Аббас Али о. АЛИЕВ
Доктор философии по политическим наукам
Азербайджанский Университет языков

ЭНЕРГЕТИЧЕСКАЯ БЕЗОПАСНОСТЬ В ЦИФРОВУЮ ЭПОХУ: РОЛЬ И ЗНАЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

Резюме

Статья рассматривает кибербезопасность как ключевой элемент энергетической безопасности в условиях цифровизации. Анализируются угрозы кибератак, интеграция информационных и операционных технологий, а также влияние новых технологий, таких как IoT, AI и блокчейн. Особое внимание уделяется комплексному подходу к устойчивости энергетических систем: технические решения (шифрование, IDS, интеллектуальные сети), организационные меры (политики кибербезопасности, специализированные команды) и человеческий фактор (обучение, культура безопасности). Приводятся примеры известных инцидентов и обсуждаются стратегии минимизации рисков.Эффективное управление киберрисками обеспечивает защиту инфраструктуры, экономическую стабильность и устойчивое развитие. Рекомендации включают инвестиции в новые технологии, стандартизацию процессов, межсекторное сотрудничество и интеграцию возобновляемой энергии.

Ключевые слова: энергетическая безопасность, кибербезопасность, цифровизация, возобновляемые источники, угрозы.

UOT: 339
JEL: F-52
DOI: https://doi.org/ 10.54414/BQBM6650

Введение

Энергетическая безопасность в цифровую эпоху выступает одним из ключевых факторов стабильного и устойчивого развития общества. В условиях глобализации и ускоренного технологического прогресса энергетические системы сталкиваются с новыми вызовами, требующими переосмысления традиционных подходов к обеспечению безопасности. Она охватывает широкий спектр вопросов — от доступности и надежности энергоресурсов до защиты от киберугроз.

Энергетическая безопасность определяется как способность государства или региона обеспечивать надежное и непрерывное снабжение энергией, минимизируя риски, связанные как с внутренними, так и с внешними угрозами. В этом контексте выделяются следующие ключевые аспекты:

Доступность и диверсификация источников энергии: Устойчивое снабжение достигается через использование различных видов энергии, включая уголь, газ, атомную, солнечную и ветровую. Диверсификация снижает зависимость от отдельных поставщиков и создает резервы на случай непредвиденных обстоятельств — стихийных бедствий или политических кризисов. Геополитические факторы остаются значимым элементом, влияющим на доступность ресурсов

Надежность и устойчивость инфраструктуры: Энергетические системы должны сохранять функционирование в условиях аварий, природных катастроф и кибератак.

Устойчивость подразумевает способность адаптироваться к изменениям и восстанавливаться после кризисов. Важную роль играют технологические инновации, такие как автоматизация и интеллектуальные сети, повышающие эффективность управления.

Экономическая и экологическая устойчивость: Энергетическая безопасность включает доступность энергоресурсов и минимизацию экологического воздействия. Важным является внедрение возобновляемых источников энергии, сокращение углеродного следа и адаптация к экологическим требованиям. Переход к цифровым технологиям делает энергетические системы более взаимосвязанными и, одновременно, уязвимыми к кибератакам. Нарушения работы критической инфраструктуры могут вызвать не только локальные сбои, но и цепную реакцию, затрагивающую экономику в целом. Например, атака на энергосеть способна привести к отключению электроснабжения, что затронет другие сектора экономики.

Кибербезопасность в условиях цифровизации. С внедрением цифровых технологий в энергетическом секторе кибербезопасность становится ключевым элементом обеспечения энергетической безопасности. Основные составляющие этого направления включают:

1. Угрозы кибератак: Энергетическая инфраструктура, являясь критически важным сектором, подвержена рискам кибератак, способных вызвать значительные сбои. Примеры, такие как атака Stuxnet, показали, что уязвимости в системах управления могут быть использованы для достижения стратегических целей противника [1].

2. Интеграция информационных и операционных технологий: Объединение IT и OT создаёт новые уязвимости, которые злоумышленники могут эксплуатировать. Это требует разработки комплексных мер кибербезопасности, обеспечивающих безопасность как физических, так и цифровых компонентов инфраструктуры [2].

3. Нормативное регулирование и стандарты: Усиление требований к кибербезопасности, включая стандарты NIST и ISO, заставляет организации внедрять многоуровневые стратегии защиты, объединяющие технические меры (шифрование, сегментацию сети) и организационные подходы (обучение персонала, аудит безопасности) [3].

4. Устойчивость к инцидентам и реагирование: Эффективные системы кибербезопасности обеспечивают постоянный мониторинг, быструю идентификацию угроз и оперативное реагирование на инциденты, что критически важно для минимизации последствий атак и восстановления нормального функционирования энергетических систем.

5. Влияние новых технологий: Развитие интернет вещей (IoT) и искусственного интеллекта (AI) создаёт новые вызовы для киберзащиты. Эти технологии повышают эффективность, но одновременно формируют дополнительные уязвимости, требующие комплексного подхода к безопасности [4].

Таким образом, кибербезопасность становится неотъемлемой частью энергетической безопасности, обеспечивая защиту инфраструктуры и устойчивость экономических систем в условиях неопределенности [5]. Переход к цифровым технологиям в энергетическом секторе — сложный процесс, который трансформирует структуру и работу инфраструктуры. Интеллектуальные сети (Smart Grids): интеграция современных ИКТ с традиционными системами обеспечивает двусторонний обмен информацией между производителями и потребителями, оптимизирует распределение энергии и интегрирует распределённые источники, такие как солнечные и ветровые установки. Это повышает адаптивность и устойчивость сетей [6].

Интернет вещей (IoT): подключение миллионов сенсоров позволяет мониторить состояние инфраструктуры в реальном времени, улучшать прогнозирование потребления и ускорять реакцию на аномалии [7]. Аналитика больших данных: сбор и обработка больших массивов информации помо-

гает выявлять закономерности, оптимизировать процессы и снижать риски, связанные с колебаниями спроса и предложения.

Киберфизические системы: сочетание физических и цифровых компонентов создаёт более интегрированные и устойчивые системы, способные адаптироваться к изменяющимся условиям и противостоять кибератакам и физическим угрозам [8].Устойчивое развитие и возобновляемые источники: цифровизация способствует активной интеграции возобновляемой энергии, сокращению углеродного следа и повышению экологической устойчивости [9,10]. С внедрением цифровых технологий энергетический сектор сталкивается с новыми угрозами и рисками, которые необходимо учитывать при разработке стратегий киберзащиты. Кибератаки на системы управления представляют серьёзную опасность, причём источниками могут быть как государственные, так и негосударственные акторы, что может привести к сбоям в поставках и утечкам данных [12]. Уязвимости программного обеспечения: Современные системы управления часто имеют сложную архитектуру, содержащую потенциальные слабые места. Это требует постоянного мониторинга и своевременного обновления программного обеспечения [13].

Физические угрозы: Несмотря на рост киберугроз, физические атаки на инфраструктуру сохраняют актуальность. Экстремальные климатические явления и катастрофы также могут нарушать работу систем и повреждать объекты [14].Человеческий фактор: Недостаточная подготовка персонала и ошибки управления способны вызвать инциденты с серьёзными последствиями. Регулярное обучение и повышение квалификации сотрудников критически важны [15]. Пример атаки: Атака на Colonial Pipeline в мае 2021 года демонстрирует современные риски для энергетической инфраструктуры. Злоумышленники из группировки DarkSide заблокировали доступ к системам управления с помощью шифрующего ПО, требуя выкуп в биткойнах.

Последствия включали: Прекращение поставок: временная остановка трубопровода, снабжающего около 45 % бензина и дизельного топлива восточного побережья США, вызвала дефицит и рост цен [15].Экономические последствия: убытки оцениваются в миллионы долларов. Угрозы для национальной безопасности: инцидент обсуждался на высшем уровне в США, подчёркивая необходимость усиления киберзащиты [16]. Реакция: внедрение новых стандартов и рекомендаций для защиты критической инфраструктуры [17].

Ключевые аспекты кибербезопасности в энергетике:

Защита данных: шифрование, контроль доступа, токенизация и антивирусное ПО на основе машинного обучения обеспечивают целостность и предотвращают утечки [18]. Управление доступом: многоуровневая аутентификация, биометрические технологии и принцип наименьших привилегий с динамическим управлением ролями сотрудников, а также интеграция IAM-систем [19]. Мониторинг и реагирование: постоянный контроль сетевой активности, анализ поведенческих паттернов пользователей, использование SIEM-систем и создание команд быстрого реагирования (CERT) для оперативного противодействия инцидентам [20].

В энергетическом секторе внедрение международных стандартов и протоколов кибербезопасности является ключевым условием устойчивости систем. Основные стандарты включают:

1. NIST Cybersecurity Framework: разработанный Национальным институтом стандартов и технологий США, фреймворк предоставляет структуру управления киберрисками с категориями: идентификация, защита, обнаружение, реагирование и восстановление, что позволяет адаптировать стратегии к особенностям энергетической инфраструктуры [21].
2. ISO/IEC 27001 и 27002: задают требования к системам управления информационной безопасностью, включая технические и организационные меры, оценку рисков и непрерывное улучшение процессов [22].

3. NERC CIP: нормативные акты Североамериканской корпорации по надежности электрических сетей устанавливают обязательные требования к киберзащите операторов, включая управление доступом, защиту данных и физическую безопасность объектов.

Эти стандарты способствуют гармонизации подходов к киберзащите и внедрению лучших практик.

Роль государственных и международных организаций. Законодательная база: разработка и внедрение законов и регуляций для защиты критической инфраструктуры, включая обязательства по отчетности и процедуры реагирования на инциденты [23].Международное сотрудничество: ООН, НАТО и ЕС обеспечивают обмен информацией о киберугрозах и лучших практиках, учитывая транснациональный характер рисков.Образование и повышение квалификации: программы обучения и симуляции развивают навыки реагирования на инциденты и управления рисками, а также поддерживают исследования и разработку новых технологий защиты. Комплексный подход, включающий стандарты, участие государственных и международных структур и передовые технологии, обеспечивает надёжность и устойчивость энергетической инфраструктуры в условиях меняющегося ландшафта киберугроз.

Современные технологии AI и ML трансформируют киберзащиту анализ данных в реальном времени ML позволяет выявлять аномалии в поведении систем и сетевого трафика, указывающие на кибератаки [24].

Прогнозирование угроз: AI формирует модели для предсказания новых векторов атак на основе исторических данных, обеспечивая проактивную защиту. Автоматизация реагирования: AI-системы могут самостоятельно блокировать или изолировать скомпрометированные сегменты сети, снижая ущерб [25]. Эффективные стратегии киберзащиты. Стандарты и практики компании, такие как Siemens и Schneider Electric, используют NIST и ISO для структурирования защиты и внедрения лучших практик. Обучение персонала программы типа «Cybersecurity Awareness Program» (Duke Energy) повышают осведомлённость сотрудников и снижают риск успешных атак.

Сетевые симуляции и тестирование: «Red Team/Blue Team» упражнения выявляют слабые места и совершенствуют реагирование на инциденты [26]. Комплексный подход к кибербезопасности в энергетическом секторе включает три ключевых направления: технические, организационные и человеческие. Технические аспекты: Внедрение современных технологий защиты, включая шифрование, системы обнаружения вторжений (IDS) и SIEM, интегрированных на всех уровнях инфраструктуры.Организационные аспекты: Разработка и внедрение политик и процедур управления киберрисками, создание специализированных команд и интеграция кибербезопасности в корпоративную культуру. Человеческие аспекты: Подготовка и обучение сотрудников, формирование культуры осведомленности о киберугрозах и вовлечение всех уровней организации, что снижает риски ошибок и халатности.

Рост атак на критическую инфраструктуру: Наблюдается увеличение целенаправленных атак, таких как инцидент с Colonial Pipeline, с использованием методов ransomware и DDoS [27].Уязвимости новых технологий: IoT и искусственный интеллект создают новые точки доступа, которые могут быть эксплуатированы злоумышленниками [28,29]. Возможности и вызовы новых технологий: IoT повышает эффективность и устойчивость систем, но требует строгой безопасности на уровне устройств и сети; блокчейн обеспечивает прозрачность и безопасность управления ресурсами, но требует адаптации существующих моделей и решения регуляторных вопросов.

Рекомендации по повышению устойчивости кибербезопасности:

Инвестировать в технологии защиты: Использование AI и ML для проактивного мониторинга и реагирования на угрозы Установить стандарты безопасности: Разработка и

внедрение международных стандартов кибербезопасности для минимизации рисков.Создать культуру безопасности: Повышение осведомленности сотрудников и формирование корпоративной культуры безопасности. Сотрудничество между секторами: Партнерства между компаниями, государственными и исследовательскими организациями для создания устойчивой экосистемы кибербезопасности [30].

Заключение

В условиях роста киберугроз кибербезопасность становится ключевым элементом устойчивого развития энергетического сектора. Цифровизация инфраструктуры, включая генерацию, распределение и потребление энергии, создает новые сложные и динамичные угрозы, требующие адаптивных стратегий защиты.Интеграция инновационных технологий, таких как искусственный интеллект (AI) и машинное обучение (ML), позволяет не только обнаруживать и предотвращать кибератаки в реальном времени, но и анализировать большие объемы данных для выявления характерных паттернов угроз. Применение алгоритмов машинного обучения существенно улучшает прогнозирование атак и проактивное управление киберрисками.

Эффективная киберзащита требует комплексного подхода, включающего технические, организационные и человеческие аспекты. Технологические решения, включая системы обнаружения вторжений (IDS) и шифрование, должны внедряться на всех уровнях, однако без четко разработанных политик, процедур и специализированных команд по кибербезопасности их эффективность ограничена.Сотрудничество между государственными органами, регуляторами, энергетическими компаниями и конечными пользователями повышает уровень защиты, позволяя обмениваться информацией о киберугрозах, внедрять стандарты безопасности и организовывать обучающие программы. Образование и повышение квалификации сотрудников создают корпоративную культуру безопасности и снижают вероятность успешных атак.Современные технологии, такие как Интернет вещей (IoT), открывают новые возможности, но также увеличивают количество уязвимых точек, требующих строгих мер безопасности на уровне устройств и сетей

Таким образом, долгосрочная устойчивость и развитие энергетического сектора зависят от системного управления киберрисками, сочетающего технические решения, организационные меры и вовлеченность персонала. Только комплексный подход обеспечивает надежность критической инфраструктуры и защиту для будущих поколений.

Литература:

4. NIST. Cybersecurity Framework. — https://www.nist.gov/cyberframework
5. ISO. ISO/IEC 27001. — https://www.iso.org/isoiec-27001
6. CISA. Cybersecurity. — https://www.cisa.gov/cybersecurity
7. US DOE. Cybersecurity for Energy Sector. — https://www.energy.gov/oe/cybersecurity
8. ENISA. European Union Agency for Cybersecurity. — https://www.enisa.europa.eu
9. Smart Grid. Smart Grids and Cybersecurity. — https://www.smartgrid.gov
10. IoT Security Foundation. IoT Security in Energy Sector. — https://www.iotsecurityfoundation.org
11. ScienceDirect. Big Data Analytics in Energy. — https://www.sciencedirect.com/topics/computer-science/big-data-analytics-in-energy
12. NIST. Cyber-Physical Systems. — https://www.nist.gov/cyber-physical-systems
13. IEEE. Renewable Energy and Cybersecurity. — https://www.ieee.org
14. CISA. Energy Sector. — https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector
15. US-CERT. Cybersecurity Resources. — https://www.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf
16. NIST. Cybersecurity Framework. — https://www.nist.gov/cyberframework

17. IEEE. Climate Change and Energy. — https://ieee-pes.org/climate-change-content/
18. NIST. Cybersecurity Training – The Human Factor. — https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf
19. CISA. Cyber Threats to Critical Infrastructure. — https://www.cisa.gov/topics/cyber-threats-and-advisories
20. Insurica. Colonial Pipeline Ransomware Attack. — https://insurica.com/blog/colonial-pipeline-ransomware-attack/
21. US DOE. Cybersecurity Strategy 2024. — https://www.energy.gov/cio/articles/doe-cybersecurity-strategy-2024
22. NCSC. Cyber Threats to Energy Sector. — https://www.ncsc.gov.uk/
23. NIST. Cybersecurity Framework v2.0. — https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework
24. NIST. Cybersecurity Framework – PDF. — https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
25. ISO. ISO/IEC 27002 Overview. — https://www.isms.online/iso-27002/#:~:text=ISO%2FIEC%2027002%3A2022%20is,implementing%20an%20ISO%2027001%20ISMS
26. IEEE Xplore. Cybersecurity in Energy Sector. — https://ieeexplore.ieee.org/document/8461501
27. Springer. Artificial Intelligence in Cybersecurity. — https://link.springer.com/chapter/10.1007/978-3-030-41106-6_4
28. Duke Energy. Cybersecurity Role Development. — https://illumination.duke-energy.com/articles/how-caleb-foster-earned-his-way-into-a-cybersecurity-role
29. NIST. Cybersecurity Framework. — https://www.nist.gov/cyberframework
30. IoT Security Foundation. IoT Security. — https://iotsecurityfoundation.org/
31. US DOE. Cybersecurity in Energy Sector. — https://www.energy.gov/cybersecurity
32. World Economic Forum. Blockchain for Net Zero. — https://www.weforum.org/agenda/2023/05/setting-blockchain-on-a-net-zero-path/
33. ManageEngine. CISA Cybersecurity Culture. — https://insights.manageengine.com/it-security/cisa-wants-you-to-harden-your-cybersecurity-culture/

ENERGY SECURITY IN THE DIGITAL ERA: THE ROLE OF CYBERSECURITY

Abstract

This article examines cybersecurity as a critical component of energy security. It analyzes cyber threats, IT–OT integration, and the impact of emerging technologies such as IoT, AI, and blockchain. The study emphasizes a comprehensive approach: technical solutions (encryption, IDS, smart grids), organizational measures (policies, specialized teams), and human factors (training, security culture). Notable incidents are discussed, along with risk mitigation strategies. Effective cyber risk management ensures infrastructure protection, economic stability, and sustainable development. Recommendations include investing in technologies, standardizing processes, cross-sector collaboration, and integrating renewable energy.

Keywords: energy security, cybersecurity, digitalization, renewable energy, threats.

RƏQƏMSAL DÖVRDƏ ENERJI TƏHLÜKƏSIZLIYI: KIBER TƏHLÜKƏSIZLIYIN ROLU

Xülasə

Məqalədə kiber təhlükəsizlik rəqəmsal dövrdə enerji təhlükəsizliyinin əsas elementi kimi araşdırılır. Təhlil edilən çağırışlar: kiberhücumlar, informasiya və əməliyyat texnologiyalarının inteqrasiyası, IoT, AI və blokçeyn.Kompleks yanaşma: texnoloji həllər (şifrələmə, IDS, ağıllı şəbəkələr), təşkilati tədbirlər (siyasətlər, ixtisaslaşdırılmış komandalar) və insan faktoru (təlim, təhlükəsizlik mədəniyyəti). Məqalədə kritik infrastrukturun zəifliyi və risklərin azaldılması strategiyaları təqdim olunur.Effektiv kiber risklərin idarə olunması infrastrukturu qoruyur, iqtisadi sabitliyi və dayanıqlı inkişafı dəstəkləyir. Tövsiyələr: texnologiyalara investisiya, proseslərin standartlaşdırılması, sektorlararası əməkdaşlıq, bərpa olunan enerji mənbələrinin inteqrasiyası.

Açar sözlər: enerji təhlükəsizliyi, kiber təhlükəsizlik, rəqəmsallaşma, bərpa olunan enerji, təhdidlər.