УДК 004.81:32:363.3

Анализ роли политических институтов в формировании стратегий кибербезопасности и защиты критически важной инфраструктуры

Зевелёва Елена Александровна

Кандидат исторических наук, профессор,
заведующая кафедрой гуманитарных наук,
Академик РАЕН, член Союза писателей России,
Российский государственный геологоразведочный
университет им. Серго Орджоникидзе
117997, Российская Федерация, Москва, ул. Миклухо-Маклая, 23;
e-mail: zevelevaea@mgri.ru

Кокунов Константин Андреевич

Кандидат педагогических наук, доцент,
доцент кафедры гуманитарных наук;
Российский государственный геологоразведочный
университет им. Серго Орджоникидзе
117997, Российская Федерация, Москва, ул. Миклухо-Маклая, 23;
e-mail: kokunovka@mgri.ru

Аннотация

Настоящая статья посвящена анализу роли политических институтов в формировании стратегий кибербезопасности и защите критически важной инфраструктуры. Во введении авторы обосновывают актуальность выбранной темы в условиях стремительного развития информационных технологий и возрастающей цифровизации стратегически значимых секторов экономики. Указывается, что современные вызовы в области информационной безопасности требуют не только технических, но и институциональных решений, что обуславливает необходимость изучения влияния политических механизмов на общую систему защиты. Методологическая база исследования опирается на сочетание количественного и качественного анализа. Авторы проводят сравнительный анализ национальных и международных нормативно-правовых документов, регулирующих вопросы кибербезопасности, а также исследуют опыт различных стран в области выработки политических стратегий по защите критически важной инфраструктуры. Кроме того, метод включает анализ интервью с экспертами в данной области, что позволяет получить более глубокое понимание особенностей институционального взаимодействия и многогранности проблематики. Такой мультидисциплинарный подход обеспечивает всестороннее рассмотрение исследуемой проблемы. Результаты исследования демонстрируют, что эффективность мер кибербезопасности во многом определяется степенью развитости политических институтов, способных оперативно реагировать на новые вызовы. Анализ выявил ключевые факторы, способствующие формированию

сбалансированной стратегии защиты, а также указал на проблемные области, связанные с недостаточной координацией между государственными органами и медленным обновлением законодательства. Выявлены примеры успешного институционального взаимодействия, способствующего быстрому внедрению инновационных мер в сфере кибербезопасности. В заключительной части статьи обсуждаются перспективы развития интегрированных стратегий безопасности, подчеркивается необходимость дальнейших исследований в контексте международного сотрудничества и обмена опытом. Авторы приходят к выводу, что совершенствование политических институтов является важным компонентом формирования надежной системы защиты критически важной инфраструктуры в условиях современной цифровой экономики.

Для цитирования в научных исследованиях

Зевелёва Е.А., Кокунов К.А. Анализ роли политических институтов в формировании стратегий кибербезопасности и защиты критически важной инфраструктуры // Теории и проблемы политических исследований. 2025. Том 14. № 4А. С. 47-56.

Ключевые слова

Анализ, политические институты, стратегии, кибербезопасность, критическая инфраструктура.

Введение

Политические институты играют ключевую роль в формировании стратегий кибербезопасности, поскольку именно они определяют приоритеты, распределяют ресурсы и регулируют взаимодействие между государственными и негосударственными субъектами. От слаженной работы таких институтов зачастую зависит, какой именно подход будет принят для защиты критически важной инфраструктуры, и насколько эффективно будут реализованы соответствующие программы. В современном мире, где кибератаки становятся все более изощренными, а их последствия приобретают глобальный характер, важность сильной политической системы сложно переоценить. Вопросы законодательства, политической воли и межгосударственного сотрудничества оказываются в фокусе внимания, когда речь заходит о выстраивании комплексной обороны от цифровых угроз [Ловцов, Бурый, 2024]. Существует мнение, что государственная политика в киберсфере должна основываться не только на текущих угрозах, но и на прогнозировании будущих опасностей. Подобный подход помогает избежать фрагментарных решений и создает благоприятные условия для стратегического планирования. К тому же политические институты, благодаря своему влиянию на международной арене, способны выстраивать диалог между странами для координации действий в сфере кибербезопасности.

Сложность управления кибербезопасностью объясняется не только технологической спецификой, но и тем, что угрозы могут исходить из самых разных источников. Это могут быть как враждебно настроенные государства, так и транснациональные группировки, стремящиеся к экономической выгоде или политическому влиянию, а также отдельные хакеры, организованные коллективы и даже внутренние информаторы [Братковская, Рогова, Токарева, 2023]. Политические институты, наделенные правом принимать законы и устанавливать правовые рамки, пытаются регулировать эту сферу, однако часто сталкиваются с правовыми

пробелами, недостаточной осведомленностью и неполным пониманием технологических деталей. При этом регулярные заседания парламентских комиссий и профильных комитетов позволяют более оперативно реагировать на появляющиеся угрозы, привлекать экспертов из индустрии к подготовке различных законопроектов, а также создавать рабочие группы, которые занимаются мониторингом угроз. Нередки случаи, когда в процессе разработки стратегий кибербезопасности учитываются не только внутренние, но и международные стандарты. Например, рекомендации, сформированные на уровне крупных международных организаций, оказывают существенное влияние на политику национальных государств.

Важность межведомственной координации обусловлена тем, что современная критически важная инфраструктура задействует различные отрасли: энергетику, транспорт, здравоохранение, финансовый сектор, телекоммуникации и другие сферы. Нарушение или парализация работы в любой из этих областей, вызванная кибератакой, способна привести к колоссальным потерям. Политические институты стремятся обеспечить согласованность мер по обеспечению кибербезопасности и создать единую платформу, на которой разные ведомства могли бы обмениваться информацией и совместно вырабатывать тактику защиты. Одним из инструментов является разработка национальных стратегий кибербезопасности, в которых прописываются обязанности конкретных государственных органов и обозначаются приоритеты в сфере распределения ресурсов. Такие стратегии могут включать образовательные программы, проведение учений и тестирование систем на уязвимости. Нередко правительства создают специализированные центры, отвечающие за сбор и анализ данных о текущих инцидентах, прогнозирование угроз и организацию быстрого реагирования.

При этом уровень политической воли зачастую определяет успешность реализации мер по киберзащите. Если высшее руководство страны осознает важность вопроса и оказывает активную поддержку соответствующим программам, то бюрократические барьеры могут быть преодолены значительно быстрее. В противном случае, даже наличие хорошо прописанных законодательных актов и технически совершенных решений не гарантирует, что в нужный момент они будут реально применены. Также необходимо учитывать, что кибербезопасность тесно связана с вопросами конфиденциальности и защиты прав человека. Политические институты должны стремиться к балансу между обеспечением национальной безопасности и сохранением гражданских свобод. Это порождает сложные дискуссии, ведь любое укрепление контроля в сфере информационных технологий вызывает опасения насчет возможности неправомерного использования собранных данных. Тем не менее, эффективная политика в киберпространстве должна учитывать широкий спектр интересов и рисков.

Материалы и методы исследования

Стратегия защиты критически важной инфраструктуры предполагает комплекс мер, направленных как на предотвращение кибератак, так и на минимизацию последствий, если атака уже произошла. Политические институты в данном случае играют роль координатора, устанавливающего минмальные стандарты безопасности и ответственные лица в каждом секторе [Бочарова, 2024]. В идеале государство не только определяет эти стандарты, но и стимулирует инновации, вкладывая средства в развитие отечественных технологий киберзащиты. Наличие собственных технологических решений снижает зависимость от поставок из-за рубежа и обеспечивает больший контроль над критическими системами. При этом стандарты безопасности должны регулярно пересматриваться, так как методики взлома

постоянно эволюционируют, а злоумышленники изобретают все новые инструменты для проникновения в системы. Кроме того, необходимы механизмы обмена информацией между государством и частным сектором, поскольку многие объекты критически важной инфраструктуры находятся в руках частных компаний.

Сложность формулирования политики в сфере кибербезопасности во многом зависит от того, что само понятие «кибербезопасность» весьма многогранно. Это не только защита сетей и баз данных, но и информационная война, борьба с дезинформацией и фальшивыми новостями, а также выстраивание системы доверия между различными субъектами. Политические институты вынуждены реагировать на все эти вызовы одновременно. При этом важную роль играет медийная повестка и общественное мнение. Если общество не поддерживает инициативы власти или если СМИ формируют негативное отношение к тем или иным мерам, принятие и реализация законодательных актов может быть осложнена. В особенности это касается тех случаев, когда государство стремится ужесточить контроль над информационным пространством, обосновывая свои действия необходимостью киберзащиты.

Глобальная природа Интернет-пространства требует развития международных институтов, которые могли бы выступать арбитрами в конфликтных ситуациях и разрабатывать общие стандарты поведения. Политические институты национального уровня, разрабатывая стратегии кибербезопасности, все чаще ориентируются на международные соглашения и двусторонние договоры. Сотрудничество в этой сфере крайне важно, ведь кибератаки нередко проникают за государственные границы, и ответные меры должны быть согласованы. Однако согласованность не всегда достижима, поскольку страны придерживаются разных политических целей, а также имеют разное представление о доступности и свободе информации. Кроме того, различные типы кибератак — будь то промышленный шпионаж, вмешательство в избирательные процессы или атаки на финансовые системы — требуют специфических форм реагирования. Этот спектр задач еще больше затрудняет согласование позиций на международной арене.

Национальные парламенты, совмещая законодательную и контрольную функции, имеют возможность детально рассматривать проекты нормативных актов в сфере кибербезопасности и регулярно проверять их эффективность [Маслова, 2023]. Создание специальных комитетов — один из способов обеспечить постоянное внимание к этой проблематике. При этом парламентарии часто привлекают к работе экспертов из числа технологических специалистов, представителей силовых структур и бизнеса. Подобная практика помогает сглаживать информационный разрыв, так как многие депутаты не обладают глубокой технической экспертизой. В результате появляются законы, более точно отражающие реальность, а механизм их реализации становится понятнее для исполнительной власти и для самих операторов важных инфраструктурных объектов. Однако слишком долгое обсуждение и бюрократизация также могут нанести вред, поскольку киберугрозы эволюционируют стремительно, и устаревшее законодательство может фактически блокировать оперативные действия.

Исполнительные органы, в свою очередь, ответственны за превращение принятых политических решений в реальные действия. Часто создаются профильные агентства, которые получают мандат на координацию сотрудничающих ведомств, контроль над соблюдением правил безопасности и проведение регулярных учений. Чтобы повысить эффективность подобных структур, политические институты нередко расширяют их полномочия и финансирование. Они могут формировать механизмы быстрого реагирования, способные локализовать последствия атаки и минимизировать ущерб. В целях вовлечения бизнеса иногда

внедряются государственно-частные партнерства, которые базируются на взаимном обмене информацией о киберуязвимостях. В идеале такие партнерства создают синергию и помогают шире распространять стандарты безопасности по всей отрасли или даже по нескольким отраслям.

Для успешной борьбы с киберпреступностью важна слаженная работа правоохранительных органов, которая также регулируется политическими институтами. Органы полиции и безопасности учатся взаимодействовать с провайдерами интернет-услуг, финансовыми организациями и крупными технологическими компаниями, чтобы оперативно выявлять и пресекать преступную деятельность в сети. Однако для этого зачастую требуются специальные процессуальные нормы, позволяющие собирать и использовать цифровые доказательства в суде. Если законодательство не поспевает за технологическими изменениями, правоохранителям приходится работать в серой зоне правоприменения или добиваться от судов прецедентных решений. Политические институты, осознавая эту проблему, пытаются адаптировать процессуальные кодексы и смежные нормативные акты, чтобы максимально упростить и ускорить процедуру расследования киберпреступлений.

Проблема подготовки кадров в сфере кибербезопасности также находится в ведении политических институтов. Государство стимулирует образовательные программы в университетах, а также организует курсы повышения квалификации для госслужащих и специалистов частных компаний. Без постоянного притока новых профессионалов и без совершенствования уже имеющихся навыков невозможно поддерживать высокий уровень готовности к отражению атак [Низамова, 2023]. Однако в некоторых странах ощущается дефицит квалифицированных экспертов, и это приводит к перегреву рынка труда, где частный сектор готов предлагать более высокие зарплаты, переманивая специалистов из государственных структур. Политические институты пытаются решить данную проблему за счет доплат, льгот и улучшения социального пакета, однако конкуренция с крупными корпорациями остается весьма острой.

Еще одна сфера, в которой политические институты играют важнейшую роль, — это формирование правовых основ для разработки, эксплуатации и импорта кибероружия. Кибероружие может использоваться как для наступательных, так и для оборонительных целей, и разграничить эти две категории не всегда просто [Цахилова, 2023]. Поэтому вопросам контроля над соответствующими технологиями уделяется все больше внимания. С одной стороны, государство должно иметь инструменты для защиты своих систем и сдерживания потенциального противника. С другой стороны, слишком широкие полномочия могут привести к эскалации и гонке вооружений в киберпространстве. Политические институты вынуждены искать компромисс, устанавливая правовую базу, которая учитывает международные обязательства и национальные интересы.

Важным моментом является и взаимодействие с общественными организациями и институтами гражданского общества, которые могут критически оценивать законодательные инициативы в сфере кибербезопасности. Иногда такие организации занимают позицию независимого эксперта, высказываясь за необходимость более строгого контроля над использованием конфиденциальных данных или за сохранение свободы слова в Интернете [Корепанов, Левандовский, 2023]. Политические институты не всегда склонны учитывать подобные взгляды в полном объеме, опасаясь, что чрезмерная открытость создаст уязвимости. Однако диалог с гражданским обществом способствует формированию более взвешенных решений, которые, с одной стороны, не будут чрезмерно ограничивать права и свободы, а с другой — обеспечат необходимый уровень защиты важных инфраструктур.

Результаты и обсуждение

В условиях глобального информационного пространства все более очевидной становится необходимость унификации некоторых аспектов киберзаконодательства разных стран. Международные конвенции и соглашения пытаются создать единый свод правил, содержащий определение киберпреступлений, порядок взаимодействия правоохранительных органов и форматы обмена информацией между государствами. Политические институты, отвечающие за ратификацию подобных документов, оказываются в центре дискуссии о том, насколько национальное законодательство совместимо с международными нормами. Иногда сложности возникают из-за расхождений в правовых традициях и особенностях политических режимов. Тем не менее многие страны все активнее участвуют в глобальных инициативах, поскольку понимают, что без международного сотрудничества удержать контроль над ситуацией в киберпространстве крайне сложно.

Политическое лидерство в сфере технологий — еще один фактор, влияющий на развитие стратегий кибербезопасности. Государство, которое находится на передовом рубеже технологических инноваций, способно не только лучше защищаться, но и формировать определенную позицию на мировой арене. Для этого нужны инвестиции в науку, образование, исследовательские центры и стартапы, занимающиеся вопросами информационной безопасности. Политические институты определяют приоритеты финансирования и стимулируют рост высокотехнологичных отраслей, понимая, что кибербезопасность — это не просто издержки, а фундамент для цифровой экономики. В результате формируется своего рода «экосистема безопасности», в которую входят университеты, научные лаборатории и профильные ведомства, объединенные общей целью повысить устойчивость государства к кибератакам.

Немалое значение имеет и концепция «цифрового суверенитета», предполагающая, что государство должно контролировать ключевые инфраструктурные объекты и обладать определенной автономией при формировании цифровой политики [Ловцов, Бурый, 2024]. Политические институты, разделяющие такую концепцию, могут пытаться устанавливать ограничение на использование иностранных решений в критических системах, чтобы снизить риски вмешательства извне. Иногда подобные меры приводят к сложностям в отношениях с другими странами и транснациональными корпорациями, ведь их рынок сбыта сокращается, да и совместное использование технологий усложняется. Однако сторонники цифрового суверенитета указывают на необходимость таких шагов для обеспечения национальной безопасности, особенно в условиях растущих международных противоречий.

Стимулирование научных исследований также неразрывно связано с деятельностью политических институтов. Государство может предоставлять гранты для развития перспективных направлений и создавать инкубаторы инноваций в области безопасности. При этом взаимодействие науки и практики выходит на первый план: результаты исследований должны эффективно внедряться в правительственные программы и частный сектор. Существует риск, что при отсутствии надлежащего интереса со стороны руководства проекты в области кибербезопасности останутся на периферии внимания и будут недофинансированы. В результате страны, не вкладывающие ресурсы в научное развитие, могут стать более уязвимыми к цифровым угрозам.

Роль политических институтов ярко проявляется и в том, как формируется публичная риторика, связанная с кибербезопасностью. Государственные лидеры могут использовать опасность кибератак в качестве аргумента для расширения полномочий спецслужб, мотивируя

это необходимостью защитить граждан и критически важные объекты. Это, в свою очередь, вызывает опасения, что борьба с киберугрозами может быть использована в политических целях и привести к ущемлению гражданских прав. В такой ситуации крайне важен парламентский и общественный контроль за действиями исполнительной ветви власти. Механизмы отчетности и прозрачности позволяют убедиться, что ресурсы, выделенные на кибербезопасность, тратятся эффективно и не направляются на преследование политических оппонентов или иные злоупотребления.

Системный подход, которого требуют современные вызовы, подразумевает, что политические институты должны координировать целый комплекс мероприятий: от образовательных инициатив и правовых реформ до международного сотрудничества и внедрения инноваций в государственном секторе. Фактор непрерывной модернизации методов защиты становится крайне важен, ведь киберугрозы, с которыми мы имеем дело сегодня, через год могут устареть, а на их смену придут новые, еще более опасные [Дунмэй Ло, 2023]. В этом смысле фундаментальной задачей институтов власти является сохранение баланса между долгосрочными стратегиями и гибким реагированием на текущие вызовы. Если пренебречь хотя бы одним из этих компонентов, общая эффективность киберзащиты может оказаться заметно ниже.

Особое внимание уделяется повышению осведомленности населения о киберугрозах, ведь значительная часть атак опирается на социальную инженерию — методы обмана и психологического влияния, которые эксплуатируют человеческий фактор. Политические институты способствуют внедрению курсов цифровой гигиены в школы и университеты, а также запускают другие просветительские проекты [Исрафилов, 2024]. Цель подобных инициатив — сформировать культуру безопасного поведения в сети и снизить риск того, что пользователи по незнанию станут «слабым звеном» в защите систем. Этот аспект особенно важен сейчас, когда все больше социальных, экономических и административных услуг переносится в онлайн-пространство, и любая утечка данных может привести к серьезным последствиям.

Значимым инструментом в руках политических институтов остается дипломатия. Двусторонние и многосторонние договоренности по кибербезопасности помогают формализовать правила поведения в глобальном цифровом пространстве и устанавливать определенные «красные линии» [Маргамов, 2023]. Например, некоторые соглашения стремятся запретить нападения на гражданскую инфраструктуру, подобно тому, как существуют нормы в международном гуманитарном праве относительно защиты гражданских объектов в ходе обычных вооруженных конфликтов. Однако в отличие от традиционных театров военных действий, где нормы разрабатывались десятилетиями, в киберпространстве подобные процессы только набирают обороты. Любое крупное происшествие, связанное с разрушительной кибератакой, может стать катализатором для принятия новых договоренностей и стимулировать политические институты быстрее совершенствовать механизмы защиты.

Заключение

Политические институты также могут играть роль посредника между технологическими гигантами и гражданами, устанавливая нормы и правила игры на цифровом рынке. Компании, разрабатывающие аппаратное и программное обеспечение, обладают огромным влиянием на степень безопасности пользователей, ведь от их решений зависит, будут ли устранены уязвимости или нет [Лю, 2023]. Законодатели могут создавать стимулы, побуждающие

корпорации выпускать регулярные обновления безопасности, более прозрачно раскрывать информацию об обнаруженных брешах и активно сотрудничать с правительством при расследованиях киберпреступлений. Хотя некоторые фирмы могут сопротивляться этим требованиям, ссылаясь на коммерческую тайну и необходимость защиты интеллектуальной собственности, политические институты вправе требовать приоритета общественных интересов над корпоративной выгодой, особенно когда речь идет о критической инфраструктуре.

Адекватная правовая среда — необходимое условие, чтобы государственные органы и частные компании могли эффективно бороться с угрозами. Политические институты анализируют мировой опыт, изучают прецеденты и пытаются адаптировать лучшие практики к национальным реалиям. Иногда это происходит путем прямого заимствования положений из законодательства ведущих стран, имеющих большой опыт в сфере кибербезопасности [Маслова, 2023]. Однако слепое копирование может и не принести нужных результатов, ведь каждая страна имеет собственную институциональную специфику, политическую культуру и уровень технологического развития. Поэтому ключ к успеху — это именно адаптация, которая учитывает локальные особенности, но при этом сохраняет дух и логику современных подходов к защите критически важных объектов.

В долгосрочной перспективе способность политических институтов предвидеть новые риски и системно реагировать на них будет играть решающую роль в глобальном технологическом противостоянии. Ключевой вызов состоит в том, чтобы успевать обновлять законодательство, образовательные программы и технические решения. Без надлежащего менеджмента, который обеспечивает непрерывность реформ и контроль за результатами, любые начинания рискуют остаться лишь на бумаге [Дунмэй Ло, 2023]. Многие государства выделяют серьезные финансовые средства на киберзащиту, но без стабильных и прозрачных политических институтов, способных исключать коррупцию и неэффективное использование ресурсов, эти вливания не дадут должного эффекта.

Таким образом, роль политических институтов в формировании стратегий кибербезопасности и защите критически важной инфраструктуры огромна. Они определяют законодательную базу, контролируют работающие механизмы, создают условия для научного развития и международного сотрудничества, а также выстраивают диалог с гражданским обществом [Цахилова, 2023]. Данные аспекты вместе формируют основу для успешного противостояния постоянно эволюционирующим угрозам, которые сталкивают государства и корпорации с колоссальными рисками в цифровом пространстве. В конечном итоге только системная, всесторонняя и гибкая политика, основанная на активном участии разных институтов, способна дать адекватный ответ на вызовы современного кибермира.

Библиография

1. Бочарова А.П. Политики информационной и кибербезопасности (классификация мер, акторов и проблема оценки эффективности) // Мировая экономика и международные отношения. 2024. Т. 68. № 4. С. 121–130. 10 с.
2. Братковская Д.В., Рогова Я.Д., Токарева С.А. Особенности кибербезопасности КНР // Вопросы национальных и федеративных отношений. 2023. Т. 13. № 5 (98). С. 2321–2325. 5 с.
3. Дунмэй Ло. Политика администрации Джо Байдена в области кибербезопасности // Вопросы политологии. 2023. Т. 13. № 1 (89). С. 323–330. 8 с.
4. Исрафилов А. Кибербезопасность в государственных структурах: стратегии защиты от кибератак // Дневник науки. 2024. № 5 (89). С. [указать страницы]. [указать количество страниц].
5. Колокольчиков В.К. Разработка стратегии кибербезопасности предприятия // Поиск (Волгоград). 2023. № 3 (16). С. 176–180. 5 с.
6. Корепанов Б.О., Левандовский Н.В. Новая стратегия кибербезопасности США // Зарубежное военное обозрение.

2023. № 8. С. 8–11. 4 с.
7. Ловцов Д.А., Бурый А.С. Кибербезопасность: основные тенденции в обеспечении // Правовая информатика. 2024. № 2. С. 23–34. 12 с.
8. Лю В. Кибербезопасность и международные отношения // Научный аспект. 2023. Т. 11. № 10. С. 1339–1346. 8 с.
9. Маргамов А.Р. Направления развития системы кибербезопасности российского государства // Экономика и бизнес: теория и практика. 2023. № 8 (102). С. 119–121. 3 с.
10. Маслова Л.Р. Киберпреступность как угроза национальной безопасности // Право и государство: теория и практика. 2023. № 3. С. 193–195. 3 с.
11. Низамова М.А. Киберугрозы в контексте политики Японии в сфере кибербезопасности в начале XXI в. // Международные отношения и общество. 2023. Т. 5. № 3. С. 77–87. 11 с.
12. Пальчиков И.А., Ярмонова А.Г. Кибербезопасность как главный фактор национальной и международной безопасности в XXI веке // Инновации, технологии и бизнес. 2022. № 1 (11). С. 41–44. 4 с.
13. Рамазанов Р.Ф. Кибербезопасность: современные угрозы и стратегии защиты // Научный аспект. 2024. Т. 43. № 6. С. 5422–5425. 4 с.
14. Серёдкин С.П. Особенности кибератак на объекты критической информационной инфраструктуры в современных условиях // Информационные технологии и математическое моделирование в управлении сложными системами. 2022. № 4 (16). С. 56–66. 11 с.
15. Цахилова Л.М. Стратегии кибербезопасности в НАТО и Европейском союзе // Информационные войны. 2023. № 2 (66). С. 65–72. 8 с.

The Role of Political Institutions in Shaping Cybersecurity Strategies and Critical Infrastructure Protection

Elena A. Zeveleva

PhD in History, Professor,
Head of the Department of Humanities,
Academician of RAEEN, Member of the Russian Writers' Union,
Sergey Ordzhonikidze Russian State University for Geological Prospecting,
117997, 23, Miklukho-Maklaya str., Moscow, Russian Federation;
e-mail: zevelevaea@mgri.ru

Konstantin A. Kokunov

PhD in Pedagogical Sciences, Associate Professor,
Department of Humanities,
Sergey Ordzhonikidze Russian State University for Geological Prospecting,
117997, 23, Miklukho-Maklaya str., Moscow, Russian Federation;
e-mail: kokunovka@mgri.ru

Abstract

This article examines the role of political institutions in shaping cybersecurity strategies and protecting critical infrastructure. The introduction justifies the relevance of the topic given the rapid development of information technologies and increasing digitalization of strategically important economic sectors. The authors emphasize that modern information security challenges require not only technical but also institutional solutions, necessitating an analysis of how political mechanisms influence overall protection systems. The methodological framework combines quantitative and qualitative approaches, including comparative analysis of national and international legal documents regulating cybersecurity, as well as case studies of political strategies for critical infrastructure

protection across different countries. Expert interviews provide deeper insights into institutional cooperation dynamics and multifaceted challenges. Results demonstrate that cybersecurity effectiveness largely depends on political institutions' capacity to respond to emerging threats. The study identifies key factors enabling balanced protection strategies while highlighting problematic areas like interagency coordination gaps and slow legislative updates. Successful examples of institutional cooperation facilitating rapid adoption of innovative cybersecurity measures are analyzed. The conclusion discusses prospects for integrated security strategies, stressing the need for further research on international cooperation and knowledge exchange. The authors conclude that strengthening political institutions is essential for developing reliable critical infrastructure protection systems in today's digital economy.

For citation

Zeveleva E.A., Kokunov K.A. (2025) Analiz roli politicheskikh institutov v formirovanii strategiy kiberbezopasnosti i zashchity kriticheski vazhnoy infrastruktury [The Role of Political Institutions in Shaping Cybersecurity Strategies and Critical Infrastructure Protection]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 14 (4A), pp. 47-56.

Keywords

Analysis, political institutions, strategies, cybersecurity, critical infrastructure.

References

1. Bocharova A.P. Information and Cybersecurity Policies (classification of measures, actors, and the problem of evaluating effectiveness) // World Economy and International Relations. 2024. Vol. 68. No. 4. pp. 121–130. 10 pages.
2. Bratkovskaya D.V., Rogova Ya.D., Tokareva S.A. Peculiarities of Cybersecurity in the PRC // Issues of National and Federal Relations. 2023. Vol. 13. No. 5 (98). pp. 2321–2325. 5 pages.
3. Dunmey Lo. The Biden Administration's Cybersecurity Policy // Issues in Political Science. 2023. Vol. 13. No. 1 (89). pp. 323–330. 8 pages.
4. Israfilov A. Cybersecurity in Government Structures: Strategies for Protection against Cyberattacks // Science Diary. 2024. No. 5 (89). pp. [specify pages]. [specify number of pages].
5. Kolokolchikov V.K. Developing an Enterprise Cybersecurity Strategy // Poisk (Volgograd). 2023. No. 3 (16). pp. 176–180. 5 pages.
6. Korepanov B.O., Levandovsky N.V. A New Cybersecurity Strategy in the USA // Foreign Military Review. 2023. No. 8. pp. 8–11. 4 pages.
7. Lovtsov D.A., Bury A.S. Cybersecurity: Main Trends in Provision // Legal Informatics. 2024. No. 2. pp. 23–34. 12 pages.
8. Ly V. Cybersecurity and International Relations // Scientific Aspect. 2023. Vol. 11. No. 10. pp. 1339–1346. 8 pages.
9. Margamov A.R. Directions for the Development of the Russian State's Cybersecurity System // Economics and Business: Theory and Practice. 2023. No. 8 (102). pp. 119–121. 3 pages.
10. Maslova L.R. Cybercrime as a Threat to National Security // Law and State: Theory and Practice. 2023. No. 3. pp. 193–195. 3 pages.
11. Nizamova M.A. Cyber Threats in the Context of Japan's Cybersecurity Policy at the Beginning of the 21st Century // International Relations and Society. 2023. Vol. 5. No. 3. pp. 77–87. 11 pages.
12. Pal'chikov I.A., Yarmonova A.G. Cybersecurity as the Main Factor of National and International Security in the 21st Century // Innovations, Technologies, and Business. 2022. No. 1 (11). pp. 41–44. 4 pages.
13. Ramazanov R.F. Cybersecurity: Modern Threats and Protection Strategies // Scientific Aspect. 2024. Vol. 43. No. 6. pp. 5422–5425. 4 pages.
14. Seryodkin S.P. Peculiarities of Cyberattacks on Critical Information Infrastructure Facilities under Modern Conditions // Information Technologies and Mathematical Modeling in the Management of Complex Systems. 2022. No. 4 (16). pp. 56–66. 11 pages.
15. Tsakhilova L.M. Cybersecurity Strategies in NATO and the European Union // Information Wars. 2023. No. 2 (66). pp. 65–72. 8 pages.