ISSN k181-9505
Doi Journal 10.k6739/k181-9505

Philosophy and Life

FALSAFA VA HAYOT • ФИЛОСОФИЯ И ЖИЗНЬ

2026 №1 (32)

ISSN k181-9505
Doi Journal 10.k6739/k181-9505

Mirzo Ulug'bek nomidagi O'zbekiston Milliy Universiteti

O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi
Imom Buxoriy xalqaro ilmiy-tadqiqot markazi
O‘zbekiston falsafa jamiyati

Национальный Yниверситет Ys6екистана имени Мирso Yлуг6ека

Мewдународный науино-исследовательский центр Имам Бухари
при Ка6инете Министров Республики Ys6екистан
Философское общество Ys6екистана

The National University of Uzbekistan named after Mirzo Ulugbek

Imam Bukhari International Research Center under the Cabinet of Ministers
of the Republic of Uzbekistan
Philosophical Society of Uzbekistan

FALSAFA VA HAYOT
XALQARO JURNAL

ФИЛОСОФИЯ И ХИЗНЬ
МЕХДУНАРОДНЫЙ ХУРНАЛ

PHILOSOPHY AND LIFE
INTERNATIONAL JOURNAL

2026 №1 (32)

Jurnal bir yilda 4 marta nashr qilinadi.
Хурнал выходит 4 раза в год.
The journal is published 4 times in a year.

Toshkent

СОДЕРЖАНИЕ

ФИЛОСОФИЯ ПОЛИТИКИ И ОБЩЕСТВА

ФИЛОСОФИЯ ОБРАЗОВАНИЯ И НАУК

ИСТОРИЯ ФИЛОСОФИИ И ФИЛОСОФИЯ ИСТОРИИ

МИРОВАЯ КУЛЬТУРА И РЕЛИГИОЗНЫЕ ТРАДИЦИИ

УДК: 004.056:323
10.5281/zenodo.20181814

Усмонов Саидикромхужа Саидалиевич
доктор философии PhD, доцент
Национальный университет Узбекистана
имени Мирзо Улугбека
(Ташкент, Узбекистан)
saidikromxojausmonov@gmal.com

КИБЕРБЕЗОПАСНОСТЬ КАК ФАКТОР ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОГО СУВЕРЕНИТЕТА В ЭПОХУ ГЛОБАЛИЗАЦИИ

Аннотация. В условиях стремительного развития цифровых технологий и углубления глобализационных процессов кибербезопасность приобретает ключевое значение как важнейший фактор обеспечения национального суверенитета, поскольку государственные институты, экономика и социальная сфера становятся все более зависимыми от устойчивости информационных систем. Актуальность данной темы обусловлена возрастанием масштабов киберугроз, транснациональным характером цифровых атак и необходимостью защиты критической информационной инфраструктуры в условиях глобальной взаимосвязанности. Вместе с тем, усиление контроля в сфере кибербезопасности может сопровождаться ограничением цифровых свобод, ростом государственного надзора и рисками нарушения конфиденциальности персональных данных. В связи с этим в данной статье раскрываются теоретико-методологические основы кибербезопасности как элемента национального суверенитета, анализируются современные угрозы и предлагаются эффективные механизмы их нейтрализации.

Ключевые слова: кибербезопасность суверенитет, глобализация, цифровизация, киберугрозы, риски, информационная безопасность, защита данных, государственная политика, регулирование, цифровое пространство, контроль.

ВВЕДЕНИЕ

В современную эпоху глобализации, характеризующуюся стремительным развитием информационно-коммуникационных технологий, формируется качественно новая реальность, в которой цифровое

пространство становится неотъемлемой частью функционирования государства, общества и личности. Расширение масштабов цифровизации приводит к трансформации традиционных представлений о суверенитете, дополняя его новым измерением киберпространством, где пересекаются интересы государств, транснациональных корпораций и негосударственных акторов. В этих условиях обеспечение кибербезопасности становится одним из ключевых приоритетов государственной политики. Национальный суверенитет в цифровую эпоху уже не ограничивается территориальными границами и военной мощью, а включает в себя способность государства эффективно защищать свои информационные ресурсы, критическую инфраструктуру и цифровые системы управления. Возрастающая зависимость экономики, политики и социальной сферы от цифровых технологий усиливает уязвимость перед киберугрозами, которые могут иметь как внутреннее, так и внешнее происхождение. В результате киберпространство становится ареной геополитического соперничества и инструментом давления на государственный суверенитет. Особую значимость приобретает тот факт, что киберугрозы носят транснациональный и асимметричный характер, что существенно усложняет процессы их выявления и нейтрализации. Кибератаки способны нарушать функционирование государственных институтов, дестабилизировать экономические процессы, влиять на общественное сознание и подрывать доверие к власти. При этом развитие технологий, включая искусственный интеллект, большие данные и облачные вычисления, одновременно расширяет возможности защиты и создает новые риски, требующие комплексного и системного подхода. В этих условиях возникает объективная необходимость в теоретическом осмыслении роли кибербезопасности как фактора обеспечения национального суверенитета, а также в разработке эффективных стратегий противодействия современным угрозам. Настоящее исследование направлено на анализ сущности и содержания кибербезопасности в контексте глобализационных процессов, выявление ключевых вызовов цифровой эпохи и обоснование механизмов укрепления национального суверенитета в условиях цифровой трансформации общества.

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ

Методологическая основа исследования базируется на междисциплинарном подходе, объединяющем политологический, правовой и информационно-технологический анализ, что позволяет рассматривать кибербезопасность не только как техническую категорию, но и как фактор обеспечения национального суверенитета. В частности, в работе используется концептуальный анализ понятий «кибербезопасность» и «цифровой суверенитет», опирающийся на позицию узбекского исследователя Б. М. Носирова, который трактует кибербезопасность как систему мер по защите информационных ресурсов и инфраструктуры от кибератак [Носиров, 2023, с. 1]. Данное определение подчеркивает

институциональный характер кибербезопасности и ее роль в обеспечении устойчивости государства, что особенно значимо в условиях цифровизации современного общества. Значение данной идеи заключается в том, что она формирует основу для понимания кибербезопасности как элемента государственной политики, а не только технической сферы. Существенное методологическое значение имеет сравнительный анализ зарубежных и региональных исследований, в частности работ казахстанских ученых С. С. Саятбека и К. Ч. Байсултановой, которые рассматривают киберпространство как ключевую сферу глобальной безопасности и подчеркивают отсутствие универсальных международно-правовых механизмов регулирования [Саятбек, Байсултанова, 2025, с. 2]. Их подход раскрывает проблему фрагментарности международного регулирования и сложности атрибуции кибератак, что позволяет глубже понять уязвимость национального суверенитета в условиях глобальной сети. В современном мире данная идея приобретает особую значимость, поскольку подчеркивает необходимость международного сотрудничества при одновременном сохранении национальных интересов.

В качестве эмпирической базы используются исследования ученых стран Центральной Азии, в частности казахстанских авторов С. Р. Мубараковой, С. Т. Аманжоловой и Р. К. Ускенбаевой, которые акцентируют внимание на росте киберугроз и их влиянии на социально-экономические процессы [Мубаракова и др., 2021, с. 3]. Данный подход позволяет рассматривать кибербезопасность как фактор устойчивого развития государства. Одновременно в работах узбекских исследователей, таких как Ф. У. Хамдамова, подчеркивается, что цифровизация порождает новые формы угроз — кибертерроризм, киберпреступность и кибервойны [Хамдамова, 2024, с. 2], что свидетельствует о двойственной природе технологического прогресса. Значение этих идей в современном контексте заключается в необходимости формирования гибких стратегий безопасности, способных учитывать быстро меняющуюся цифровую среду. Особое внимание уделяется анализу правовых и политических аспектов кибербезопасности на основе работ российских исследователей, в частности А. В. Яковлевой, которая рассматривает правовое регулирование киберпространства как ключевой инструмент обеспечения безопасности государства [Яковлева, 2021, с. 70]. Данный подход показывает, что киберсуверенитет невозможен без развитой нормативно-правовой базы и эффективных механизмов государственного контроля. В свою очередь, узбекский исследователь У. Шукуриллаев подчеркивает связь кибербезопасности с информационной политикой и управлением общественным сознанием [Шукуриллаев, 2024, с. 546], что расширяет понимание данного феномена до уровня идеологического воздействия. Зарубежные и региональные исследователи сходятся в признании кибербезопасности ключевым фактором национального суверенитета, однако различаются в акцентах: западные авторы (например, D. Craigen и соавт.)

сосредотачиваются на технологических аспектах и моделировании угроз, тогда как ученые Центральной Азии и России уделяют больше внимания политико-правовым и социальным аспектам. Такой синтез подходов позволяет сформировать комплексное понимание кибербезопасности как многоуровневого явления, включающего технологические, правовые и идеологические компоненты. В результате применяемая методология обеспечивает целостный анализ проблемы и позволяет выявить эффективные механизмы укрепления национального суверенитета в условиях глобализации. Выбор методов исследования обусловлен сложной, многоуровневой природой кибербезопасности как феномена, находящегося на пересечении технологий, политики и права. В этой связи в работе применяется системный метод, позволяющий рассматривать кибербезопасность как целостную структуру, включающую институциональные, технологические и социальные элементы. Данный подход опирается на идеи узбекского исследователя Пахруддинова Ш. И., который подчеркивает необходимость анализа общественно-политических процессов в их взаимосвязи и динамике [Пахруддинов, 2020, с. 45], что позволяет выявить внутренние механизмы функционирования киберпространства и его влияние на суверенитет государства. Значение этого метода в современном мире заключается в возможности комплексной оценки угроз, выходящих за рамки исключительно технических параметров.

Не менее важным является сравнительный метод, применяемый для сопоставления различных национальных моделей обеспечения кибербезопасности. Использование данного метода обосновано тем, что киберугрозы носят глобальный характер, однако стратегии их нейтрализации формируются в рамках конкретных государств. В этом контексте позиция казахстанских исследователей С. С. Саятбека и К. Ч. Байсултановой о фрагментарности международного регулирования [Саятбек, Байсултанова, 2025, с. 2] демонстрирует необходимость сопоставительного анализа для выявления эффективных практик. В современном мире данный метод приобретает особую значимость, поскольку позволяет заимствовать успешный опыт и адаптировать его к национальным условиям. Применение институционального метода обусловлено необходимостью анализа роли государственных структур и правовых механизмов в обеспечении кибербезопасности. Как отмечает российский исследователь А. В. Яковлева, именно правовое регулирование формирует основу устойчивости киберпространства и определяет границы допустимого поведения субъектов [Яковлева, 2021, с. 70]. Это мнение подчеркивает, что без институциональной поддержки даже самые современные технологические решения оказываются недостаточно эффективными. В современных условиях значение данного метода заключается в выявлении оптимального баланса между безопасностью и сохранением гражданских свобод. Кроме того, в исследовании используется контент-анализ, направленный на изучение стратегических документов, нормативно-правовых актов и научных

публикаций. Обоснование данного метода связано с необходимостью выявления доминирующих подходов и дискурсов в области кибербезопасности. Узбекский ученый Ахтам Жалилов отмечает, что анализ политико-идеологических текстов позволяет выявить скрытые механизмы формирования общественного сознания и государственной политики [Жалилов, 2022, с. 88]. Значимость данного метода в современном мире определяется тем, что киберпространство становится не только технической, но и информационно-идеологической средой. Совокупность применяемых методов системного, сравнительного, институционального и контент-анализа обеспечивает комплексное исследование кибербезопасности как фактора национального суверенитета. Их сочетание позволяет не только глубже понять природу современных угроз, но и обосновать эффективные механизмы их предотвращения в условиях глобализации.

ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ

В условиях становления цифровой цивилизации категория национального суверенитета претерпевает существенную трансформацию, выходя за пределы традиционного понимания, основанного на территориальной целостности и политической независимости. Современный суверенитет все в большей степени определяется способностью государства контролировать и защищать собственное информационно-коммуникационное пространство, включая критическую цифровую инфраструктуру, государственные информационные системы и каналы передачи данных. В этой связи кибербезопасность выступает не просто вспомогательным элементом, а структурообразующим компонентом суверенитета, обеспечивающим его устойчивость в условиях глобальной взаимосвязанности. Как отмечает Пахруддинов Ш. И., суверенитет в цифровую эпоху приобретает качественно новое содержание, включающее контроль над информационными потоками и защиту национальных интересов в киберпространстве [Пахруддинов, 2020, с. 52]. Данная позиция подчеркивает, что утрата контроля в цифровой сфере фактически равнозначна ослаблению государственной независимости. Научное обоснование данного положения находит отражение и в работах российских исследователей, где акцент делается на правовых механизмах обеспечения киберсуверенитета. Так, А. В. Яковлева утверждает, что наличие эффективной нормативно-правовой базы и механизмов регулирования цифрового пространства является необходимым условием защиты национальных интересов [Яковлева, 2021, с. 75]. Это означает, что кибербезопасность выполняет институциональную функцию, формируя рамки допустимого поведения субъектов в сети и предотвращая деструктивное вмешательство извне. В сравнении с узбекским подходом, ориентированным на политико-идеологический аспект, российская научная традиция делает акцент на юридической формализации суверенитета, что в совокупности раскрывает многомерную природу данного феномена. Особую

значимость кибербезопасность приобретает в контексте защиты критической инфраструктуры, включающей энергетические системы, транспортные сети, банковский сектор и государственные информационные ресурсы. Казахстанские исследователи отмечают, что нарушение функционирования таких систем в результате кибератак может привести к масштабным социально-экономическим последствиям и подрыву государственной стабильности [Саятбек, Байсултанова, 2025, с. 4]. В этом контексте кибербезопасность выступает гарантом непрерывности функционирования государства, а значит — одним из ключевых факторов его суверенитета. Аналогичные выводы содержатся в зарубежных исследованиях, где подчеркивается, что современные конфликты все чаще смещаются в киберпространство, приобретая форму кибервойн и информационного противоборства [Craigen, 2014, с. 19]. Практическое подтверждение данной теоретической позиции можно наблюдать на примере ряда государств, столкнувшихся с масштабными кибератаками. Так, атака на государственные информационные системы Эстонии в 2007 году продемонстрировала, что даже высокоразвитые цифровые государства могут оказаться уязвимыми перед внешними угрозами, что привело к временной дестабилизации работы государственных институтов и финансовой системы. Аналогично, кибератаки на энергетическую инфраструктуру Украины показали, что вмешательство в цифровые системы управления может привести к реальным последствиям в физическом мире, включая отключение электроэнергии и нарушение жизнедеятельности населения. Эти примеры подтверждают тезис о том, что киберпространство становится новой ареной реализации государственной власти и одновременно полем угроз национальному суверенитету. Важным аспектом является также идеологическое измерение кибербезопасности, связанное с управлением информационными потоками и формированием общественного сознания. Узбекский исследователь Ахтам Жалилов подчеркивает, что киберпространство становится инструментом идеологического воздействия, способным влиять на политические процессы и общественное мнение [Жалилов, 2022, с. 93]. В этом контексте кибербезопасность выполняет функцию защиты не только инфраструктуры, но и информационного суверенитета, предотвращая манипуляцию сознанием и распространение деструктивных идеологий. В сравнении с западными концепциями, где акцент делается на защите данных и приватности, в странах Центральной Азии большее внимание уделяется вопросам информационной устойчивости и идеологической безопасности.

Кибербезопасность как структурный элемент национального суверенитета представляет собой многомерное явление, включающее технологические, правовые и идеологические компоненты. Ее значение в современном мире определяется не только способностью предотвращать кибератаки, но и обеспечивать устойчивое функционирование государства, защиту общественного сознания и сохранение политической независимости в условиях глобализации. Проведённый анализ и приведённые примеры

свидетельствуют о том, что без эффективной системы кибербезопасности реализация национального суверенитета в цифровую эпоху становится невозможной. В условиях углубляющейся глобализации киберпространство становится единым, взаимосвязанным и практически не имеющим территориальных границ пространством, в котором традиционные механизмы государственного контроля существенно ограничены. Это приводит к формированию нового типа угроз, которые приобретают транснациональный характер и могут исходить одновременно из разных регионов мира, затрагивая критически важные сферы жизнедеятельности государства. Как отмечают казахстанские исследователи С. С. Саятбек и К. Ч. Байсултанова, современная киберсреда характеризуется высокой степенью взаимозависимости государств, при которой локальные инциденты могут быстро приобретать глобальные последствия [Саятбек, Байсултанова, 2025, с. 3]. Данное положение подчеркивает, что киберугрозы перестают быть исключительно внутренней проблемой государства и превращаются в элемент международной безопасности. Сравнительный анализ показывает, что зарубежные исследователи, в частности D. Craigen, рассматривают киберугрозы преимущественно через призму технологической уязвимости сетевых систем и инфраструктур [Craigen, 2014, с. 16], тогда как ученые постсоветского пространства уделяют больше внимания политико-правовым последствиям этих угроз. Такая разница в подходах объясняется различием исследовательских традиций: западная наука ориентирована на инженерно-техническое моделирование рисков, тогда как региональные исследования акцентируют внимание на государственном суверенитете и безопасности. В результате формируется необходимость синтеза этих подходов для более полного понимания природы киберугроз. Особую роль в усилении транснационального характера киберугроз играет развитие цифровой экономики и расширение использования облачных технологий, искусственного интеллекта и больших данных. Эти процессы, с одной стороны, повышают эффективность государственного управления и бизнеса, а с другой создают новые уязвимости, связанные с утечкой данных и несанкционированным доступом к информационным системам. Российская исследовательница А. В. Яковлева подчеркивает, что цифровая взаимосвязанность усиливает эффект «цепной реакции» кибератак, при котором нарушение одного элемента системы может привести к масштабным сбоям [Яковлева, 2021, с. 77]. Это свидетельствует о том, что современные угрозы имеют системный характер и требуют комплексных мер реагирования. Примеры практической реализации транснациональных киберугроз можно наблюдать в ряде глобальных инцидентов. Так, распространение вредоносного программного обеспечения WannaCry в 2017 году затронуло более 150 стран, парализовав работу медицинских учреждений, государственных органов и частных компаний. Аналогично, кибератаки на финансовые системы ряда государств показали, что даже локальное вмешательство в цифровую инфраструктуру может привести к

международным экономическим последствиям. Эти случаи подтверждают, что киберугрозы приобретают характер глобальных кризисов, выходящих за рамки национальных границ. Важным аспектом является также то, что транснациональный характер киберугроз затрудняет установление их источника и применение традиционных механизмов международной ответственности. Узбекский исследователь Ахтам Жалилов отмечает, что анонимность цифровой среды и отсутствие единых международных норм создают условия для безнаказанного использования киберпространства в деструктивных целях [Жалилов, 2022, с. 95]. В этом контексте возникает необходимость формирования новых форм международного сотрудничества и правового регулирования, способных учитывать специфику цифровой среды.

Глобализация не только усиливает взаимосвязанность государств, но и радикально трансформирует природу угроз, делая их транснациональными, асимметричными и трудно идентифицируемыми. Это требует перехода от традиционных моделей национальной безопасности к комплексным международным стратегиям киберзащиты, основанным на сотрудничестве, обмене информацией и унификации правовых норм. Развитие цифрового общества закономерно привело к необходимости институционального закрепления кибербезопасности как одного из ключевых направлений государственной политики. В современных условиях именно государственные институты формируют нормативно-правовую основу, определяющую правила функционирования киберпространства, распределение ответственности и механизмы реагирования на угрозы. Российская исследовательница А. В. Яковлева отмечает, что правовое регулирование в сфере кибербезопасности выступает системообразующим элементом защиты национальных интересов, поскольку именно закон определяет границы допустимого поведения в цифровой среде [Яковлева, 2021, с. 80]. Это положение позволяет утверждать, что без институциональной базы кибербезопасность не может быть устойчивой и эффективной. В странах Центральной Азии институциональный подход к кибербезопасности находится на стадии активного формирования. Узбекский исследователь Пахруддинов Ш. И. подчеркивает, что эффективность государственной политики в цифровой сфере напрямую зависит от степени координации между различными органами власти и наличия единой стратегической концепции [Пахруддинов, 2020, с. 55]. В отличие от этого, в Российской Федерации и Казахстане наблюдается более развитая система нормативного регулирования, включающая специализированные законы, национальные стратегии и центры реагирования на киберинциденты. Такое различие свидетельствует о неоднородности институционального развития в регионе и необходимости унификации подходов.

Особое значение в обеспечении кибербезопасности имеет взаимодействие государственных и частных структур, поскольку значительная часть цифровой инфраструктуры принадлежит

негосударственным субъектам. Кыргызский исследователь А. Т. Касымалиев отмечает, что эффективная система киберзащиты невозможна без партнерства государства, бизнеса и научного сообщества, что формирует модель «совместной ответственности» [Касымалиев, 2021, с. 60]. В западной научной традиции аналогичный подход рассматривается как модель multi-stakeholder governance, где регулирование осуществляется на основе взаимодействия различных акторов. Сравнение этих подходов показывает, что несмотря на различия в терминологии, общая логика развития институциональных механизмов является схожей. Важным направлением институционального обеспечения кибербезопасности является создание национальных центров мониторинга и реагирования на киберугрозы. Практика Казахстана, где функционирует система CERT-KZ, демонстрирует эффективность централизованного подхода к обработке инцидентов и координации действий различных ведомств. Аналогичные структуры существуют в России и ряде стран Европы, что подтверждает универсальность данного института в системе цифровой безопасности. Казахстанские исследователи С. С. Саятбек и К. Ч. Байсултанова подчеркивают, что наличие таких центров значительно повышает устойчивость государства к кибератакам и сокращает время реагирования [Саятбек, Байсултанова, 2025, с. 6]. Отдельное внимание следует уделить правовому аспекту регулирования трансграничных киберугроз, который остается одной из наиболее сложных проблем современного международного права. Узбекский исследователь У. Шукуриллаев отмечает, что отсутствие единого международного правового механизма приводит к фрагментарности регулирования и затрудняет привлечение к ответственности субъектов кибератак [Шукуриллаев, 2024, с. 550]. В то же время зарубежные авторы, такие как J. Nye, указывают на необходимость формирования гибридных моделей управления киберпространством, сочетающих государственное регулирование и международное сотрудничество [Nye, 2017, с. 145]. Сравнение этих подходов показывает, что будущее кибербезопасности связано с развитием многоуровневой правовой архитектуры. Таким образом, институциональные и правовые механизмы выступают фундаментальной основой обеспечения кибербезопасности. Их развитие определяет способность государства не только реагировать на существующие угрозы, но и формировать устойчивую систему предотвращения рисков в цифровой среде. Проведенный анализ показывает, что эффективность кибербезопасности напрямую зависит от степени зрелости правовой системы, уровня межведомственной координации и международного сотрудничества.

Развитие цифровой среды приводит к тому, что киберугрозы начинают оказывать комплексное воздействие не только на государственные институты, но и на социально-экономическую стабильность общества. В современных условиях информационные системы становятся основой функционирования финансового сектора, здравоохранения, образования и

государственного управления, поэтому любые киберинциденты способны вызывать системные сбои. Казахстанские исследователи С. Р. Мубаракова и С. Т. Аманжолова отмечают, что кибератаки приводят к нарушению экономических процессов и снижению уровня доверия населения к государственным институтам [Мубаракова, Аманжолова, 2021, с. 7]. Это положение подчеркивает, что киберугрозы имеют не только технический, но и социальный характер, затрагивая устойчивость общества в целом. Сравнительный анализ научных подходов показывает, что в узбекской исследовательской традиции особое внимание уделяется идеологическому измерению киберугроз. Так, Ахтам Жалилов рассматривает киберпространство как инструмент воздействия на общественное сознание, где информационные технологии могут использоваться для формирования определённых политических установок и ценностей [Жалилов, 2022, с. 98]. В отличие от этого, российские и западные исследователи чаще акцентируют внимание на экономических и технологических последствиях цифровых угроз. Например, J. Nye вводит концепцию «информационной силы», подчеркивая способность информации влиять на поведение государств и обществ в глобальной политике [Nye, 2017, с. 150]. Такое различие подходов демонстрирует многомерность киберугроз, охватывающих как материальную, так и нематериальную сферы. Особую роль в социально-экономическом измерении киберугроз играет цифровая зависимость государств и населения от онлайн-сервисов и платформ. Нарушение работы банковских систем, транспортных сетей или государственных порталов может приводить к прямым экономическим потерям и социальной дестабилизации. Российская исследовательница А. В. Яковлева подчеркивает, что цифровая экономика усиливает уязвимость государства перед киберинцидентами, поскольку высокая степень автоматизации увеличивает масштаб потенциального ущерба [Яковлева, 2021, с. 82]. Это свидетельствует о том, что технологический прогресс одновременно усиливает как возможности развития, так и риски нестабильности. Практические примеры подтверждают данное положение. Так, массовые кибератаки на финансовые учреждения различных стран приводили к временной блокировке банковских операций и утечке персональных данных миллионов пользователей. В социальных сетях и цифровых платформах неоднократно фиксировались случаи распространения дезинформации, направленной на дестабилизацию общественно-политической ситуации. Казахстанские исследователи С. С. Саятбек и К. Ч. Байсултанова отмечают, что такие процессы напрямую влияют на уровень социальной напряженности и могут использоваться в качестве инструмента гибридного воздействия [Саятбек, Байсултанова, 2025, с. 8]. Важным аспектом является также формирование нового типа идеологической уязвимости, связанной с информационной перегрузкой и манипуляцией цифровым контентом. Узбекский исследователь У. Шукуриллаев указывает, что современное информационное пространство характеризуется высокой степенью

конкуренции за внимание пользователей, что создает условия для распространения деструктивных нарративов [Шукуриллаев, 2024, с. 553]. В этом контексте кибербезопасность приобретает значение не только защиты данных, но и сохранения информационной устойчивости общества.

Социально-экономические и идеологические последствия киберугроз свидетельствуют о их системном характере и глубоком влиянии на все сферы общественной жизни. Сравнительный анализ научных подходов показывает, что различные исследовательские школы по-разному акцентируют внимание на этих последствиях, однако сходятся в признании их значимости для национальной безопасности и устойчивого развития государства. Современный этап цифровой трансформации общества формирует качественно новые условия функционирования государства, при которых кибербезопасность становится неотъемлемым элементом стратегического развития. Усложнение информационных систем, внедрение искусственного интеллекта, технологий больших данных и облачных вычислений требует переосмысления традиционных подходов к защите цифрового пространства. Узбекский исследователь Пахруддинов Ш. И. подчеркивает, что устойчивость государства в цифровую эпоху напрямую зависит от уровня развития национальной цифровой инфраструктуры и кадрового потенциала в сфере информационной безопасности [Пахруддинов, 2020, с. 60]. Это положение указывает на необходимость перехода от реактивной модели защиты к проактивной системе предотвращения угроз.

Необходимо отметит, что в зарубежной литературе особое внимание уделяется технологическому развитию кибербезопасности, прежде всего внедрению искусственного интеллекта для автоматического выявления и нейтрализации угроз. Так, J. Nye отмечает, что будущая система безопасности будет основываться на способности государств адаптироваться к быстро меняющимся цифровым условиям и использовать технологические инновации как инструмент стратегического преимущества [Nye, 2017, с. 155]. В отличие от этого, исследователи Центральной Азии и России акцентируют внимание на институциональных и кадровых аспектах, подчеркивая важность государственного регулирования и подготовки специалистов. Особую роль в перспективах развития кибербезопасности играет международное сотрудничество, поскольку транснациональный характер угроз делает невозможным их эффективное преодоление в рамках одного государства. Казахстанские исследователи С. С. Саятбек и К. Ч. Байсултанова указывают, что создание региональных механизмов обмена информацией и координации действий является ключевым условием повышения устойчивости к кибератакам [Саятбек, Байсултанова, 2025, с. 9]. Аналогичные идеи содержатся и в работах российских ученых, которые подчеркивают необходимость формирования глобальной архитектуры кибербезопасности на основе международных соглашений. Важным направлением будущего развития является также усиление роли государственно-частного партнерства, поскольку значительная часть

цифровой инфраструктуры принадлежит частным компаниям. Российская исследовательница А. В. Яковлева отмечает, что без участия бизнеса и научного сообщества невозможно создать устойчивую систему киберзащиты, способную эффективно реагировать на современные вызовы [Яковлева, 2021, с. 85]. В свою очередь, узбекский исследователь У. Шукуриллаев подчеркивает, что развитие информационной политики государства должно сопровождаться формированием культуры цифровой безопасности среди населения [Шукуриллаев, 2024, с. 556]. Практические тенденции последних лет демонстрируют, что государства постепенно переходят к созданию комплексных национальных стратегий кибербезопасности, включающих правовые, технологические и образовательные компоненты. Например, внедрение национальных центров киберзащиты и систем раннего предупреждения позволяет значительно снизить риски масштабных атак. При этом особое значение приобретает подготовка специалистов нового поколения, способных работать в условиях быстро меняющейся цифровой среды. Перспективы развития кибербезопасности связаны с интеграцией технологических инноваций, укреплением международного сотрудничества и формированием устойчивой институциональной базы. Сравнительный анализ показывает, что несмотря на различия в акцентах различных научных школ, общим является признание необходимости комплексного подхода, объединяющего технологии, право и образование в единую систему защиты цифрового суверенитета.

ЗАКЛЮЧЕНИЕ

Проведённое исследование позволяет сделать вывод о том, что кибербезопасность в условиях глобализации приобретает статус одного из ключевых факторов обеспечения национального суверенитета. Современное государство уже не может рассматриваться вне цифрового измерения, поскольку значительная часть его политических, экономических и социальных функций реализуется через информационные системы. В этой связи защита киберпространства становится неотъемлемым элементом устойчивости государственной власти и сохранения её независимости. Анализ показал, что киберугрозы обладают транснациональным, асимметричным и динамичным характером, что существенно осложняет их выявление и нейтрализацию. В условиях глобальной взаимосвязанности даже локальные киберинциденты могут вызывать цепную реакцию и приводить к системным сбоям на международном уровне. Это требует формирования новых подходов к обеспечению безопасности, основанных на международном сотрудничестве, обмене информацией и согласовании правовых норм. Особое значение имеет институциональное и правовое обеспечение кибербезопасности, которое выступает основой формирования цифрового суверенитета государства. Эффективность государственной политики в данной сфере определяется уровнем развития нормативно-правовой базы, координацией между государственными структурами и

участием частного сектора. В то же время важную роль играет и идеологическое измерение, связанное с защитой информационного пространства и общественного сознания от деструктивных воздействий. Сравнительный анализ научных подходов показал, что несмотря на различия в акцентах различных исследовательских школ, существует общая тенденция к признанию кибербезопасности как системного явления, охватывающего технологические, правовые, политические и социальные аспекты. При этом наиболее перспективным направлением является формирование комплексной модели киберзащиты, объединяющей государственные, международные и частные механизмы. Кибербезопасность следует рассматривать не только как инструмент защиты информационных систем, но и как стратегический ресурс национального суверенитета в эпоху цифровой трансформации. Ее дальнейшее развитие будет определять уровень устойчивости государств к глобальным вызовам и способность адаптироваться к стремительно изменяющейся цифровой среде.

БИБЛИОГРАФИЯ

1. Носиров Б. М. (2023) Кибербезопасность: значение, определение и содержательные различия. – Ташкент,
2. Саятбек С. С., Байсултанова К. Ч. (2025) Актуальные проблемы исследования кибербезопасности в современных международных отношениях. – Алматы,
3. Мубаракова С. Р., Аманжолова С. Т., Ускенбаева Р. К. (2021) Relevance of cybersecurity in the modern world. – Алматы,
4. Хамдамова Ф. У. (2024) Цифровые технологии как фактор угроз международной безопасности. – Ташкент,
5. Яковлева А. В. (2021) Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт). – Санкт-Петербург,
6. Шукуриллаев У. (2024) Информационная безопасность и политология: кибербезопасность и управление пропагандой. – Ташкент,
7. Пахруддинов Ш. И. (2020) Политические процессы в условиях глобализации. – Ташкент: Узбекистан, – 120 с.
8. Жалилов А. И. (2022) Идеологические аспекты информационной безопасности. – Ташкент: Фан, – 150 с.
9. Яковлева А. В. (2021) Кибербезопасность и правовое регулирование: зарубежный и российский опыт. – Санкт-Петербург: Наука, – 180 с.
10. Саятбек С. С., Байсултанова К. Ч. (2025) Кибербезопасность в системе международных отношений. – Алматы: Қазақ университеті, – 95 с.
11. Касымалиев А. Т. (2021) Государственная политика в сфере кибербезопасности. – Бишкек: Илим, – 130 с.
12. Craigen D., Diakun-Thibault N., Purse R. (2014) Defining Cybersecurity. – Ottawa: Technology Innovation Management Review, – 25 p.

13. Nye J. (2017) The Future of Power. – New York: PublicAffairs,. – 300 p.
14. Яковлева А. В. Кибербезопасность и правовое регулирование. – СПб.: Наука, 2021. – 180 с.
15. Жалилов А. И. Идеологические аспекты информационной безопасности. – Ташкент: Фан, 2022. – 150 с.
16. Мубаракова С. Р., Аманжолова С. Т. (2021) Проблемы кибербезопасности в современном обществе. – Алматы, – 110 с.

Usmonov Saidikromkhoja Saidaliyevich
Doctor of Philosophy (PhD), Associate Professor
National University of Uzbekistan named after Mirzo Ulugbek
(Tashkent, Uzbekistan)
saidikromxojausmonov@gmal.com

CYBERSECURITY AS A FACTOR OF ENSURING NATIONAL SOVEREIGNTY IN THE ERA OF GLOBALIZATION

Abstract. In the context of the rapid development of digital technologies and the deepening processes of globalization, cybersecurity is gaining key importance as a crucial factor in ensuring national sovereignty, since state institutions, the economy, and the social sphere are increasingly dependent on the stability of information systems. The relevance of this topic is driven by the growing scale of cyber threats, the transnational nature of digital attacks, and the need to protect critical information infrastructure in conditions of global interconnectedness. At the same time, strengthening control in the field of cybersecurity may be accompanied by restrictions on digital freedoms, increased state surveillance, and risks of violating personal data confidentiality. In this regard, the article reveals the theoretical and methodological foundations of cybersecurity as an element of national sovereignty, analyzes modern threats, and proposes effective mechanisms for their neutralization.

Keywords: cybersecurity, sovereignty, globalization, digitalization, cyber threats, risks, information security, data protection, state policy, regulation, digital space, control.

Usmonov Saidikromxo‘ja Saidaliyevich
Falsafa doktori (PhD), dotsent
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti
(Tashkent, O’zbekiston)
saidikromxojausmonov@gmal.com

KIBERXAVFSIZLIK GLOBALIZATSIYA DAVRIDA MILLIY SUVERENITETNI TA’MINLASH OMILI SIFATIDA

Annotatsiya. Raqamli texnologiyalarning jadal rivojlanishi va globallashuv jarayonlarining chuqurlashuvi sharoitida kiberxavfsizlik davlat institutlari,

iqtisodiyot va ijtimoiy sohaning axborot tizimlari barqarorligiga tobora ko‘proq bog‘liq bo‘lib borayotgani sababli milliy suverenitetni ta’minlashning muhim omili sifatida alohida ahamiyat kasb etmoqda. Mazkur mavzuning dolzarbligi kiberxavf-xatarlar ko‘lamining kengayishi, raqamli hujumlarning transmilliy xususiyati hamda global o‘zaro bog‘liqlik sharoitida muhim axborot infratuzilmasini himoya qilish zarurati bilan izohlanadi. Shu bilan birga, kiberxavfsizlik sohasida nazoratni kuchaytirish raqamli erkinliklarning cheklanishi, davlat nazoratining ortishi hamda shaxsiy ma’lumotlar maxfiyligining buzilishi xavfini keltirib chiqarishi mumkin. Shu bois, mazkur maqolada kiberxavfsizlikning milliy suverenitet elementi sifatidagi nazariy-metodologik asoslari ochib beriladi, zamonaviy tahdidlar tahlil qilinadi hamda ularni bartaraf etishning samarali mexanizmlari taklif etiladi.

Kalit so‘zlar: kiberxavfsizlik, suverenitet, globallashuv, raqamlashtirish, kiberxavf-xatarlar, risklar, axborot xavfsizligi, ma’lumotlarni himoya qilish, davlat siyosati, tartibga solish, raqamli makon, nazorat.