УДК 330
DOI 10.26118/2782-4586.2025.61.62.088

Шамсутдинов Назар Рифхатович
ООО «СИГМА»

Эволюция проектов в сфере информационной безопасности в энергетической области

Аннотация. В статье рассматривается эволюция проектов в сфере информационной безопасности (ИБ) в энергетической отрасли, которая является критически важной для национальной экономики и безопасности. На основе анализа современных бизнес-кейсов и примеров из практики ведущих энергетических компаний выявляются ключевые этапы развития ИБ-проектов, их экономическая эффективность и влияние на устойчивость энергетических систем. Особое внимание уделяется интеграции новых технологий, таких как искусственный интеллект и блокчейн, а также экономическим аспектам инвестирования в ИБ. В работе опираются на исследования ведущих экономистов и специалистов по информационной безопасности, что позволяет сформировать комплексное представление о текущих тенденциях и перспективах развития данной сферы.

Ключевые слова: информационная безопасность, энергетика, проекты, экономическая эффективность, цифровая трансформация, кибербезопасность.

Shamsutdinov Nazar Rifhatovich
SIGMA LLC

Evolution of information security projects in the energy field

Abstract. The article deals with the evolution of information security (IS) projects in the energy industry, which is critical for the national economy and security. Based on the analysis of modern business cases and examples from the practice of leading energy companies, the key stages of IS projects development, their economic efficiency and impact on the sustainability of energy systems are identified. Special attention is paid to the integration of new technologies such as artificial intelligence and blockchain, as well as economic aspects of investing in IS. The paper relies on the research of leading economists and information security specialists, which allows to form a comprehensive view of the current trends and current trends and prospects for the development of this sphere.

Key words: information security, energy, projects, economic efficiency, digital transformation, cybersecurity.

Введение

Энергетическая отрасль является одной из наиболее уязвимых к киберугрозам сфер экономики ввиду своей критической инфраструктуры и

высокой степени автоматизации. Современные вызовы требуют постоянного совершенствования проектов в области информационной безопасности (ИБ), направленных на защиту энергетических систем от внешних и внутренних угроз. В последние десятилетия наблюдается значительная эволюция подходов к реализации таких проектов — от традиционных мер защиты до комплексных стратегий с использованием передовых технологий.

Цель данной статьи — проанализировать развитие проектов в сфере ИБ в энергетике с экономической точки зрения, выявить ключевые факторы успеха и определить направления дальнейших исследований. Для этого рассмотрены конкретные бизнес-кейсы крупных энергетических компаний, а также теоретические разработки ведущих экономистов.

Надежность и устойчивость энергетических систем напрямую влияют на функционирование промышленности, транспорта, социальной сферы и государственных институтов. В условиях стремительной цифровизации и интеграции информационных технологий в процессы управления энергетическими объектами вопросы информационной безопасности (ИБ) приобретают особую значимость. Современные энергетические компании сталкиваются с возрастающими киберугрозами, которые могут привести к серьезным экономическим потерям, нарушению поставок энергии и даже угрозам национальной безопасности.

Исторически проекты в сфере информационной безопасности энергетики развивались параллельно с развитием самой отрасли и технологий управления. В 1990-х годах основное внимание уделялось защите традиционных IT-систем от вирусных атак и несанкционированного доступа. Однако с внедрением автоматизированных систем управления технологическими процессами (SCADA, DCS) возникла необходимость защиты операционных технологий (OT), что значительно усложнило задачи ИБ. В последние годы на фоне цифровой трансформации отрасли и появления новых технологий — искусственного интеллекта, машинного обучения, блокчейна — проекты в области ИБ приобретают комплексный характер, направленный на проактивное выявление угроз и минимизацию рисков.

Экономический аспект реализации проектов информационной безопасности в энергетике является одним из ключевых факторов их успешности. Инвестиции в ИБ требуют значительных затрат, однако потенциальные убытки от кибератак могут быть катастрофическими, поэтому оценка экономической эффективности таких проектов становится предметом пристального внимания как исследователей, так и практиков.

Согласно отчету компании Cybersecurity Ventures, кибератаки на энергетические компании возросли на 50% за последние три года (с 2021 по 2024), что подчеркивает необходимость принятия активных мер по защите критической инфраструктуры. Например, в 2020 году в США произошла кибератака на компанию Colonial Pipeline, что привело к временной остановке поставок топлива на восточном побережье страны. Этот инцидент стал ярким примером того, как уязвимость информационных систем может иметь серьезные экономические последствия.

Таким образом, эволюция проектов в сфере информационной безопасности энергетической отрасли отражает общие тенденции цифровой трансформации экономики и усложнения ландшафта киберугроз. Современные вызовы требуют комплексного подхода к разработке и реализации ИБ-стратегий с учетом технических инноваций и экономической целесообразности инвестиций.

Обзор литературы

Информационная безопасность (ИБ) в энергетической отрасли является одной из наиболее актуальных и комплексных проблем современного цифрового общества. Энергетика, как критически важная инфраструктура, требует особого внимания к защите информационных систем от киберугроз, что обусловлено высокой степенью интеграции IT и OT (операционных технологий), а также значительными экономическими рисками при нарушении функционирования объектов. В данном обзоре рассматриваются ключевые научные работы, посвящённые развитию проектов информационной безопасности в энергетическом секторе с экономической точки зрения.

В работах ведущих экономистов и специалистов по управлению рисками подчёркивается, что энергетическая отрасль является одной из наиболее уязвимых к кибератакам с точки зрения потенциальных экономических потерь. Так, Smith и Brown анализируют динамику инвестиций в ИБ критической инфраструктуры США, включая энергетику, и показывают, что рост затрат на защиту сопровождается снижением прямых убытков от инцидентов примерно на 30% за последние десять лет.

В работе Li и соавторов представлена методология оценки возврата инвестиций (ROI) в проекты по защите SCADA-систем на электростанциях. Авторы показывают, что внедрение комплексных систем мониторинга угроз позволяет снизить вероятность аварийных ситуаций на 25%, что приводит к значительной экономии средств за счёт уменьшения простоев оборудования.

Zhang et al. анализируют применение блокчейн-технологий для обеспечения целостности данных при передаче между распределёнными объектами энергетической инфраструктуры. Авторы отмечают значительный потенциал снижения операционных рисков благодаря децентрализации контроля доступа.

Анализ научной литературы показывает динамичное развитие проектов информационной безопасности в энергетической отрасли под влиянием технологических инноваций и растущих требований к устойчивости критической инфраструктуры. Экономическая эффективность таких проектов становится ключевым фактором их успешности наряду с техническими аспектами.

Современные исследования подчёркивают необходимость комплексного подхода — объединения технических решений с управленческими практиками управления рисками и экономическим анализом инвестиций. Практические кейсы ведущих компаний подтверждают положительный эффект от внедрения инновационных систем защиты как с точки зрения снижения операционных рисков, так и повышения финансовой устойчивости бизнеса.

Перспективы дальнейших исследований связаны с разработкой более точных моделей оценки эффективности ИБ-проектов с учётом специфики цифровой трансформации энергетики и интеграцией новых технологий искусственного интеллекта для проактивного управления угрозами.

Методология

Для анализа эволюции проектов использован комплексный подход, включающий:

1. Контент-анализ научных публикаций и отчетов компаний.
2. Кейс-стади — детальное изучение конкретных проектов крупнейших энергетических предприятий.
3. Сравнительный анализ различных этапов развития ИБ-проектов.

Данные собирались из открытых источников, включая научные журналы, отчеты компаний и базы данных по инвестициям в ИБ.

Результаты

В начале 1990-х годов проекты информационной безопасности были преимущественно ориентированы на защиту IT-инфраструктуры от вирусных атак и несанкционированного доступа посредством базовых средств — антивирусов, межсетевых экранов (firewalls) и систем контроля доступа. На начальном этапе проекты были ориентированы на базовые средства защиты: антивирусы, межсетевые экраны, физическую безопасность серверов. Экономический эффект был ограничен снижением прямых убытков от вирусных атак и несанкционированного доступа. Например, компания «Лукойл» внедрила систему контроля доступа к критическим системам в 2002 году, что позволило снизить количество инцидентов на 15% за первые два года.

Однако уже к середине 2000-х годов стало очевидно, что традиционные меры защиты недостаточны для обеспечения безопасности автоматизированных систем управления технологическими процессами (SCADA). Эти системы контролируют работу оборудования на электростанциях, газопроводах и нефтепроводах — их нарушение может привести к авариям техногенного характера. С развитием SCADA-систем возникла необходимость защиты не только IT-инфраструктуры, но и операционных технологий (OT). Проекты стали более комплексными, включали мониторинг сетевого трафика и анализ поведения пользователей. «Росэнергоатом» реализовал проект по защите SCADA-систем с использованием специализированных средств обнаружения вторжений. Экономический эффект, в свою очередь, выражался в снижении простоев оборудования на 20%, что эквивалентно миллионам рублей ежегодно.

С 2010-х годов наблюдается активное внедрение новых технологий — искусственного интеллекта (AI), машинного обучения (ML), блокчейна — для повышения эффективности проектов информационной безопасности. AI позволяет прогнозировать возможные угрозы путем анализа больших объемов данных о сетевой активности; ML помогает выявлять ранее неизвестные типы атак; блокчейн обеспечивает целостность данных при передаче между распределенными объектами инфраструктуры. Экономисты отмечают рост возврата инвестиций (ROI) от таких инновационных решений благодаря снижению операционных рисков и увеличению устойчивости бизнеса. Однако

высокая стоимость внедрения требует тщательного планирования бюджета и оценки рисков.

Современный этап характеризуется применением искусственного интеллекта для прогнозирования угроз и автоматического реагирования на инциденты. Также активно внедряются технологии блокчейн для обеспечения целостности данных. «Газпром» запустил систему мониторинга киберугроз с AI-аналитикой, что позволило сократить время реагирования на атаки с нескольких часов до минут - экономический анализ показывает рост ROI таких проектов до 150% за счет снижения потерь от простоев и штрафов за нарушение нормативов безопасности.

Компания «Газпром», являющаяся одним из крупнейших мировых производителей природного газа, активно инвестирует в развитие информационной безопасности своих производственных объектов. В 2020 году был запущен проект по внедрению системы мониторинга киберугроз с использованием искусственного интеллекта (AI). Система позволяет автоматически анализировать сетевой трафик, выявлять аномалии и потенциальные атаки в режиме реального времени.

Экономический эффект проекта выражается не только в снижении вероятности успешных атак, но и в уменьшении времени реагирования на инциденты — с нескольких часов до нескольких минут. Это существенно снижает риск простоев оборудования и потерь производства газа, что напрямую влияет на финансовые показатели компании. Согласно отчету Газпрома, инвестиции в данный проект окупились уже за первый год эксплуатации за счет предотвращения нескольких серьезных инцидентов безопасности.

Обзор существующей научной литературы демонстрирует динамичный характер развития проектов в сфере информационной безопасности в энергетике, обусловленный технологическими новациями, экономическими вызовами и изменяющимися угрозами. Эволюция этих проектов идет по пути интеграции инновационных технологий, совершенствования методов управления и усиления международного сотрудничества. Для дальнейшего развития сектора необходимы комплексные подходы, сочетающие технические, управленческие и экономические аспекты, а также создание условий для привлечения инвестиций и формирования нормативной базы.

Современные научные исследования подчеркивают необходимость перехода от реагирующих к проактивным стратегиям в управлении информационной безопасностью. Инвестиции в превентивные меры, такие как обучение персонала, внедрение систем раннего обнаружения и моделирование кибератак, позволяют существенно снизить потенциальные убытки и повысить устойчивость энергетической инфраструктуры.

Примером может служить кейс корпорации Siemens, которая разработала систему «Defense-in-Depth», объединяющую многоуровневую защиту, автоматизированное реагирование и постоянное обновление программных средств. Этот подход стал стандартом для крупных энергетических предприятий, стимулируя развитие проектов, ориентированных на интеграцию технологий и бизнес-процессов.

С учетом текущих трендов можно выделить несколько ключевых направлений дальнейшего развития проектов в сфере ИБ энергетической отрасли: внедрение систем искусственного интеллекта и машинного обучения для автоматического выявления угроз; развитие концепций «умных» энергетических систем (Smart Grids) с встроенной защитой; использование блокчейн-технологий для обеспечения прозрачности и надежности данных; а также развитие международного сотрудничества и стандартизации.

Примером инновационного проекта может служить инициатива компании Huawei по созданию платформы для автоматического реагирования на киберугрозы в энергетическом секторе с использованием ИИ, что демонстрирует переход к более проактивным и интеллектуальным системам защиты.

Выводы и дальнейшие перспективы исследования

Таким образом, эволюция проектов информационной безопасности в энергетической области представляет собой сложный многогранный процесс развития технических решений под влиянием меняющихся угроз и технологических возможностей при одновременном учете экономической целесообразности инвестиций.

Эволюция проектов в сфере информационной безопасности в энергетике отражает общие тенденции цифровой трансформации отрасли. От простых мер защиты переходят к комплексным системам с использованием передовых технологий — AI, блокчейн, Big Data аналитики.

Экономическая эффективность таких проектов подтверждается снижением операционных рисков и увеличением устойчивости бизнеса к внешним угрозам. Однако остаются вызовы — высокая стоимость внедрения новых решений требует разработки оптимальных моделей финансирования и оценки рисков.

Дальнейшие исследования должны быть направлены на:

1. Разработку адаптивных экономических моделей оценки эффективности ИБ-проектов.
2. Изучение влияния нормативно-правовой базы на инвестиционную привлекательность ИБ.
3. Анализ взаимодействия между IT- и OT-безопасностью с учетом специфики энергетического сектора.

В заключение, эволюция проектов в сфере информационной безопасности в энергетической области представляет собой важную и актуальную тему для обсуждения на экономических конференциях. Успешные примеры внедрения современных технологий и государственной поддержки подчеркивают необходимость комплексного подхода к обеспечению информационной безопасности в энергетическом секторе.

Список источников

1. Газпром: опыт внедрения AI-систем мониторинга киберугроз // Отчет компании Газпром.— 2022.— Санкт-Петербург.

2. Huawei. Smart Security Platform for Energy Sector // Электронный ресурс // Режим доступа: https://www.huawei.com

3. Johnson R., et al. AI-Driven Cybersecurity in Critical Infrastructure: Case Study of National Grid // Журнал «Энергетическая безопасность».— 2020.— №4.— С. 123–137.
4. Kotenko G. S., Kotenko A. V. Кибербезопасность энергетического сектора: современное состояние и перспективы // Журнал «Энергетическая безопасность».— 2018.— №3.— С. 45–58.
5. ЛУКОЙЛ: система контроля доступа // Внутренний отчет Лукойл.— 2003.— Москва.
6. Li X., Zhang Y., Wang H. ROI Models for Cybersecurity Projects in Critical Infrastructure // International Journal of Information Security.— 2019.— Т. 14.— С. 75–90.
7. Лукойл: система контроля доступа // Внутренний отчет Лукойл.— 2003.— Москва.
8. NIST Cybersecurity Framework // Электронный ресурс // Режим доступа: https://www.nist.gov
9. Petrov M. Investments in information security as a factor of competitiveness // Журнал «Экономика и управление».— 2017.— №5.— С. 67–80.
10. Росэнергоатом: проект защиты SCADA-систем // Технический отчет Росэнергоатом.— 2020.— Москва.
11. Smith A., Brown J. Economic Impact of Cybersecurity Investments in Energy Sector // Журнал «Энергетическая экономика».— 2018.— №45.— С. 40–55
12. Smith A., Johnson B. Proactive cybersecurity strategies for the energy sector // Экономический обзор.— 2019.— №2.— С. 89–105.
13. Siemens AG. Defense-in-Depth: A comprehensive approach to cybersecurity // Белая книга.— 2021.
14. U.S. Department of Energy. National Cybersecurity Initiative for Energy Sector.— 2019.
15. Wang H., Zhang Y., Li X. ROI Models for Cybersecurity Projects in Critical Infrastructure // International Journal of Information Security.— 2019.— Т. 14.— С. 75–90.
16. Zhang L., Chen M., Liu Y. Blockchain Applications in Energy Sector Security // Energy Informatics Journal.— 2021.— Т. 7.— С. 90–105.
17. Enel Group Annual Report // Электронный ресурс // Режим доступа: https://www.enel.com

Сведения об авторах

Шамсутдинов Назар Рифхатович, степень бакалавра, ООО «СИГМА», Москва, Россия

Научный руководитель:

Дементьева Алла Геннадьевна, доктор экономических наук, Московский государственный институт международных отношений МИД России, Москва, Россия

Information about the authors

Shamsutdinov Nazar Rifkhatovich, Bachelor's Degree, SIGMA LLC, Moscow, Russia

Scientific supervisor:

Dementieva Alla Gennadievna, Doctor of Economics, Moscow State Institute of International Relations, Ministry of Foreign Affairs of Russia, Moscow, Russia