Киберсуверенитет Государства и Критические Инфраструктуры: Проблемы и Пути Их Решения

Рамиз Алыгулиев[1], Людмила Сухостат[2]
[1,2]Институт Информационных Технологий, Баку, Азербайджан
[1]r.aliguliyev@gmail.com, [2]lsuhostat@hotmail.com

***Аннотация*— Обеспечение безопасности критических инфраструктур имеет решающее значение для обеспечения цифрового суверенитета государства путем их защиты от внешних киберугроз. Последствия кибератак, таких как DDoS-атаки, несанкционированный доступ и др., сводят на нет принципы цифрового суверенитета. Государства должны противостоять постоянно растущим и меняющимся угрозам. В данном исследовании анализируются текущие проблемы безопасности критических инфраструктур с целью обеспечения киберсуверенитета государства, включая различные уязвимости и угрозы. Исследуются международный опыт и стандарты обеспечения кибербезопасности критических инфраструктур. Данное исследование может способствовать повышению киберустойчивости критической инфраструктуры в целях поддержки цифрового суверенитета. В данной работе подчеркиваются важные вопросы, связанные с киберсуверенитетом и безопасностью критической инфраструктуры в условиях быстро меняющегося мира, движимого цифровой трансформацией.**

Ключевые слова— киберсуверенитет; критическая инфраструктура; киберугрозы; киберустойчивость.

I. Введение

Цифровой суверенитет и кибербезопасность взаимоствязаны. Обеспечение кибербезопасности важно для защиты государства, его национальных интересов от кибератак или внешнего вмешательства со стороны иностранных субъектов. Кибербезопасность должна обеспечивать защиту персональных данных граждан и конфиденциальности национальных данных, снижая риск внешнего наблюдения [1]. Кибербезопасность обеспечивает устойчивость к киберугрозам, которые могут подорвать суверенитет, а также укрепляет доверие к национальной инфраструктуре [2].

Сложности при обеспечении киберсуверенитета связаны с зависимостью от иностранных технологий, в частности, ПО, технологий и оборудования. Это создает риски в виде уязвимостей, которые могут быть использованы для шпионажа. С появлением новых технологий проблемы усугубляются, возникают новые уязвимости, и увеличивается поверхность кибератак.

В настоящее время проводятся исследования в области кибербезопасности в стремлении к обеспечению киберсуверенитета. Это доказывает, что политические, законодательные и стратегические аспекты киберсуверенитета находятся в центре внимания общества.

Изменение обстановки в сфере кибербезопасности и более разнообразные угрозы усилили необходимость защиты критической инфраструктуры и повышения киберустойчивости критически важных объектов.

На сегодняшний день в Азербайджанской Республике все технологии Индустрии 4.0 применяются в различных критических инфраструктурах, таких как нефтегазовые платформы, транспортные системы и т.д. 17 апреля 2021 года был подписан указ «О некоторых мерах по обеспечению безопасности критической информационной инфраструктуры».

Понятие «критическая информационная инфраструктура» закреплено в Законе Азербайджанской Республики «Об информации, информатизации и защите информации». 28 августа 2023 утверждена «Стратегия информационной и кибербезопасности Азербайджанской Республики на 2023-2027 годы». 29 ноября 2024 года кабинет министров Азербайджана утвердил «Перечень объектов критической информационной инфраструктуры».

На Рис. 1 показано, как критическая инфраструктура связана с различными прикладными технологиями. В совокупности эти технологии способствуют переходу к интеллектуальным, адаптивным и человекоцентрированным системам, улучшая взаимодействие в режиме реального времени, киберустойчивость и персонализацию в различных отраслях.

Цифровой суверенитет связан с критической инфраструктурой, так как эти понятия неразрывны. Национальная кибербезопасность все больше переплетается с защитой критической инфраструктуры.

Критическая инфраструктура состоит из множества подключенных устройств и систем для сбора и обмена огромными объемами данных на платформах ОТ (операционные технологии) и ИТ (информационные технологии).

Защита критической инфраструктуры начинается с регулирования суверенитета данных. Необходимо обеспечить киберустойчивость критической инфраструктуры.

DOI: 10.25045/cyber.gov.2026.05

Рисунок 1. Критическая инфраструктура и современные технологии.

Кибербезопасность критической инфраструктуры больше не является чем-то необязательным или чисто техническим. Цифровой суверенитет, прозрачность и стратегический контроль имеют важное значение для национальной устойчивости в эпоху нестабильной геополитической обстановки. Киберсуверенитет требует наличия критической инфраструктуры, обладающей суверенитетом – облачных сред и сетей, масштабируемых по мере развития задач. Для этого государства работают над повышением киберустойчивости критической инфраструктуры и внедрением ИИ в операции по обеспечению кибербезопасности.

19 марта 2025 года в Азербайджанской Республике утверждена «Стратегия искусственного интеллекта на 2025-2028 годы».

Критически важная инфраструктура – это энергетические системы, транспорт, здравоохранение, финансы и связь, являющиеся мишенью киберзлоумышленников. Критическая инфраструктура влияет на социальную, экономическую и государственную деятельность. При этом сбои в системе могут привести к необратимым последствиям, включая значительные финансовые потери и угрозу общественной безопасности [3].

Будучи энергетическим и транзитным узлом, Азербайджан особенно уязвим для киберугроз, способных нарушить работу нефтегазовых предприятий, сетей связи и национальных логистических систем [4].

Из-за роста числа кибератак на критически важную инфраструктуру, государства во всем мире стремятся повысить киберустойчивость этих стратегических национальных активов [5].

После кибератаки Stuxnet наблюдается рост кибератак на критическую инфраструктуру. Был проанализирован набор данных из Европейского репозитория кибер-инцидентов (EuRepoC) [6]. EuRepoC — это независимый исследовательский консорциум, предоставляющий научно обоснованный анализ киберинцидентов для лучшего понимания текущей ситуации с киберугрозами. Он предоставляет всеобъемлющую, междисциплинарную и постоянно обновляемую базу данных киберинцидентов с 2000 года по настоящее время по всему миру. EuRepoC рассматривает инциденты из ~3000 статей и 220 источников, сканируемых и обрабатываемых ежедневно.

На Рис. 2 приведены данные полученные из панели мониторинга EuRepoC, которые дают обзор киберинцидентов против критической инфраструктуры в мире в период с 01.01.2005 по сегодняшний день.

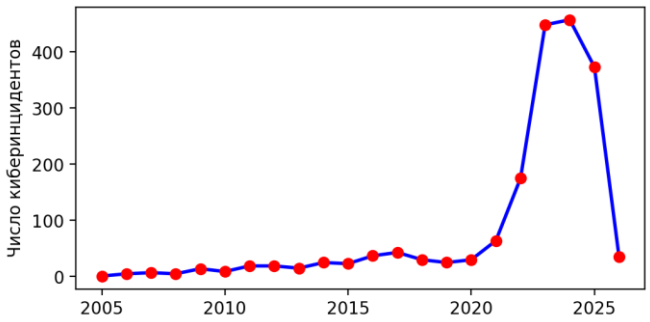

Рисунок 2. Число киберинцидентов против критической инфраструктуры в мире (источник: EuRepoC dashboard)

Видно, что ситуация значительно ухудшилась в глобальном масштабе, особенно за последние 4 года. Так в 2024 году количество киберинцидентов против критической инфраструктуры составило 457. Дальнейший анализ соответствующих случаев позволяет получить более глубокое понимание ситуации в мире и выявить новые киберугрозы.

II. Кибератаки на Критическую Инфраструктуру

Киберугрозы для критической инфраструктуры характеризуются не только количеством, но еще и сложностью и масштабами разрушительных последствий в результате кибератак. Последние могут осуществляться не только отдельными лицами или группами, но и государственными субъектами с целью саботажа, шпионажа, дезинформации и т.д. [7]. В Таблице 1. приводятся примеры кибератак на критическую инфраструктуру различных стран.

Выделятся такие типы киберугроз как постоянная угрозы повышенной сложности (Advanced Persistent Threat, APT), уязвимость нулевого дня, атака программ-вымогателей (ransomware), инсайдерская угроза, распределенный отказ в обслуживании (Distributed Denial of Service, DDoS).

ТАБЛИЦА 1. ПРИМЕРЫ КИБЕРУГРОЗ ДЛЯ КРИТИЧЕСКОЙ ИНФРАСТРУСТРУКТУРЫ

Тип киберугрозы	Примеры кибератак	Цель кибератаки	Описание
APT	Stuxnet (2010)	Ядерные объекты Ирана	Ранее неизвестные уязвимости Windows были использованы для заражения систем и дальнейшего распространения.
Уязвимость нулевого дня	WannaCry (2017)	Компьютерные системы пользователей, а также ряд коммерческих и государственных структур	Наличие уязвимостей старых версий ОС Windows позволило получить контроль над системой с целью получения выкупа.
Ransomware	Colonial pipeline attack (2021)	Трубопровод США по поставкам нефти и газа.	Кибератака с использованием вымогателя DarkSide привела к вынужденному отключению некоторых ОТ-систем.
Кибератака с применением ИИ	DeepLocker (2018)	Вирус-вымогатель WannaCry был скрыт в приложении для видеоконференций.	Исследователи IBM представили кибератаку, которая активировалось только при обнаружении цели.
Инсайдерская угроза	Кибератака на систему водоснабжения Пенсильвании (2023)	Получение доступа к контроллерам Unitronics водонасосной станции.	Уязвимость при использовании небезопасных или стандартных паролей на оборудовании, подключенном к интернету привела к переводу системы в режим ручного управления.
DDoS	Атаки на DNS-серверы (2016)	Осуществлялась через ботнет, состоящий из миллионов IoT устройств.	Привела к перегрузке сети и вывела из строя удаленные узлы.

Кибератака с применением ИИ в настоящее время получают большое развитие, предотвратить которые становится сложно традиционными методами. С этим может помочь справиться разработка комплексных и контекстуальных стратегий защиты.

Киберфизические угрозы сложны и требуют быстрого реагирования со стороны служб безопасности. С точки зрения киберсуверенитета - это экзистенциальные угрозы национальной автономии [7].

Обеспечение кибербезопасности и киберустойчивости критической инфраструктуры стран — это критически важный аспект поддержания государственного киберсуверенитета. Децентрализация приводит к тому, что любой незащищенный объект критической инфраструктуры может привести к краже персональных данных, нарушить целостность (integrity) и достигаемость (availability) [8].

Методы машинного обучения показали свою применимость в обеспечении сохранения киберсуверенитета перед лицом различных киберугроз для критических инфраструктур. Однако, современные подходы с применением искусственного интеллекта (ИИ) их превосходят с точки зрения эффективности [9]. Например, широкое распространение получили гибридные модели, визуальная обработка и анализ текстовых данных.

Ahmad и соавт. (2025) предложили комплексную систему, способную в режиме реального времени обнаруживать вторжения и учитывать конфиденциальность решения, которое обеспечивает адаптивную кибербезопасность критической инфраструктуры [10]. В качестве примера была рассмотрена система водоочистки SWaT. В работе [11] описана система PRAETORIAN для обнаружения угроз и генерации оповещений, связанных с физической и кибер-областями критически важных инфраструктур. Система координации реагирования помогает в принятии решений, предоставляя информацию о мерах по смягчению последствий. Tirulo и соавт. (2025) предложили генеративную структуру на основе ИИ, которая использует большие языковые модели (Large Language Models, LLM) для проактивного выявления атак нулевого дня в КФС [12]. В работе [9] был разработан подход на основе ИИ для обеспечения киберустойчивости нелинейных динамических систем к кибератакам, что знаменует собой повышение безопасности КФС.

III. МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ПО ОБЕСПЕЧЕНИЮ КИБЕРУСТОЙЧИВОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Ниже представлены стандарты, которые могут служить полезным руководством по оценке киберустойчивости критической инфраструктуры. Эти стандарты были проанализированы с целью выявления информации, связанной с обеспечением киберустойчивости, такой как определения, руководства, рекомендации, требования, а также ссылки на методы оценки кибербезопасности [13]:

ISO 22301:2019 - Security and resilience

NIST SP 800-160 - Developing Cyber Resilient Systems: A Systems Security Engineering Approach

NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security

ISO 10218 - Industrial robots – Safety requirements

ISO/IEC 27001 - Information security, cybersecurity and privacy protection

ISO/IEC 27002 - Information technology — Security techniques — Code of practice for information security controls

ISA/IEC 62443 - Industrial Automation and Control Systems Security

ISO 13849 - Safety of machinery - Safety-related parts of control systems.

ISO 22301

Стандарт ISO 22301 имеет решающее значение для повышения устойчивости организаций к различным непредвиденным сбоям, обеспечивая непрерывность операций и услуг [14].

ISO 10218

ISO 10218 — это стандарт, регулирующий требования безопасности промышленных роботов, включая коботов [15]. Он также определяет уровень защиты и уровень целостности безопасности с целью снижения риска до приемлемого уровня для систем управления в различных ситуациях. Он охватывает безопасную остановку, обучение, контроль скорости и расстояния между транспортными средствами, а также ограничение мощности.

ISO 13849

Стандарт ISO 13849 устанавливает требования безопасности и содержит рекомендации по принципам проектирования и интеграции компонентов систем управления, связанных с безопасностью, включая проектирование программного обеспечения. Хотя в стандарте ISO 13849 используются различные методологии проектирования систем управления, связанных с безопасностью, его цель – снижение рисков [16].

NIST SP 800-160

Так NIST представил специальную публикацию «Разработка киберустойчивых систем: подход к проектированию системной безопасности», в которой определяется набор методов обеспечения киберустойчивости. Каждый метод включает в себя набор стандартных методологий и практик, направленных на разработку систем, устойчивых к атакам.

ISO/IEC 27001 и ISO/IEC 27002

ISO/IEC 27001 [17] является наиболее фундаментальным стандартом управления информационной безопасностью, признанным во всем мире и применяемым организациями различного профиля (коммерческими, государственными, некоммерческими и т. д.) и размеров. Стандарты имеют широкий охват и не ориентированы на какую-либо конкретную область, сектор или технологию. ISO 27002 предоставляет вспомогательные, практические рекомендации по внедрению ISO 27001 [18].

Международные стандарты ISO/IEC 27001 и 27002 могут применяться ко всем компонентам архитектуры интеллектуальной сети. Меры и цели безопасности, определенные в стандартах, могут быть подвергнуты оценке кибербезопасности.

ISA/IEC 62443

IEC 62443 (ранее ISA99) — это набор международных стандартов, посвященных безопасности систем промышленной автоматизации и управления, которые являются жизненно важным компонентом критической инфраструктуры (например, интеллектуальных энергосетей). Набор стандартов может применяться для тестирования на соответствие всех компонентов архитектуры интеллектуальной сети.

NIST SP 800-82

NIST SP 800-82 «Руководство по безопасности промышленных систем управления» — это основная публикация NIST, посвященная безопасности промышленных систем управления [19]. Он широко признан и принят во всем мире.

Стандарт представлен как Инструмент оценки кибербезопасности (Cyber Security Evaluation Tool , CSET), разработанный Министерством внутренней безопасности (Department of Homeland Security, DHS). CSET призван помочь организациям в защите их ключевых кибер-активов, предоставляя систематический и воспроизводимый подход к оценке киберустойчивости.

Т.о., представлены стандарты, направленные на решение проблемы киберустойчивости критической инфраструктуры, предоставляющие обоснованные рекомендации по оценке безопасности. Однако, очевидна необходимость дальнейших исследований.

IV. Международный Опыт по Обеспечению Кибербезопасности Критической Инфраструктуры

В результате известных кибератак на критическую инфраструктуру страны по всему миру принимают соответствующие стратегии защиты своего киберсуверенитета (Таблица 2). Государства выявляют объекты, критически важные для общества, и укреплять их способность противостоять сбоям и кризисам. Законы регулируют не только информационную безопасность, но и физическую защиту объектов от атак.

Можно отметить ряд законодательных актов, устанавливающих минимальные стандарты защиты критической инфраструктуры в рамках государственных политик.

ТАБЛИЦА 2. МЕЖДУНАРОДНЫЙ ОПЫТ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Страна	Законы о безопасности критической инфраструктуры	Сектора критической инфраструктуры
США	Закон о защите критической инфраструктуры (2001), Закон об отчетности о киберинцидентах (CIRCIA 2022), Меморандум по национальной безопасности (NSM-22) об устойчивости критической инфраструктуры	Химическая промышленность, оборонная промышленность, энергетика, здравоохранение и др. (16 секторов)
КНР	Закон о кибербезопасности (CSL), Закон о защите данных (DSL), Закон о защите персональных данных (PIPL)	Государственные коммуникационные и информационные услуги, энергетика, транспорт, водные ресурсы, финансы и др.
ЕС	Закон о данных, Закон об управлении данными Закон об ИИ GDPR	Энергетика, транспорт, здравоохранение, цифровая инфраструктура, космические технологии и др. (11 секторов)
Австралия	Закон о безопасности критической инфраструктуры (SOCI Act 2018)	Энергетика, водоснабжение, транспорт, здравоохранение, финансы и др. (11 секторов)
Новая Зеландия	Закон об управлении чрезвычайными ситуациями в области гражданской обороны (2002)	Энергетика, здравоохранение, транспорт, водоснабжение и коммуникации.
Финляндия	Закон о защите критически важной для общества инфраструктуры и повышении ее устойчивости (CER Act 2025)	Энергетика, транспорт, здравоохранение, цифровая инфраструктура, космические технологии и др. (11 секторов)

V. ПРОБЛЕМЫ И РЕШЕНИЯ

Одной из главных проблем в обеспечении безопасности критически важной кибер-инфраструктуры является наличие системных уязвимостей, которые часто трудно обнаружить и контролировать. Эти уязвимости возникают не только из-за технических недостатков в аппаратном и программном обеспечении устройств, но также включают человеческий фактор, процессы управления и ограничения существующих политик и правил [3].

Современное киберпространство представляет собой ряд угроз национальной безопасности, которые неизбежно затрагивают суверенитет государств. На основе анализа ряда источников и доктрин в области кибербезопасности мы выделили следующие угрозы и вызовы, которые они представляют для государственной безопасности (Таблица 3) [20].

ТАБЛИЦА 3. УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ И ВЫЗОВЫ КИБЕРСУВЕРЕНИТЕТУ ГОСУДАРСТВА

Киберугроза	Вызовы киберсуверенитету государства
Кибератаки на критическую инфраструктуру. Атаки на энергетические системы, транспортные сети, финансовые учреждения и другие жизненно важные сектора могут иметь разрушительные последствия для национальной безопасности и экономики.	**Экономические потери.** Атаки на критическую инфраструктуру могут привести к значительным экономическим потерям и увеличить зависимость от международной помощи для восстановления.
Дезинформация. Целенаправленное распространение ложной информации через социальные сети или другие онлайн-каналы может подорвать демократические процессы, посеяв путаницу и конфликты в обществе.	**Потеря контроля над информационным пространством.** Кибератаки и кампании по дезинформации могут подорвать доверие общественности к правительству и институтам, ослабив способность государства обеспечивать информационную безопасность.
Кибершпионаж. Враждебные государства или злоумышленники могут использовать киберпространство для шпионажа с целью получения доступа к конфиденциальной информации, военным секретам или интеллектуальной собственности.	**Нарушение конфиденциальности.** Кибершпионаж и фишинговые атаки угрожают конфиденциальной информации, что может привести к потере суверенного контроля над внутренними данными.
Кибертерроризм. Использование киберпространства террористическими группами для подрыва национальной безопасности, причинения вреда гражданам или создания массовой паники.	**Вызовы национальной обороне.** Кибертерроризм и крупномасштабные кибератаки требуют от государств разработки новых оборонных стратегий и технологий, что также может изменить традиционные подходы к национальной безопасности.

Когда национальная безопасность государства находится под угрозой киберинцидентов, это не только нарушает внутренний порядок и стабильность, но и ставит под сомнение его способность защитить себя и своих граждан. Такие инциденты могут служить признаком слабости государства перед лицом международного сообщества, снижая его авторитет и влияние на международной арене. Нарушение национальной безопасности вследствие киберугроз также приводит к необходимости пересмотра стратегий национальной безопасности и инвестиций в киберзащиту. Это, в свою очередь, требует значительных ресурсов и может

ограничить суверенитет государства из-за усиления зависимости от международной технической помощи и сотрудничества в области кибербезопасности. Таким образом, киберугрозы представляют собой серьезный вызов национальной безопасности и суверенитету государств. Они требуют комплексного подхода к разработке и внедрению эффективных стратегий кибербезопасности, которые могли бы защитить критическую инфраструктуру, укрепить правовую основу для противодействия киберугрозам и развивать международное сотрудничество в области кибербезопасности для укрепления национального суверенитета.

Заключение

Что касается управления кибербезопасностью критической инфраструктуры в рамках обеспечения киберсуверенитета государств, прежде всего следует отметить, что невозможно защитить всю инфраструктуру от угрозы террористических кибератак. Однако, применяя методы управления киберрисками, можно сосредоточить внимание на областях наибольшего риска. Обеспечение киберустойчивости — это целенаправленный процесс определения киберрисков, принятия решений и реализации мер по снижению рисков до определенного уровня при приемлемых затратах.

Можно выделить следующие тенденции:

Атаки на критическую инфраструктуру и объекты с высокими требованиями к безопасности: увеличивается число целевых атак на промышленные предприятия, энергетические объекты, объекты транспортной инфраструктуры, что требует внедрения более сложных и многоуровневых систем защиты.

Интеграция киберугроз и физических угроз: кибератаки становятся частью комплексных сценариев, например, отключение систем видеонаблюдения для проведения физического проникновения или саботажа.

Применение искусственного интеллекта и автоматизированных систем: с их помощью злоумышленники ищут уязвимости в системах физической безопасности и проводят многоступенчатые атаки с применением дипфейков, социальной инженерии и автоматизированных сценариев.

Многоуровневая защита должна включать диверсификацию технологий. Избегайте опоры на один технологический блок, распределяя западные и незападные технологии по различным уровням безопасности, чтобы снизить системные и геополитические риски.

Применение криптографии — это решение связанное с киберсуверенитетом. Государства должны принять стратегии по созданию «собственных ключей» и разработать технологии, устойчивые к квантовым кибератакам для обеспечения долгосрочной защиты.

Разработка отечественных технологий, таких как межсетевые экраны, EDR (Endpoint Detection and Response), DPI (Deep Packet Inspection) и др., с целью обеспечения киберустойчивость, которые смогут дополнить коммерческие решения.

Ключевые стратегические направления по обеспечению киберсуверенитета:

Определение уровней: Государства определяют и обеспечивают различные уровни суверенитета данных, операционной и технической безопасности.

Обеспечение безопасности секторов критической инфраструктуры (энергетика, транспорт, финансы): Обеспечение киберустойчивости критической инфраструктуры к киберфизическим атакам посредством локализованного контроля, переходя от простого облачного хостинга к активному локальному оперативному управлению.

Соблюдение нормативных требований: Обеспечение соблюдения законов о защите данных (например, GDPR (General Data Protection Regulation)).

Подводя итоги, в данной статье предпринимается попытка подчеркнуть важные вопросы, связанные с киберсуверенитетом и безопасностью критической инфраструктуры в условиях быстро меняющегося мира, движимого цифровой трансформацией.

Список Литературы

[1] C. Demchak and P. Dombrowski, “Rise of a cybered Westphalian age,” Strategic Studies Quarterly, vol. 5, no. 1, pp. 32-61, 2011.

[2] J. Lewis, “Sovereignty and the role of government in cyberspace,” The Brown Journal of World Affairs, vol. 16, no. 2, pp. 55-65, 2010.

[3] A. Dengkeng, A. Halid, G. Pratiwi, and A. I. Rachman, “Cyber security challenges and solutions in critical infrastructure: A systematic review of threat spectrum, systemic vulnerabilities, and multi-level protection strategies,” Journal La Multiapp, vol. 6, no. 5, pp. 1183-1193, 2025. https://doi.org/10.37899/journallamultiapp.v6i5.2469

[4] “Cyber Sovereignty in the 21st Century: How Azerbaijan Is Building a Digital Shield, Baku Network.” 2026. [Online]. https://www.bakunetwork.org/en/news/analytics/14672

[5] “Cybersecurity and critical infrastructure defence strategies converging, GovInsider.” 2026. [Online]. https://govinsider.asia/intl-en/article/cybersecurity-and-critical-infrastructure-defence-strategies-converging

[6] “EuRepoC: European Repository of Cyber Incidents.” 2026. [Online]. https://eurepoc.eu/

[7] I. C. Tochukwu, O. F. Nonyelum, S. Misra, and S. Chockalingam, “Securing mobile edge computing: A survey on cyber-physical threat mitigation for digital sovereignty,” Procedia Computer Science, vol. 254, pp. 211-220, 2024. https://doi.org/10.1016/j.procs.2025.02.080

[8] H. Zeyu, X. Geming, W. Zhaohang, and Y. Sen, “Survey on Edge Computing Security,” In Proc. of International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), 2020, pp. 96–105. https://doi.org/10.1109/ICBAIE49996.2020.00027

[9] Y. Li, S. Zhang, and Y. Li, “AI-enhanced resilience in power systems: Adversarial deep learning for robust short-term voltage stability assessment under cyber-attacks,” Chaos, Solitons & Fractals, vol. 196, 116406, 2025. https://doi.org/10.1016/j.chaos.2025.116406

[10] H. B. Ahmad, H. Gao, and N. Latif, “Adaptive anomaly detection and classification in critical infrastructure systems: A real-time privacy-preserving multi-model framework,” High-Confidence Computing, 100360, in press. https://doi.org/10.1016/j.hcc.2025.100360

[11] L. Papadopoulos, K. Demestichas, E. Muñoz-Navarro, J. J. Hernández-Montesinos, S. Paul, N. Museux, S. König, S. Schauer, A. C. Alarcón, I.

P. Llopis, T. Stelkens-Kobsch, T. Hadjina, and J. Levak, "Protection of critical infrastructures from advanced combined cyber and physical threats: The PRAETORIAN approach," International Journal of Critical Infrastructure Protection, vol. 44, 100657, 2024. https://doi.org/10.1016/j.ijcip.2023.100657

[12] A. Tirulo, S. Chauhan, and M. Shafie-khah, "LLM-powered threat intelligence: Proactive detection of zero-day attacks in electric vehicle cyber-physical systems," Sustainable Energy, Grids and Networks, vol. 43, 101877, 2025. https://doi.org/10.1016/j.segan.2025.101877

[13] R. Leszczyna, "Standards on cyber security assessment of smart grid," International Journal of Critical Infrastructure Protection, vol. 22, pp. 70-89, 2018. https://doi.org/10.1016/j.ijcip.2018.05.006

[14] "ISO 22301, Security and resilience – Business continuity management systems – Requirements. International Organization for Standardization." 2019. [Online]. https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en

[15] S. Basu, "Plant hazard analysis and safety instrumentation systems,. Elsevier. Academic Press, 2025. https://doi.org/10.1016/C2024-0-00374-8

[16] M. Sága, I. Kuric, I. Klačková, and D. Więcek, "Comparison of risk assessment approaches and analyzes used in technical transport systems," Transportation Research Procedia, vol. 74, pp. 516-521, 2022. https://doi.org/10.1016/j.trpro.2023.11.176

[17] "ISO/IEC, ISO/IEC 27001:2013: Information technology Security techniques Information security management systems Requirements. International Organization for Standardization." 2013. [Online]. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[18] "ISO/IEC, ISO/IEC 27002:2013: Information technology –Security techniques – Code of practice for information security controls. International Organization for Standardization." 2013. [Online]. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

[19] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, NIST SP 800-82 Guide to Industrial Control Systems ICS Security Revision 2. Technical report, NIST, 2015.

[20] N. Makovetska, G. O. Dubov, T. O. Didych, B. V. Malyshev, and O. Varych, "Global challenges to state sovereignty in the 21st century," Salud, Ciencia y Tecnología - Serie de Conferencias, vol. 3, pp. 1-13, 2024. https://doi.org/10.56294/sctconf2024.661.

Government Cybersovereignty and Critical Infrastructures: Problems and Solutions

Ramiz Aliguliyev[1], Lyudmila Sukhostat[2]
[1,2]Institute of Information Technology, Baku, Azerbaijan

***Abstract*—** Ensuring the security of critical infrastructure is crucial to protecting the government's digital sovereignty against external cyber threats. The consequences of cyberattacks, such as DDoS attacks, unauthorized access, and others, undermine the principles of digital sovereignty. The government must counter constantly growing and evolving threats. This study analyses current critical infrastructure security issues to ensure state cybersovereignty, including various vulnerabilities and threats. International experience and standards for ensuring the cybersecurity of critical infrastructure are explored. This research can contribute to the cyberresilience of critical infrastructure to support digital sovereignty. This paper highlights important issues related to cybersovereignty and the cybersecurity of critical infrastructure in a rapidly changing world driven by digital transformation.

Keywords— cybersovereignty; critical infrastructure; cyberthreats; cyberresilience.