УДК 343.34:004
ББК 67.408.135

ЦИФРОВАЯ ИНФРАСТРУКТУРА И КИБЕРБЕЗОПАСНОСТЬ КАК ОСНОВОПОЛАГАЮЩИЕ КОМПОНЕНТЫ СТРАТЕГИЧЕСКОЙ ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ

Ю. П. Хамутовская
Луганский государственный университет им. В. Даля (Луганск, Россия)

В данной статье рассматривается цифровая инфраструктура и кибербезопасность в качестве ключевых элементов стратегической технологической независимости государства. Проводится анализ взаимозависимости между развитием суверенной цифровой инфраструктуры и обеспечением кибербезопасности в рамках формирования технологического суверенитета. Также рассматривается международный и российский опыт защиты критической информационной инфраструктуры. Подчеркивается необходимость комплексного подхода к обеспечению технологической самостоятельности через развитие собственных программных и аппаратных решений, а также систем кибербезопасности.

Ключевые слова: цифровая инфраструктура, кибербезопасность, технологическая самостоятельность, цифровой суверенитет, критическая информационная инфраструктура, информационная безопасность

DIGITAL INFRASTRUCTURE AND CYBERSECURITY AS FUNDAMENTAL COMPONENTS OF STRATEGIC TECHNOLOGICAL INDEPENDENCE

Yu. P. Khamutovskaya
Lugansk State University named after V. Dal (Lugansk, Russia)

This article examines digital infrastructure and cybersecurity as key elements of a state's strategic technological independence. It analyzes the interdependence between the development of sovereign digital infrastructure and cybersecurity as part of the development of technological sovereignty. It also examines international and Russian experience in protecting critical information infrastructure. It emphasizes the need for a comprehensive approach to ensuring technological independence through the development of domestic software and hardware solutions, as well as cybersecurity systems.

Keywords: digital infrastructure, cybersecurity, technological independence, digital sovereignty, critical information infrastructure, information security

Doi: https://doi.org/10.14258/ralj(2025)3.9

В условиях быстрого прогресса цифровизации, охватывающего все аспекты жизнедеятельности как общества, так и государственного управления, вопросы, касающиеся обеспечения стратегической технологической независимости, становятся критически важными. Эта тенденция обусловлена необходимостью адаптации к новым экономическим и социальным реалиям, что ставит стратегическую технологическую самостоятельность в центр общественного и политического дискурса.

Цифровая трансформация экономики и государственного управления, развитие информационно-коммуникационных технологий и внедрение инновационных решений создают новые возмож-

ности для развития, одновременно формируя принципиально новые вызовы и угрозы национальной безопасности. В этой связи цифровая инфраструктура и кибербезопасность становятся ключевыми факторами, определяющими способность государства осуществлять независимую технологическую политику и обеспечивать свой цифровой суверенитет.

Стратегическая технологическая самостоятельность представляет собой способность государства разрабатывать и применять критически важные технологии, обеспечивающие его независимость и конкурентоспособность на международной арене. В контексте цифровой экономики это понятие тесно связано с концепцией цифрового суверенитета, который определяется как самостоятельность государства в управлении цифровой трансформацией и формировании новой экосистемы, которая исключает возможность внешнего воздействия на его функционирование и устойчивость [1]. Цифровой суверенитет предполагает контроль над внешним контуром цифровой инфраструктуры, наличие автономной программной и аппаратной базы, развитый IT-сектор и технологии производства электронных компонентов.

Цифровая инфраструктура представляет собой комплекс взаимосвязанных информационных систем, технических средств, сетей электросвязи и организационных структур, обеспечивающих функционирование цифровой экономики и электронного государства. Она включает в себя сети передачи данных, центры обработки данных, системы хранения информации, программное обеспечение, аппаратные решения и иные компоненты, необходимые для эффективного функционирования цифровых сервисов и платформ. В условиях глобальной цифровизации и возрастающей взаимозависимости различных секторов экономики от информационных технологий надежная и защищенная цифровая инфраструктура становится критически важным фактором обеспечения национальной безопасности и технологической самостоятельности государства.

Кибербезопасность, в свою очередь, представляет собой совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных [2]. В современных условиях кибербезопасность не ограничивается только защитой компьютерных систем от вирусов и хакерских атак — она охватывает широкий спектр мер, направленных на обеспечение безопасности всей цифровой экосистемы, включая промышленные сети, облачные сервисы, интернет вещей, автоматизированные системы управления и иные элементы критической информационной инфраструктуры.

Взаимосвязь между цифровой инфраструктурой и кибербезопасностью проявляется в том, что без надежной защиты от киберугроз невозможно обеспечить стабильное функционирование цифровой инфраструктуры, а без развитой собственной инфраструктуры невозможно гарантировать должный уровень кибербезопасности. Эта взаимозависимость создает необходимость комплексного подхода к обеспечению технологической самостоятельности, охватывающего как развитие собственных технологических решений, так и формирование эффективной системы защиты от киберугроз.

Международный опыт показывает различные подходы к обеспечению цифрового суверенитета и кибербезопасности. Китай, являющийся лидером в данной области, реализует системную политику суверенизации цифровой сферы, включающую строгий контроль над информационными потоками, развитие собственных технологических платформ и систем, а также жесткое регулирование деятельности иностранных IT-компаний. В 2016 г. в Китае были приняты «Закон о кибербезопасности» и «Национальная стратегия безопасности киберпространства», которые закрепили принципы обеспечения суверенитета и национальной безопасности в киберпространстве [3]. Ключевым элементом китайской стратегии является инициатива «Цифровой шелковый путь», направленная на развитие трансграничной цифровой инфраструктуры и укрепление технологического влияния Китая.

В современном геополитическом и технологическом контексте Европейский Союз придает особую значимость формированию стратегической автономии, под которой подразумевается способность обеспечивать устойчивое развитие цифровой сферы без критической зависимости от внешних поставщиков и влияний. В рамках этой парадигмы Евросоюз предпринимает последовательные шаги, направленные на укрепление технологического суверенитета, повышение уровня защищенности цифровых инфраструктур и минимизацию уязвимостей, связанных с глобальной конкуренцией и транснациональными киберугрозами. Концептуальной основой данной политики стала принятая в 2020 г.

Стратегия кибербезопасности Европейского Союза, в которой акцент сделан не только на развитии нормативной и институциональной базы, но и на интеграции кибербезопасности в широкий спектр отраслей, критически значимых для функционирования современного цифрового общества [4]. При этом важнейшим координирующим звеном, на которое возложена реализация и методологическое сопровождение кибербезопасностных инициатив на наднациональном уровне, выступает Европейское агентство по сетевой и информационной безопасности (ENISA). Его функции охватывают как подготовку аналитических материалов и оценок угроз, так и разработку рекомендаций для гармонизации киберполитик государств-членов.

Анализируя подход, реализуемый в Соединенных Штатах Америки, следует подчеркнуть, что вопросы кибербезопасности приобрели системообразующий характер в архитектуре национальной безопасности. Создание в 2018 г. Агентства по кибербезопасности и защите инфраструктуры (CISA) стало институциональным ответом на усложнение киберугроз и на необходимость усиления защиты федеральных сетей и критических объектов. На этом фоне CISA выполняет не только функции по реагированию на инциденты и мониторингу уязвимостей, но и осуществляет стратегическую координацию между различными уровнями власти и частным сектором, что обеспечивает горизонтальную интеграцию усилий и обмен информацией в реальном времени [5]. Характерной особенностью американского подхода выступает сочетание централизованного государственного управления с активным участием негосударственных структур, что позволяет оперативно адаптироваться к изменяющимся вызовам цифровой среды. Такой баланс способствует выработке гибкой и динамичной модели управления кибербезопасностью, способной учитывать интересы как национальной обороны, так и рыночной конкуренции.

В Российской Федерации проблематика информационной и кибербезопасности также получила устойчивое развитие в рамках государственной политики, акцент которой сделан на достижении цифрового суверенитета и защите от внешних воздействий, способных нарушить функционирование ключевых информационно-телекоммуникационных систем. Законодательной основой регулирования в этой сфере стал Федеральный закон от 26.07.2017 г. № 187-ФЗ, детально регламентирующий вопросы безопасности критической информационной инфраструктуры. Этот нормативный акт не только установил правовой режим для субъектов, владеющих или эксплуатирующих соответствующие объекты, но и зафиксировал обязательства по принятию технических и организационных мер, направленных на предупреждение и отражение компьютерных атак. В дальнейшем в Стратегии национальной безопасности Российской Федерации, обновленной в 2021 г., вопросы обеспечения информационной устойчивости и цифровой независимости были институционализированы в качестве одного из приоритетов государственной политики [6]. Следует отметить, что в рамках реализации национальной программы «Цифровая экономика», а именно ее составной части — федерального проекта «Информационная безопасность», предпринимаются масштабные усилия по укреплению научно-технического потенциала, развитию отечественных технологий и формированию условий для автономного функционирования критически значимых информационных систем. Тем самым Россия стремится минимизировать зависимость от иностранных решений, одновременно развивая собственную инфраструктуру киберзащиты, способную эффективно реагировать на современные вызовы.

Очевидно, что глобальная трансформация в сфере цифровой безопасности требует от государств выстраивания комплексной, многоуровневой системы реагирования и превентивного управления рисками. Как показывает сравнительный анализ, несмотря на различие правовых и организационных моделей, все три рассмотренные юрисдикции — ЕС, США и РФ — исходят из понимания цифрового суверенитета как базовой предпосылки устойчивого развития, что само по себе свидетельствует о формировании нового вектора технологической конкуренции, в которой критической валютой становится способность к самодостаточному обеспечению информационной безопасности.

Для эффективного обеспечения стратегической технологической самостоятельности необходима реализация комплексного подхода, включающего следующие ключевые направления:

1. Развитие собственной технологической базы. Критически важно наличие отечественных решений в области аппаратного и программного обеспечения, особенно для объектов критической информационной инфраструктуры. Это включает разработку собственных операционных систем, СУБД,

средств защиты информации, микроэлектроники, сетевого оборудования и других компонентов цифровой инфраструктуры.

2. Формирование эффективной системы обеспечения кибербезопасности. Необходимо создание многоуровневой системы защиты от киберугроз, включающей организационные, правовые и технические меры. Важными элементами такой системы являются центры мониторинга и реагирования на компьютерные инциденты, системы обнаружения и предотвращения атак, механизмы обмена информацией о киберугрозах.

3. Развитие кадрового потенциала. Подготовка высококвалифицированных специалистов в области информационных технологий и кибербезопасности является фундаментальным условием для обеспечения технологической самостоятельности. Необходимо развивать образовательные программы, создавать научно-исследовательские центры и лаборатории, стимулировать научные исследования в данной сфере.

4. Совершенствование нормативно-правовой базы. Правовое регулирование должно обеспечивать баланс между развитием цифровых технологий и обеспечением безопасности. Необходимо разрабатывать современные стандарты и требования к информационным системам, регламентировать вопросы защиты персональных данных, определять правовой режим для новых технологий.

5. Международное сотрудничество. Несмотря на стремление к технологической самостоятельности, необходимо развивать взаимодействие с международными партнерами в области кибербезопасности, обмениваться опытом и координировать усилия по противодействию трансграничным киберугрозам.

Практическая реализация этих направлений требует системного подхода и значительных ресурсов. Примером успешной реализации таких мер может служить создание в России Единой цифровой платформы «ГосТех» — облачной платформы для госсектора, предназначенной для создания государственных информационных систем и цифровых сервисов [7]. Данная платформа обеспечивает единую информационную среду для органов государственной власти и способствует технологической независимости в сфере государственного управления.

Одним из значимых направлений государственной политики Российской Федерации в области обеспечения цифровой безопасности и подготовки профессиональных кадров, обладающих компетенциями в сфере противодействия киберугрозам, выступает реализация университетами проектов в рамках государственной программы «Приоритет 2030». Данная инициатива направлена на формирование научно-образовательных платформ, способных эффективно реагировать на вызовы цифровой трансформации и усиливающуюся конкуренцию в сфере высоких технологий. В частности, особого внимания заслуживает деятельность Московского государственного юридического университета им. О.Е. Кутафина (МГЮА), где развивается стратегическая инициатива под названием «Киберправо». В рамках данного проекта осуществляется комплексная подготовка специалистов, обладающих углубленными знаниями в области правового обеспечения информационной и кибербезопасности, что особенно важно в условиях динамичного изменения нормативной среды и усложнения механизмов регулирования цифровых угроз. Таким образом, образовательные учреждения становятся не только центрами генерации знаний, но и важнейшими агентами по формированию кадрового резерва для реализации государственной политики в сфере цифрового суверенитета.

Не менее примечателен опыт Национального исследовательского университета «МЭИ», где с целью практического моделирования и анализа рисков кибератак на энергетическую инфраструктуру был создан специализированный киберполигон, получивший название «Технологии транспортировки электроэнергии и распределенных интеллектуальных энергосистем». Данная экспериментальная площадка позволяет в контролируемой среде воспроизводить сценарии атак и отрабатывать алгоритмы реагирования на потенциальные угрозы, тем самым формируя практикоориентированные компетенции у студентов и исследователей, занятых в критически важной отрасли электроэнергетики. В этом контексте университетская наука приобретает стратегическое значение, становясь неотъемлемой частью национальной системы защиты от информационных угроз.

В современных условиях особую актуальность приобретает задача защиты критической информационной инфраструктуры (КИИ), представляющей собой интегрированную совокупность техно-

логических систем, программных решений и каналов передачи данных, без надежного функционирования которых невозможна стабильная работа базовых секторов экономики и социальной сферы. Согласно действующему определению, под КИИ понимается совокупность значимых объектов, а также инфраструктурных компонентов, обеспечивающих их взаимодействие, включая сети электросвязи, автоматизированные комплексы управления и информационные системы, действующие в стратегически значимых отраслях — здравоохранении, транспорте, связи, энергетике, оборонной промышленности, атомной энергетике, горнодобывающем и металлургическом секторах, финансовых институтах, а также в научных организациях. Учитывая масштаб и многоуровневую структуру КИИ, обеспечение ее безопасности требует не только правового регулирования и технического контроля, но и выстраивания межведомственных механизмов координации, оперативного обмена информацией и системы превентивного реагирования на инциденты.

Одним из ключевых элементов, обеспечивающих функционирование данной системы, является процедура категорирования объектов КИИ, на основании которой определяется степень значимости каждого из них и устанавливаются соответствующие уровни защиты. После категорирования для объектов разрабатываются индивидуализированные модели угроз и меры реагирования, интегрированные в единую государственную систему обнаружения и ликвидации последствий кибератак. Ведущую координирующую роль в данном процессе выполняет Национальный координационный центр по компьютерным инцидентам (НКЦКИ), задачей которого является организация совместных действий операторов КИИ, направленных на своевременное обнаружение, предупреждение и минимизацию ущерба от киберинцидентов. Эффективность функционирования такой структуры во многом зависит от качества взаимодействия между субъектами инфраструктуры и органов государственной власти, а также от уровня профессиональной подготовки персонала, способного действовать в условиях информационного кризиса.

Важно подчеркнуть, что построение полноценной системы цифрового суверенитета не означает полного отказа от международного сотрудничества и участия в глобальных процессах. Наоборот, устойчивое развитие в цифровой сфере требует нахождения оптимального баланса между внутренней автономией и включенностью в международную кооперацию. Такая сбалансированная модель предполагает активное участие в разработке и согласовании международных технических стандартов, правовых механизмов и протоколов взаимодействия, что способствует формированию единого пространства доверия и укреплению глобальной устойчивости к киберугрозам. Очевидно, что в условиях цифровой взаимозависимости невозможно эффективно обеспечить национальную безопасность исключительно за счет внутренних ресурсов, особенно с учетом трансграничного характера большинства киберинцидентов. Поэтому принципиально важным направлением остается развитие партнерств с дружественными государствами, а также расширение участия в международных организациях, разрабатывающих механизмы регулирования и практики информационной безопасности.

Показательным примером таких усилий служит деятельность в рамках Международного союза электросвязи (МСЭ), где реализуется Глобальная программа кибербезопасности, призванная обеспечить институциональные и методологические основания для укрепления доверия между государствами и формирования международной нормативной базы информационной безопасности. Эта инициатива ориентирована на выработку стратегических решений, способных не только противостоять вызовам киберугроз, но и создавать условия для справедливого и безопасного развития цифровой экономики. Участие в подобных международных инициативах открывает доступ к лучшим практикам, научно-техническому опыту и позволяет субъектам цифрового взаимодействия выступать активными участниками формирования глобальной повестки, тем самым продвигая национальные интересы в трансграничной цифровой среде.

Однако реализация концепции цифрового суверенитета и обеспечение технологической самостоятельности сталкиваются с рядом вызовов. Среди них можно выделить:

1. Технологическую зависимость от зарубежных решений. Многие ключевые компоненты цифровой инфраструктуры — от микроэлектроники до программного обеспечения — до сих пор импортируются, что создает риски для национальной безопасности.

2. Нехватку квалифицированных кадров. Подготовка специалистов в области информационных технологий и кибербезопасности требует времени и ресурсов, в то время как потребность в таких специалистах постоянно растет.

3. Быстрое развитие технологий. Цифровые технологии развиваются экспоненциально, что требует постоянного обновления нормативной базы, технических средств защиты и подходов к обеспечению безопасности.

4. Глобальный характер киберугроз. Киберпреступность и кибершпионаж не знают границ, что требует международного сотрудничества даже в условиях геополитической напряженности.

Преодоление этих вызовов требует системного подхода и координации усилий государства, бизнеса, научного сообщества и гражданского общества. Необходимо разрабатывать долгосрочные стратегии развития цифровой инфраструктуры и обеспечения кибербезопасности, инвестировать в научные исследования и разработки, стимулировать развитие отечественных технологий и решений.

В заключение следует отметить, что цифровая инфраструктура и кибербезопасность действительно являются ключевыми элементами стратегической технологической самостоятельности. В условиях глобальной цифровизации и растущих киберугроз способность государства обеспечивать безопасное функционирование своей цифровой инфраструктуры становится критическим фактором национальной безопасности и суверенитета. Развитие собственных технологических решений, формирование эффективной системы кибербезопасности, подготовка квалифицированных кадров и совершенствование нормативно-правовой базы — все эти меры в комплексе обеспечивают основу для технологической самостоятельности государства в цифровой сфере.

Таким образом, обеспечение стратегической технологической самостоятельности в цифровой сфере должно стать одним из приоритетов государственной политики. Только при системном подходе к развитию цифровой инфраструктуры и обеспечению кибербезопасности можно гарантировать суверенитет государства в условиях глобальной цифровой трансформации и эффективно противостоять современным угрозам и вызовам в киберпространстве.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Интеграционный «план ГОЭЛРО» для XXI века. Цифровой суверенитет — самостоятельность государства в управлении цифровой трансформацией. URL: https://globalaffairs.ru/articles/czifrovoj-suverenitet-eaes

2. Касперский. Что такое кибербезопасность? URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security

3. РСМД: Практика цифрового суверенитета в России и КНР. URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr

4. Кибербезопасность критически важной инфраструктуры: новые вызовы. URL: https://globalaffairs.ru/articles/kiberbezopasnost-novye-vyzovy

5. Cybercrime Module 8: International Cooperation on Cybersecurity Matters. URL: https://sherloc.unodc.org/cld/ru/education/tertiary/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

6. Цифровой суверенитет: как российские вузы обеспечивают кибербезопасность. URL: https://minobrnauki.gov.ru/press-center/news/novosti-podvedomstvennykh-uchrezhdeniy/54877/

7. Как обеспечить цифровой суверенитет IT-продуктов. URL: https://teamly.ru/blog/cifrovoj-suverenitet-it-produktov