно нарушать работу объектов солнечной генерации [18]. Данный случай наглядно

иллюстрирует, как уязвимости в цепочке поставок могут быть использованы для проведения скоординированных атак на энергосистему.

Фундаментальным препятствием для предотвращения этих рисков является отсутствие в Индии достаточных национальных мощностей для глубокого тестирования импортируемого оборудования. Существующие лаборатории, такие как STQC, способны проводить анализ программного обеспечения только при условии предоставления исходного кода, что маловероятно со стороны иностранных поставщиков. При этом критически важное тестирование на уровне аппаратного обеспечения (аппаратные закладки, hardware trojans) практически не осуществляется из-за отсутствия необходимой технической экспертизы и оборудования. Как отмечает Hemant Mahajan в своем исследовании для Indus Research, сочетание кибератак с новыми формами угроз, такими как дроны, нацеленными на энергетическую инфраструктуру, требует срочного развития собственных возможностей для аудита и тестирования безопасности [24]. Таким образом, импортозависимость ставит под сомнение саму эффективность национальной стратегии кибербезопасности, поскольку уязвимости закладываются на этапе, предшествующем действию каких-либо внутренних регуляторных норм.

Данный системный вызов, основанный на геоэкономической зависимости, определяет необходимость перехода от исключительно регуляторных мер к комплексной стратегии, сочетающей развитие собственного производства, инвестиции в НИОКР и международное сотрудничество. Это закономерно подводит к вопросу о том, насколько текущие подходы Индии к обеспечению киберустойчивости адекватны для противодействия столь сложным и многоуровневым угрозам.

Киберустойчивость: оценка текущих подходов

Проведенный обзор нормативных и институциональных мер демонстрирует значительный прогресс Индии в осознании киберрисков и формировании комплексного ответа. Однако возникает закономерный вопрос: насколько

амбициозные регуляторные цели соответствуют техническим и операционным возможностям отрасли для их практической реализации? Анализ выявляет ряд системных проблем, создающих разрыв между декларируемыми целями и реальной практикой.

Фундаментальной уязвимостью, нивелирующей эффективность внутренних мер, остается технологическая импортозависимость. Как показано в разделе о ветроэнергетике, зависимость от импорта критического оборудования, такого как контроллеры электростанций из Китая, делает бессильными даже самые строгие внутренние предписания против преднамеренных закладок, внедренных на этапах проектирования и производства. Эта проблема усугубляется отсутствием в Индии национальных лабораторий, способных проводить глубокое тестирование на уровне аппаратного обеспечения (hardware trojans), что соответствует глобальным вызовам, отмеченным МЭА [9, 12].

Кадровый дефицит серьезно подрывает операционную безопасность энергетического сектора Индии. По данным Международного консорциума по сертификации безопасности информационных систем (ISC2), в стране не хватает около 800 000 специалистов по кибербезопасности, особенно в области операционных технологий (OT) [12]. Этот дефицит усугубляет уязвимость сектора на фоне роста киберугроз: по данным CERT-In, с 2018 по 2022 г. количество инцидентов в энергетическом секторе увеличилось на 278%, причем атаки преимущественно нацелены на системы SCADA и смарт-устройства [19]. Согласно отчету India Cyber Threat Report 2025, 73% организаций не имеют представления о том, подвергались ли они атакам, а 57% не соблюдают базовые принципы кибергигиены [23]. В результате, готовность энергетических компаний остается на низком уровне: исследование Morya и Singh [25] показывает, что лишь 27% организаций располагают специализированными командами по безопасности OT, что резко контрастирует с более зрелыми рынками, такими как ЕС.

Непосредственную угрозу стабильности создают операционные сложности. Многие энергокомпании, особенно в распределительном сегменте,

работают на устаревшей инфраструктуре и имеют ограниченные ресурсы для полноценного внедрения предписаний CEA. Это усиливает риски, связанные с конвергенцией IT/OT и целевыми атаками, такими как внедрение ложных данных (False Data Injection, FDI) [15]. Актуальность этой угрозы подтверждается данными India Cyber Threat Report 2025: в 2024 году 48% всех атак на энергетический сектор были нацелены на системы SCADA и промышленные системы управления (ICS) [17].

Несмотря на создание разветвленной институциональной архитектуры, сохраняются координационные пробелы. Эффективное взаимодействие между государством, частным сектором и международными партнерами, как подчеркивается в системном обзоре Nuraeni et al. [26], требует дальнейшего улучшения для обеспечения своевременного обмена информацией об угрозах и выработки скоординированных ответных мер.

Таким образом, существует значительный разрыв между амбициозными целями регуляторов и операционными возможностями отрасли, усугубляемый внешними факторами. Этот разрыв подчеркивает необходимость перехода от исключительно регуляторного давления к комплексной стратегии, сочетающей инвестиции в национальный технологический потенциал, развитие человеческого капитала и укрепление международной кооперации.

Выводы и рекомендации

Проведенный анализ свидетельствует, что кибербезопасность является не вспомогательным элементом, а критическим фактором цифровой трансформации энергетической инфраструктуры Индии. Несмотря на значительный прогресс в формировании комплексной нормативно-правовой базы и институциональной архитектуры, системная уязвимость, порождаемая импортозависимостью от критических технологий, создает фундаментальный вызов, который невозможно преодолеть исключительно мерами внутреннего регулирования.

В качестве стратегического ответа предлагается холистический подход, интегрирующий несколько взаимодополняющих направлений. Первым направлением является продолжение курса на ужесточение и детализацию отраслевых требований, включая обязательную сертификацию всего импортного оборудования и программного обеспечения национальными органами, что соответствует лучшим международным практикам, таким как рамки NIST.

Второе ключевое направление связано с развитием национального технологического суверенитета. Это предполагает создание экономических стимулов для локализации производства критических компонентов, включая контроллеры электростанций, и размещения центров НИОКР иностранных компаний на территории Индии. Параллельно необходимы целевые инвестиции в исследования и разработки, а также создание испытательных лабораторий, способных проводить глубокий анализ, в том числе на уровне аппаратного обеспечения. Важнейшим элементом является преодоление кадрового дефицита через развитие образовательных программ в области безопасности операционных и информационных технологий.

Третье направление заключается в активизации международного сотрудничества. Участие в международных форумах и заключение двусторонних соглашений с дружественными странами позволит наладить обмен информацией об угрозах и скоординировать ответ на трансграничные киберриски.

Наконец, устойчивость системы невозможно обеспечить без внедрения передовых технологий. Искусственный интеллект (AI) и машинное обучение для систем обнаружения вторжений, цифровые двойники (digital twins) для моделирования атак и тестирования защиты, а также блокчейн (blockchain) для обеспечения целостности и прозрачности данных формируют многоуровневый киберзащитный каркас, способный противостоять сложным целевым атакам.

Таким образом, лишь комплексный подход, сочетающий жесткое регулирование, развитие внутреннего потенциала, международную кооперацию и технологическую модернизацию, позволит Индии обеспечить

киберустойчивость своей энергетической инфраструктуры в условиях цифровой трансформации.

Список литературы

1. APT-атаки на промышленные компании в первом полугодии 2021 г. Kaspersky ICS CERT [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-Ru.pdf (дата обращения: 09.09.2025).
2. Матюхина Е.Н. Эволюция инфраструктуры информационной и кибербезопасности Индии // СибСкрипт. – 2024. – №3 (33) [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/evolyutsiya-infrastruktury-informatsionnoy-i-kiberbezopasnosti-indii (дата обращения: 09.09.2025).
3. Соловьева Ю.В., Черняев М.В. Энергоемкость экономики и энергоэффективность: проблемы и перспективы // ЭТАП: экономическая теория, анализ, практика. – 2019. – № 6. – С. 118-130. DOI 10.24411/2071-6435-2019-10127.
4. Bellamkonda S. Ransomware attacks on critical infrastructure: A study of the Colonial Pipeline incident // International Journal of Research in Computer Applications and Information Technology. – 2024. – Vol. 7. – Issue 2. – Pp. 1423–1433 [Электронный ресурс]. URL: www.researchgate.net/publication/386014193_Ransomware_Attacks_On_Critical_Infrastructure_A_Study_Of_The_Colonial_Pipeline_Incident (дата обращения: 09.09.2025).
5. Cisco Cybersecurity Readiness Index: Resilience in a Hybrid World. India edition. Cisco, 2023 [Электронный ресурс]. URL: www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-market-snapshot-india.pdf (дата обращения: 14.09.2025).
6. Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards // World Economic Forum, 2019 [Электронный ресурс].

URL: www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf (дата обращения: 12.09.2025)

7. Cyber Security Guidelines, 2021. Central Electricity Authority of India (CEA). [Электронный ресурс]. URL: https://cea.nic.in/?lang=en&s=cyber+security (дата обращения: 09.09.2025).

8. Cyber Security in Power Sector Regulations Draft, 2024. Central Electricity Authority of India (CEA). [Электронный ресурс]. URL: https://cea.nic.in/?lang=en&s=cyber+security (дата обращения: 09.09.2025).

9. Cybersecurity - is the power system lagging behind? // IEA, Paris, 2023 [Электронный ресурс]. URL: www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind (дата обращения: 09.09.2025).

10. Cybersecurity Concerns: Strategies for Safeguarding Smart Grid Infrastructure, 2024 // PowerLine magazine. [Электронный ресурс]. URL: https://powerline.net.in/2024/03/07/cybersecurity-concerns-strategies-for-safeguarding-smart-grid-infrastructure/ (дата обращения: 09.09.2025).

11. Domestic Manufacturing Capacity & Potential Cyber Security Challenges in the wind sector and Way Forward, 2024. NITI Aayog [Электронный ресурс]. URL: www.niti.gov.in/sites/default/files/2024-07/Domestic%20Manufacturing%20Capacity%20%26%20Potential%20Cyber%20Secuirty%20Challanges%20in%20Wind%20Sector%20and%20Way%20Forward.pdf (дата обращения: 11.09.2025)

12. Enhancing cyber resilience in electricity systems // IEA, Paris, 2021 [Электронный ресурс]. URL: www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (дата обращения: 09.09.2025).

13. From Risk to Readiness: How India’s Electrical Sector Can Tackle Emerging Cyber Threats // RenewableWatch, 2025, August 19 [Электронный ресурс]. URL: https://renewablewatch.in/2025/08/19/from-risk-to-readiness-how-indias-electrical-sector-can-tackle-emerging-cyber-threats/ (дата обращения: 15.09.2025).

14. Government establishes dedicated Cyber Security Training Lab for Power Sector, 2023 // Press Information Bureau (PIB). [Электронный ресурс]. URL:

www.pib.gov.in/PressReleasePage.aspx?PRID=2148943 (дата обращения: 15.09.2025).

15. Habib AKM A., Hasan M.K., Alkhayyat A., Islam Sh., Sharma R., Alkwai L.M. False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction // Computers and Electrical Engineering. – 2023. – Vol.107. – 108638. DOI: 10.1016/j.compeleceng.2023.108638.

16. Hassine L., Quadar N., Ledmaoui Y. et al. Enhancing smart grid security in smart cities: A review of traditional approaches and emerging technologies // Applied Energy. – 2025. – Vol. 398. – 126430. DOI: 10.1016/j.apenergy.2025.126430.

17. India Cyber Threat Report 2025. New Delhi: Data Security Council of India [Электронный ресурс]. URL: www.dsci.in/files/content/knowledge-centre/2024/India-Cyber-Threat-Report-2025.pdf (дата обращения: 18.09.2025).

18. India Moves to Shield Power Grids from Solar Equipment Malware, 2025. Bloomberg [Электронный ресурс]. URL: www.bloomberg.com/news/articles/2025-07-24/india-moves-to-shield-power-grids-from-solar-equipment-malware (дата обращения: 19.09.2025).

19. India to enforce strict cybersecurity law for power sector from 2026 to guard against attacks, 2024. EQ International [Электронный ресурс]. URL: www.eqmagpro.com/india-to-enforce-strict-cybersecurity-law-for-power-sector-from-2026-to-guard-against-attacks-eq/ (дата обращения: 16.09.2025).

20. India’s Latest Push for a Holistic Domestic Wind Turbine Manufacturing Market, 2024 // JMK Research. [Электронный ресурс]. URL: https://jmkresearch.com/indias-latest-push-for-a-holistic-domestic-wind-turbine-manufacturing-market/ (дата обращения: 19.09.2025).

21. ISC2 Cybersecurity Workforce Study, 2023 [Электронный ресурс]. URL: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf (дата обращения: 13.09.2025).

22. Joe R.R. Cybersecurity’s Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack // Cyberdefensereview [Электронный ресурс].

URL: https://cyberdefensereview.army.mil/Portals/6/Documents/2021_summer_cdr/02_ReederHall_CDR_V6N3_2021.pdf (дата обращения: 12.09.2025).

23. Luigi C., Nardone R., Petruolo A., Romano L. Building Cyber-Resilient Smart Grids with Digital Twins and Data Spaces // Applied Sciences. – 2023. – № 13(24). – 13060. DOI: 10.3390/app132413060.

24. Mahajan H. Emerging Threats to India's Energy Security: Drone Warfare, Cyber Attacks and Geopolitical Risks // Indus Research, 2024 [Электронный ресурс]. URL: https://indusresearch.in/emerging-threats-to-indias-energy-security-drone-warfare-cyber-attacks-and-geopolitical-risks-by-brigadier-hemant-mahajan/ (дата обращения: 19.09.2025).

25. Morya K., Singh M. Associated threats of industrial control systems and awareness of cyber security in ENR Sector of India - a Case Study // Industrial Engineering Journal. – 2020. – Vol. 13. – № 2 [Электронный ресурс]. URL: www.researchgate.net/publication/347410166_'Associated_threats_of_industrial_control_systems_and_awareness_of_cyber_security_in_ENR_Sector_of_India_-_a_Case_Study'_Industrial_Engineering_Journal_132_Singh_M_Morya_K_K_2020 (дата обращения: 11.09.2025)

26. Nuraeni A., Nugraha Y., Aminanto M. Revisiting Cyber Threats in Government Sectors: A Systematic Review of Attacks, Challenges, and Policy-Level Defenses // International Journal of Advances in Data and Information Systems. – 2025. – Vol. 6. – pp. 447-459. DOI: 10.59395/ijadis.v6i2.1404

27. Powell J., McCafferty-Leroux A., Hilal W. et al. Smart grids: A comprehensive survey of challenges, industry applications, and future trends // Energy Reports. – 2024. – Vol. 11. – Pp. 5760-5785. DOI: 10.1016/j.egyr.2024.05.051

28. Sanders P., Bronk C., Bazilian M.D. Critical energy infrastructure and the evolution of cybersecurity // The Electricity Journal. – 2022. – Vol. 35. – Issue 10. – p. 107224. DOI: 10.1016/j.tej.2022.107224

29. Satapathy A.S., Sahoo S.K., Mohanty A., Fouad Ya., Soudagar M.E.M., Cuce E. Market Drivers in India's Smart Grid: Responsibilities and Roles of Stakeholders //

Energy Engineering. – 2024. – Vol. 122. – Issue 1. – Pp. 101-128. DOI: 10.32604/ee.2024.055105.

30. Security of Energy Infrastructure on the Frontline, 2024. ORF Online. [Электронный ресурс]. URL: www.orfonline.org/expert-speak/security-of-energy-infrastructure-on-the-frontline (дата обращения: 19.09.2025).

31. Singh K., Goyal S.B., Rajawat A.S., Waked H.N. A Blockchain-Integrated AI Framework for Enhancing Energy Efficiency and Sustainability in Smart Grids // Procedia Computer Science. – 2025. – Vol. 258. – Pp. 2302-2311. DOI: 10.1016/j.procs.2025.04.485.

32. Umar I., Ullah H., Khan N., Saleem K., Ahmad I. AI-enhanced intrusion detection in smart renewable energy grids: A novel industry 4.0 cyber threat management approach // International Journal of Critical Infrastructure Protection. – 2025. – Vol. 50. – 100769. DOI: 10.1016/j.ijcip.2025.100769.

33. Venkatachary S.K., Prasad J., Alagappan A., Andrews L.J.B., Raj R.A., Duraisamy S. Cybersecurity and cyber-terrorism challenges to energy-related infrastructures – Cybersecurity frameworks and economics – Comprehensive review // International Journal of Critical Infrastructure Protection. – 2024. – Vol. 45. – 100677. DOI: 10.1016/j.ijcip.2024.100677.

References

1. ART-ataki na promyshlennye kompanii v pervom polugodii 2021 [APT attacks on industrial companies in the first half of 2021]. Kaspersky ICS CERT. Available at: https://ics-cert.kaspersky.ru/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-Ru.pdf (accessed: 09.09.2025).

2. Matyuhina E.N. Evolutsiya infrastruktury informatsionnoy I kiberbezopasnosti Indii [The Evolution of India's Information and Cybersecurity infrastructure]. SibSkript, 2024, no. 3 (33). Available at: https://cyberleninka.ru/article/n/evolyutsiya-infrastruktury-informatsionnoy-i-kiberbezopasnosti-indii (accessed: 09.09.2025).

3. Solovieva Y.V., Chernyaev M.V. Energoemkost ekonomiki I energoeffektivnost: problem I perspektivy [Energy intensity of the economy and

energy efficiency: problems and prospects]. ETAP: economic theory, analysis, practice, 2019, no. 6, pp. 118-130. DOI 10.24411/2071-6435-2019-10127.

4. Bellamkonda S. Ransomware attacks on critical infrastructure: A study of the Colonial Pipeline incident. International Journal of Research in Computer Applications and Information Technology, 2024, no. 7(2), pp. 1423–1433. Available at: www.researchgate.net/publication/386014193_Ransomware_Attacks_On_Critical_Infrastructure_A_Study_Of_The_Colonial_Pipeline_Incident (accessed: 09.09.2025).

5. Cisco Cybersecurity Readiness Index: Resilience in a Hybrid World. India edition. Cisco, 2023. Available at: www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-market-snapshot-india.pdf (accessed: 14.09.2025).

6. Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards. World Economic Forum, 2019. Available at: www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf (accessed: 12.09.2025)

7. Cyber Security Guidelines, 2021. Central Electricity Authority of India (CEA). Available at: https://cea.nic.in/?lang=en&s=cyber+security (accessed: 09.09.2025).

8. Cyber Security in Power Sector Regulations Draft, 2024. Central Electricity Authority of India (CEA). Available at: https://cea.nic.in/?lang=en&s=cyber+security (accessed: 09.09.2025).

9. Cybersecurity - is the power system lagging behind? IEA, Paris, 2023 Available at: www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind (accessed: 09.09.2025).

10. Cybersecurity Concerns: Strategies for Safeguarding Smart Grid Infrastructure, 2024. PowerLine magazine. Available at: https://powerline.net.in/2024/03/07/cybersecurity-concerns-strategies-for-safeguarding-smart-grid-infrastructure/ (accessed: 09.09.2025).

11. Domestic Manufacturing Capacity & Potential Cyber Security Challenges in the wind sector and Way Forward, 2024. NITI Aayog. Available at:

www.niti.gov.in/sites/default/files/2024-07/Domestic%20Manufacturing%20Capacity%20%26%20Potential%20Cyber%20Secuirty%20Challanges%20in%20Wind%20Sector%20and%20Way%20Forward.pdf (accessed: 11.09.2025)

12. Enhancing cyber resilience in electricity systems. IEA, Paris, 2021. Available at: www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (accessed: 09.09.2025).

13. From Risk to Readiness: How India's Electrical Sector Can Tackle Emerging Cyber Threats. RenewableWatch, 2025, August 19. Available at: https://renewablewatch.in/2025/08/19/from-risk-to-readiness-how-indias-electrical-sector-can-tackle-emerging-cyber-threats/ (accessed: 15.09.2025).

14. Government establishes dedicated Cyber Security Training Lab for Power Sector, 2023. Press Information Bureau (PIB). Available at: www.pib.gov.in/PressReleasePage.aspx?PRID=2148943 (accessed: 15.09.2025).

15. Habib AKM A., Hasan M.K., Alkhayyat A., Islam Sh., Sharma R., Alkwai L.M. False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction // Computers and Electrical Engineering, 2023, vol.107, 108638. DOI: 10.1016/j.compeleceng.2023.108638.

16. Hassine L., Quadar N., Ledmaoui Y. et al. Enhancing smart grid security in smart cities: A review of traditional approaches and emerging technologies. Applied Energy, 2025, vol. 398, 126430. DOI: 10.1016/j.apenergy.2025.126430.

17. India Cyber Threat Report 2025. New Delhi: Data Security Council of India. Available at: www.dsci.in/files/content/knowledge-centre/2024/India-Cyber-Threat-Report-2025.pdf (accessed: 18.09.2025).

18. India Moves to Shield Power Grids from Solar Equipment Malware, 2025. Bloomberg. Available at: www.bloomberg.com/news/articles/2025-07-24/india-moves-to-shield-power-grids-from-solar-equipment-malware (accessed: 19.09.2025).

19. India to enforce strict cybersecurity law for power sector from 2026 to guard against attacks, 2024. EQ International. Available at: www.eqmagpro.com/india-to-

enforce-strict-cybersecurity-law-for-power-sector-from-2026-to-guard-against-attacks-eq/ (accessed: 16.09.2025).

20. India’s Latest Push for a Holistic Domestic Wind Turbine Manufacturing Market, 2024. JMK Research. Available at: https://jmkresearch.com/indias-latest-push-for-a-holistic-domestic-wind-turbine-manufacturing-market/ (accessed: 19.09.2025).

21. ISC2 Cybersecurity Workforce Study, 2023. Available at: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf (accessed: 13.09.2025).

22. Joe R.R. Cybersecurity’s Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. Cyberdefensereview. Available at: https://cyberdefensereview.army.mil/Portals/6/Documents/2021_summer_cdr/02_ReederHall_CDR_V6N3_2021.pdf (accessed: 12.09.2025).

23. Luigi C., Nardone R., Petruolo A., Romano L. Building Cyber-Resilient Smart Grids with Digital Twins and Data Spaces. Applied Sciences, 2023, no. 13(24), 13060. DOI: 10.3390/app132413060.

24. Mahajan H. Emerging Threats to India’s Energy Security: Drone Warfare, Cyber Attacks and Geopolitical Risks. Indus Research, 2024. Available at: https://indusresearch.in/emerging-threats-to-indias-energy-security-drone-warfare-cyber-attacks-and-geopolitical-risks-by-brigadier-hemant-mahajan/ (accessed: 19.09.2025).

25. Morya K., Singh M. Associated threats of industrial control systems and awareness of cyber security in ENR Sector of India - a Case Study. Industrial Engineering Journal, 2020, no. 13(2). Available at: www.researchgate.net/publication/347410166_'Associated_threats_of_industrial_control_systems_and_awareness_of_cyber_security_in_ENR_Sector_of_India_-_a_Case_Study'_Industrial_Engineering_Journal_132_Singh_M_Morya_K_K_2020 (accessed: 11.09.2025)

26. Nuraeni A., Nugraha Y., Aminanto M. Revisiting Cyber Threats in Government Sectors: A Systematic Review of Attacks, Challenges, and Policy-Level Defenses. International Journal of Advances in Data and Information Systems, 2025, vol. 6, pp. 447-459. DOI: 10.59395/ijadis.v6i2.1404

27. Powell J., McCafferty-Leroux A., Hilal W. et al. Smart grids: A comprehensive survey of challenges, industry applications, and future trends. Energy Reports, 2024, vol. 11, pp. 5760-5785. DOI: 10.1016/j.egyr.2024.05.051

28. Sanders P., Bronk C., Bazilian M.D. Critical energy infrastructure and the evolution of cybersecurity. The Electricity Journal, 2022, no. 35(10), p. 107224. DOI: 10.1016/j.tej.2022.107224

29. Satapathy A.S., Sahoo S.K., Mohanty A., Fouad Ya., Soudagar M.E.M., Cuce E. Market Drivers in India's Smart Grid: Responsibilities and Roles of Stakeholders. Energy Engineering, 2024, no. 122(1), pp. 101-128. DOI: 10.32604/ee.2024.055105.

30. Security of Energy Infrastructure on the Frontline, 2024. ORF Online. Available at: www.orfonline.org/expert-speak/security-of-energy-infrastructure-on-the-frontline (accessed: 19.09.2025).

31. Singh K., Goyal S.B., Rajawat A.S., Waked H.N. A Blockchain-Integrated AI Framework for Enhancing Energy Efficiency and Sustainability in Smart Grids. Procedia Computer Science, 2025, vol. 258, pp. 2302-2311. DOI: 10.1016/j.procs.2025.04.485.

32. Umar I., Ullah H., Khan N., Saleem K., Ahmad I. AI-enhanced intrusion detection in smart renewable energy grids: A novel industry 4.0 cyber threat management approach. International Journal of Critical Infrastructure Protection, 2025, vol. 50, 100769. DOI: 10.1016/j.ijcip.2025.100769.

33. Venkatachary S.K., Prasad J., Alagappan A., Andrews L.J.B., Raj R.A., Duraisamy S. Cybersecurity and cyber-terrorism challenges to energy-related infrastructures – Cybersecurity frameworks and economics – Comprehensive review. International Journal of Critical Infrastructure Protection, 2024, vol. 45, 100677. DOI: 10.1016/j.ijcip.2024.100677.