УДК 004.056

Попов Александр Алексеевич
независимый исследователь

Кибербезопасность как стратегический фактор успеха цифровой трансформации общества и государства

Аннотация. В статье рассматривается кибербезопасность как стратегический фактор успешной цифровой трансформации общества и государства. Демонстрируется, что развитие цифровых сервисов, электронного государственного управления, платформенных решений и систем обработки данных повышает зависимость общественных процессов от защищенности цифровой среды. Особое внимание уделено основным угрозам цифровизации, среди которых выделяются утечки персональных данных, кибермошенничество, атаки на информационную инфраструктуру, использование искусственного интеллекта злоумышленниками, технологическая зависимость и недостаточный уровень цифровой грамотности пользователей. Обосновывается, что кибербезопасность должна рассматриваться не как вспомогательное техническое направление, а как элемент национальной безопасности, цифрового суверенитета и устойчивого государственного развития. Сделан вывод о необходимости комплексного подхода к защите цифровой среды, включающего развитие отечественных технологий, совершенствование правового регулирования, повышение цифровой грамотности граждан и внедрение системного управления киберрисками.

Ключевые слова: кибербезопасность; цифровая трансформация; цифровизация; информационная безопасность; киберугрозы; цифровая инфраструктура; цифровой суверенитет; государственное управление; персональные данные; цифровая грамотность.

Popov Alexander Alexeyevich
Independent Researcher

Cybersecurity as a strategic success factor for the digital transformation of society and the state

Abstract. This article examines cybersecurity as a strategic factor in the successful digital transformation of society and the state. It demonstrates that the development of digital services, e-government, platform solutions, and data processing systems increases the dependence of social processes on the security of the digital environment. Particular attention is paid to the main threats to digitalization, including personal data leaks, cyberfraud, attacks on information infrastructure, the use of artificial intelligence by criminals, technological dependence, and insufficient digital literacy of users. It is argued that cybersecurity should not be viewed as an auxiliary technical area, but as an element of national security, digital sovereignty, and sustainable state development. It concludes that a comprehensive approach to protecting the digital environment is necessary, including the development of domestic technologies, improved legal regulation, increased digital literacy of citizens, and the implementation of systemic cyber risk management.

Keywords: cybersecurity; digital transformation; digitalization; information security; cyber threats; digital infrastructure; digital sovereignty; public administration; personal data; digital literacy.

Кибербезопасность в условиях цифровой трансформации становится одним из ключевых условий устойчивого развития общества и государства. Цифровые технологии затрагивают государственное управление, экономику, образование, здравоохранение, финансовые сервисы и повседневные коммуникации граждан. С активным развитием

электронных услуг, платформенных решений и системы обработки данных повышается зависимость общества от защищенности цифровой среды.

Актуальность темы связана с тем, что цифровизация предоставляет государству и гражданам новые возможности, но одновременно формирует новые риски. Утечки персональных данных, кибермошенничество, атаки на информационные системы, вмешательство в работу критической инфраструктуры и распространение вредоносного программного обеспечения могут затрагивать не только отдельные организации, но и целые сферы общественной жизни. По этой причине кибербезопасность уже нельзя рассматривать только как техническое направление. Она превращается в стратегический фактор доверия, стабильности и эффективности цифрового развития.

Особую значимость тема приобретает для государства. Современные государственные сервисы все чаще работают в электронной форме, а взаимодействие граждан с органами власти становится более быстрым и удобным. Однако удобство цифровых решений сохраняет ценность только тогда, когда пользователь уверен в защите своих данных, прозрачности процессов и устойчивости цифровой инфраструктуры. Нарушение кибербезопасности способно снизить устойчивость цифровых сервисов, осложнить взаимодействие граждан с государственными платформами и замедлить внедрение новых технологий.

Научная новизна статьи состоит в уточнении роли кибербезопасности как комплексного стратегического фактора цифровой трансформации, объединяющего технологический, правовой, социальный и управленческий аспекты защиты цифровой среды.

Целью статьи является определение роли кибербезопасности в обеспечении устойчивой цифровой трансформации общества и государства.

Кибербезопасность в цифровой трансформации выступает не вспомогательным техническим элементом, а базовым условием нормального развития цифрового общества. Цифровизация меняет экономику, государственное управление, образование, социальные услуги и повседневное общение граждан. П.В. Ивлиев и С.В. Архипов прямо отмечают: «Цифровизация стала одной из главных стратегических целей» [2, с. 16]. Поэтому вопрос защиты цифровой среды сразу выходит на уровень государственной политики.

Главная особенность цифровой трансформации состоит в том, что почти каждый общественный процесс начинает зависеть от данных. Государственные услуги работают через электронные платформы, финансовые операции проходят через онлайн-сервисы, образование использует цифровые кабинеты и базы данных, а гражданин оставляет цифровой след почти при каждом взаимодействии с системой. В таких условиях уязвимость данных становится уязвимостью всего механизма управления. Если сервис удобен, но не защищен, его эффективность оказывается неполной.

С.В. Лебедь подчеркивает прямую связь между цифровым развитием и защитой информационной системы. Автор пишет, что цифровая трансформация любой организации должна включать вопросы кибербезопасности [3, с. 385]. Данный тезис применим и к государству в целом. Цифровая трансформация без кибербезопасности похожа на строительство сложной инфраструктуры без системы контроля доступа, резервирования и защиты от сбоев. Формально система может работать, но доверять ей становится рискованно.

На уровне общества кибербезопасность связана не только с серверами, программным обеспечением и сетями. Она затрагивает цифровую личность. В этом пространстве человек одновременно становится пользователем цифровых услуг, участником онлайн-коммуникаций, субъектом сетевой идентичности и объектом информационного воздействия. Значит, кибербезопасность защищает не только инфраструктуру, но и личные границы гражданина.

Для государства кибербезопасность имеет еще более широкий смысл. Электронное правительство, платформы государственных услуг, ведомственные базы данных, цифровой

документооборот и критическая информационная инфраструктура требуют устойчивости. Нарушение работы таких систем способно привести к задержке услуг, утечке сведений, сбоям в управлении и снижению доверия к цифровым реформам. Поэтому защита информации становится частью национальной безопасности, а не только задачей ИТ-специалистов.

Отдельное значение имеет технологическая независимость. В условиях санкционного давления и ухода зарубежных поставщиков программного обеспечения зависимость от внешних решений превращается в риск. Государство не может полноценно управлять цифровой средой, если ключевые элементы этой среды зависят от недоступных, закрытых или потенциально уязвимых технологий.

Кибербезопасность не сводится к запретам и ограничениям. Ее стратегическая роль состоит в создании условий, при которых цифровые сервисы развиваются быстрее, безопаснее и вызывают больше доверия у пользователей.

Показательно, что развитие цифровых технологий одновременно усиливает потребность в постоянном обновлении защитных механизмов. П.В. Ивлиев и С.В. Архипов отмечают, что с развитием цифровых технологий «возрастает и угроза кибератак» [2, с. 17]. Это означает, что кибербезопасность не может быть разовой мерой. Она должна сопровождать весь жизненный цикл цифровой трансформации, от проектирования сервисов до их эксплуатации и модернизации.

Развитие государственных и общественных сервисов делает цифровую среду более удобной, но одновременно расширяет пространство для атак. Электронные услуги, онлайн-банкинг, цифровые образовательные платформы, медицинские информационные системы и сервисы взаимодействия граждан с органами власти работают с большими массивами данных. Поэтому киберугроза здесь затрагивает не только отдельный сайт или приложение. Под удар попадают персональные данные, устойчивость управления, финансовые операции и доверие пользователей к цифровым реформам.

Наиболее очевидный риск связан с утечками информации. В государственных и общественных сервисах хранятся паспортные данные, сведения о регистрации, налогах, социальных выплатах, медицинских услугах и образовательных траекториях. Потеря таких данных опасна тем, что они могут использоваться для мошенничества, оформления кредитов, шантажа, подмены личности и доступа к другим сервисам. К.А. Стабровская и С.М. Кузьменко прямо указывают: «Утечка данных представляет собой угрозу высокой степени» [7, с. 189]. Для цифрового государства такая угроза особенно чувствительна, поскольку гражданин часто не может полностью отказаться от пользования государственными платформами.

Второй крупный блок угроз связан с атаками на инфраструктуру. Государственные порталы, ведомственные базы данных, системы электронного документооборота, платежные шлюзы и объекты критической информационной инфраструктуры требуют непрерывной работы. Даже кратковременный сбой способен вызвать цепную реакцию. Задерживаются услуги, нарушается обмен данными между ведомствами, растет нагрузка на офлайн-каналы обслуживания. А.Ю. Олимпиев и И.А. Стрельникова подчеркивают: «Уязвимость Российской Федерации в информационном пространстве очевидна» [5, с. 104]. Эта мысль показывает, что риски цифровой среды имеют не частный, а системный характер.

Особое место занимает кибермошенничество. Его опасность заключается в сочетании технических и психологических методов. Злоумышленнику уже не всегда нужно взламывать сложную систему. Часто достаточно убедить пользователя самостоятельно передать код, пароль или доступ к аккаунту. Здесь особое внимание необходимо обратить на поведение человека. Т.А. Бороненко, А.В. Кайсина и В.С. Федотова отмечают неготовность человека к безопасному и продуктивному формату взаимодействия [1, с. 48]. В условиях массового перехода услуг в онлайн такая неготовность быстро превращается в практический риск.

Новые угрозы усиливаются из-за применения искусственного интеллекта. Автоматизация позволяет быстрее подбирать пароли, создавать фишинговые сообщения, имитировать голос, генерировать поддельные документы и подстраивать атаки под конкретного пользователя. Фальшивое сообщение уже может выглядеть как официальное уведомление, а поддельный звонок может имитировать стиль реального ведомства или банка.

Отдельным источником риска выступает криминализация сети. Даркнет, закрытые форумы, нелегальные маркетплейсы и каналы обмена персональными данными создают среду, где украденная информация быстро превращается в товар. Г.Р. Ташева справедливо отмечает: «Многие преступники для достижения своих криминальных целей прочно обосновались в сети» [8, с. 489]. Это важно учитывать при оценке цифровых сервисов. Утечка сама по себе уже опасна, но еще опаснее вторичный оборот данных, когда сведения многократно перепродаются и используются в новых схемах.

Правовой риск также нельзя исключать. Цифровая среда меняется быстрее, чем успевают обновляться нормы, процедуры и механизмы ответственности. Для государства это создает сложность в регулировании новых форм киберпреступности, трансграничных атак, обработки больших данных и использования искусственного интеллекта. Т.А. Полякова, А.В. Минбалеев и В.Б. Наумов подчеркивают: «Правовое регулирование всегда носит запаздывающий характер» [6, с. 195]. Из-за этого защита цифровой среды не может строиться только на законах. Ей нужны технические, организационные и образовательные меры.

Значимой проблемой остается технологическая зависимость. Если сервисы, средства защиты или программные компоненты зависят от внешних поставщиков, возникают риски обновлений, отключения поддержки, скрытых уязвимостей и невозможности полного контроля над инфраструктурой. П.А. Магомедова, Д.Б. Гасанова и З.Н. Ашурбекова связывают факторы цифровой уязвимости с технологической зависимостью и санкционным давлением [4, с. 303]. Для государства это вопрос не только удобства закупок, но и цифрового суверенитета.

В результате основные угрозы цифровой среды можно свести к нескольким связанным направлениям:

1. Первое направление связано с утечками и незаконным оборотом данных.
2. Второе касается атак на инфраструктуру и нарушение доступности сервисов.
3. Третье выражается в мошенничестве и манипулировании пользователем.
4. Четвертое связано с применением искусственного интеллекта для автоматизации атак.
5. Пятое проявляется в отставании правового регулирования и технологической зависимости.

Все эти риски показывают, что кибербезопасность должна быть встроена в цифровые сервисы заранее, а не добавляться после возникновения инцидентов.

Устойчивое цифровое развитие требует не разовых мер защиты, а постоянной системы управления рисками. Кибербезопасность должна закладываться уже на этапе проектирования сервисов, а не добавляться после утечек, сбоев или атак. Такой подход меняет саму логику цифровизации. На первый план выходят защищенная архитектура, проверенные программные решения, резервирование данных, контроль доступа, мониторинг инцидентов и обучение пользователей. Без этих элементов цифровая среда остается удобной, но хрупкой.

Для государства особое значение имеет цифровой суверенитет. Речь идет не только о наличии отечественного программного обеспечения, но и о способности самостоятельно контролировать критически важные цифровые процессы. П.А. Магомедова, Д.Б. Гасанова и З.Н. Ашурбекова отмечают, что кибербезопасность, являясь важнейшим элементом национальной безопасности и технологического суверенитета страны, становится актуальной частью государственной политики России [4, с. 303]. В таком понимании

защита цифровой среды становится условием самостоятельности государства в технологической сфере.

Практическое значение этого вывода видно на примере критической информационной инфраструктуры. Энергетика, транспорт, связь, финансовая система, здравоохранение и государственные реестры не могут зависеть от случайной устойчивости программ и сетей. Для этих сфер кибератака способна вызвать не только информационный ущерб, но и реальные социальные последствия. Сбой в медицинской системе задерживает помощь. Атака на финансовый сервис нарушает платежи. Компрометация государственного реестра ставит под сомнение достоверность данных. Поэтому кибербезопасность становится частью нормального функционирования базовых общественных институтов.

Не менее важна связь кибербезопасности с доверием граждан. Цифровые услуги развиваются быстрее, когда пользователь понимает правила работы платформы, видит прозрачность процедур и получает гарантии защищенности доступа к сервисам. Т.А. Бороненко, А.В. Кайсина и В.С. Федотова пишут, что цифровой профиль гражданина позволяет «в один клик» получать государственные, финансовые и другие услуги, требующие достоверных персональных данных [1, с. 51]. Но такая модель работает только при высоком уровне защиты. Чем больше сведений объединяется в цифровом профиле, тем выше вероятность утечки или незаконного доступа.

Кибербезопасность также влияет на экономическую устойчивость. Нестабильность цифровых каналов увеличивает издержки бизнеса и государства, повышает расходы на восстановление систем и снижает доверие к онлайн-сервисам. Защищенная цифровая среда делает внедрение электронного документооборота, аналитических платформ и дистанционных услуг более предсказуемым.

В перспективе кибербезопасность будет все теснее связана с искусственным интеллектом, большими данными, биометрией, облачными платформами и межведомственным обменом информацией. Чем сложнее цифровая среда, тем выше значение превентивной защиты. Простая реакция на уже произошедший инцидент становится недостаточной. Нужны прогнозирование угроз, анализ поведения систем, автоматическое выявление аномалий и регулярная оценка уязвимостей.

Полученные выводы позволяют рассматривать кибербезопасность в качестве центрального звена в системе цифровой трансформации. Она связана с защитой персональных данных, стабильностью государственных сервисов, технологической независимостью и общей управляемостью цифровых процессов. Без надежной защиты цифровизация превращается в источник дополнительных рисков, поскольку рост числа сервисов одновременно увеличивает количество уязвимых точек. Анализ угроз цифровой среды позволил выделить наиболее значимые проблемы. К ним относятся утечки данных, кибермошенничество, атаки на инфраструктуру, использование искусственного интеллекта злоумышленниками, криминализация сетевого пространства и технологическая зависимость. Особенно важным оказался вывод о том, что значимым фактором цифровой безопасности является поведение пользователя, поскольку недостаток цифровой грамотности повышает вероятность мошенничества, утечек данных и несанкционированного доступа. Стратегическое значение кибербезопасности выражается в ее связи с устойчивым развитием государства. Защищенная цифровая среда снижает экономические потери, укрепляет цифровой суверенитет и позволяет развивать электронные сервисы без постоянной угрозы сбоев и утечек. Практическая ценность темы состоит в том, что выводы статьи могут применяться при оценке государственных цифровых платформ, развитии образовательных программ по цифровой грамотности и совершенствовании подходов к защите информационной инфраструктуры.

Список источников

1. Бороненко Т.А., Кайсина А.В., Федотова В.С. Цифровая грамотность цифровой личности: к вопросу об уточнении понятий // Инновационные проекты и программы в образовании. 2020. № 4 (70). С. 47-56.
2. Ивлиев П.В., Архипов С.В. Роль государства в содействии цифровизации // Право и государство: теория и практика. 2024. № 11 (239). С. 16-18.
3. Лебедь С.В. Инновационные технологии в сфере кибербезопасности // Современные информационные технологии и ИТ-образование. 2022. №2. С. 383-390.
4. Магомедова П.А., Гасанова Д.Б., Ашурбекова З.Н. Цифровая уязвимость и актуальные тенденции повышения информационной безопасности экономики России // РППЭ. 2026. №3 (185). С. 303-311.
5. Олимпиев А.Ю., Стрельникова И.А. Кибербезопасность и ее обеспечение в Российской Федерации // Уголовная юстиция. 2021. №17. С. 104-109.
6. Полякова Т.А., Минбалеев А.В., Наумов В.Б. Форсайт-сессия «информационная безопасность в XXI веке: вызовы и правовое регулирование» // Труды Института государства и права РАН. 2018. №5. С. 194-208.
7. Стабровская К.А., Кузьменко С.М. Киберугроза и кибербезопасность // Региональная и отраслевая экономика. 2025. №5. С. 189-194.
8. Ташева Г.Р. Кибербезопасность: вызовы и решения // Право и управление. 2023. №11. С. 489-492.

Сведения об авторе

Попов Александр Алексеевич, независимый исследователь, Москва, Россия

Information about the authors

Popov Alexander Alexeyevich, Independent Researcher, Moscow, Russia