# АКТУАЛИЗАЦИЯ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В СОЦИУМЕ И В СОВРЕМЕННОМ МИРЕ

**СОБИРОВ АНВАР**
Ташкентский государственный экономический университет
Независимый соискатель кафедры Философия
E-mail: dilmurodernazarov55@gmail.com
Mobil: +998997700429

**Введение**

В XXI веке информационные технологии стали неотъемлемой частью общественного развития. Глобальная цифровизация экономики, внедрение искусственного интеллекта, развитие облачных технологий и расширение интернет-коммуникаций существенно изменили формы взаимодействия людей, организаций и государств. Современное общество характеризуется высоким уровнем зависимости от информационных систем и цифровой инфраструктуры, что делает проблему кибербезопасности одной из ключевых в системе национальной и международной безопасности.

Развитие информационного общества сопровождается не только расширением возможностей обмена информацией, но и появлением новых угроз в цифровой среде. Кибератаки, утечка конфиденциальных данных, вредоносное программное обеспечение, фишинг и другие формы киберпреступности становятся все более распространенными. По данным международных исследований, ущерб от киберпреступлений ежегодно увеличивается и оказывает значительное влияние на экономику, государственное управление и социальную стабильность (Kshetri, 2021).

Актуализация проблемы кибербезопасности обусловлена несколькими факторами. Во-первых, стремительным ростом цифровых

технологий и расширением киберпространства. Во-вторых, увеличением количества пользователей сети Интернет и цифровых сервисов. В-третьих, трансформацией социальной структуры общества, в которой информационные ресурсы становятся стратегическим фактором развития государств.

В этих условиях вопросы обеспечения кибербезопасности приобретают не только технологическое, но и социально-философское значение. Киберпространство становится новой средой человеческой деятельности, в которой происходят экономические, политические и культурные процессы. Соответственно, обеспечение безопасности в данной среде становится важнейшей задачей современного общества.

Целью данной статьи является анализ актуальности проблемы кибербезопасности в современном обществе, выявление основных факторов роста киберугроз и определение ключевых направлений обеспечения безопасности цифровой среды.

**Анализ литературы**

Проблематика кибербезопасности активно исследуется в различных научных дисциплинах. Современные исследования рассматривают кибербезопасность как сложное междисциплинарное явление, включающее технологические, социальные, политические и экономические аспекты.

Одним из ключевых теоретических подходов к изучению цифрового общества является концепция **сетевого общества**, разработанная М. Кастельсом. Согласно его теории, развитие информационных технологий приводит к формированию новой социальной структуры, основанной на сетевых коммуникациях. В таких условиях информационные ресурсы становятся основным источником власти и влияния (Castells, 2010).

Исследователь Б. Уэллман отмечает, что развитие интернет-коммуникаций приводит к формированию новых форм социальной

организации, основанных на сетевых взаимодействиях. Он подчеркивает, что современный человек все чаще участвует в многочисленных цифровых сетях, что увеличивает значение информационной безопасности (Wellman, 2001).

В работах П. Сингера и А. Фридмана кибербезопасность рассматривается в контексте глобальной политики и международной безопасности. Авторы отмечают, что киберпространство становится новой ареной международных конфликтов, где государства и негосударственные акторы используют цифровые технологии для достижения политических целей (Singer & Friedman, 2014).

Дж. Най в своих исследованиях вводит понятие киберсилы, подчеркивая, что киберпространство становится важным инструментом международной политики и элементом национальной безопасности (Nye, 2017).

Экономический аспект кибербезопасности исследуется в работах Н. Кшетри, который отмечает, что киберпреступность становится одной из наиболее быстро развивающихся форм транснациональной преступности. По его мнению, рост цифровой экономики делает проблему защиты информационных систем особенно актуальной (Kshetri, 2021).

В отечественной научной традиции вопросы информационной и кибербезопасности исследуются в работах В. Н. Лопатина, И. М. Дзялошинского и других ученых. Их исследования подчеркивают важность формирования национальной системы защиты информационного пространства и регулирования цифровых коммуникаций.

Таким образом, анализ научной литературы показывает, что кибербезопасность рассматривается как комплексная проблема

современного общества, требующая междисциплинарного подхода и международного сотрудничества.

**Методология исследования**

Методологическую основу исследования составляют междисциплинарные методы анализа, применяемые для изучения феномена кибербезопасности.

В работе использовался системный подход, позволяющий рассматривать кибербезопасность как комплексное явление, включающее технологические, социальные и институциональные элементы.

Применение сравнительного анализа позволило сопоставить различные научные концепции кибербезопасности и выявить их ключевые особенности.

Также использовался контент-анализ научной литературы и нормативно-правовых документов, регулирующих вопросы информационной и кибербезопасности.

Кроме того, применялся аналитический метод, направленный на выявление основных тенденций развития киберугроз в современном мире.

Использование данных методов позволило обеспечить комплексное рассмотрение проблемы кибербезопасности в современном обществе.

**Результаты исследования**

Анализ современного состояния цифровой среды показывает, что кибербезопасность становится одним из ключевых факторов устойчивого развития общества. Рост числа кибератак и увеличение масштабов киберпреступности свидетельствуют о необходимости формирования эффективных систем защиты информационных ресурсов.

К числу основных факторов актуализации проблемы кибербезопасности относятся:

**1. Цифровизация экономики и общества**

Расширение использования цифровых технологий в различных сферах общественной жизни приводит к увеличению объема информации, передаваемой через интернет. Электронная коммерция, онлайн-банкинг, дистанционная работа и электронное государственное управление делают информационные системы ключевыми элементами современной экономики.

**2. Рост числа пользователей интернета**

По данным международных организаций, более половины населения мира активно использует интернет. Увеличение количества пользователей цифровых технологий сопровождается ростом числа киберпреступлений.

**3. Развитие киберпреступности**

Киберпреступность становится одной из наиболее прибыльных форм незаконной деятельности. Вредоносные программы, фишинговые атаки, кража персональных данных и другие формы цифровых преступлений представляют серьезную угрозу для общества.

**4. Уязвимость критической инфраструктуры**

Современные государства все больше зависят от цифровых систем управления. Нарушение функционирования энергетических систем, транспортных сетей или финансовых институтов может привести к серьезным экономическим последствиям.

**Обсуждение**

Полученные результаты исследования позволяют сделать вывод о том, что проблема кибербезопасности является одним из ключевых вызовов современного информационного общества. В условиях ускоренной цифровизации различных сфер общественной жизни значительно возрастает зависимость государств, организаций и отдельных граждан от информационно-коммуникационных технологий. Такая зависимость, с одной стороны, способствует повышению

эффективности управления, экономического развития и социальной коммуникации, а с другой — создает новые риски, связанные с уязвимостью цифровой инфраструктуры.

Одной из важнейших особенностей современного этапа развития общества является формирование глобального цифрового пространства, в котором информационные потоки практически не ограничены государственными границами. Это обстоятельство существенно усложняет процессы обеспечения кибербезопасности, поскольку большинство киберугроз имеет транснациональный характер. Кибератаки могут осуществляться из любой точки мира, а их последствия могут затрагивать различные государства и международные организации. В связи с этим обеспечение кибербезопасности требует координации усилий на международном уровне.

Современные исследования показывают, что киберугрозы становятся все более сложными и технологически продвинутыми. Если на ранних этапах развития интернета киберпреступность была в основном связана с деятельностью отдельных хакеров или небольших групп, то в настоящее время она все чаще носит организованный характер. Появление международных киберпреступных сетей, использование сложных вредоносных программ и применение методов социальной инженерии значительно усложняют борьбу с цифровыми преступлениями.

Особую обеспокоенность вызывает рост атак на критическую информационную инфраструктуру. Современные государства активно используют цифровые технологии для управления энергетическими системами, транспортной инфраструктурой, финансовыми институтами и системами государственного управления. В случае успешных кибератак на такие объекты возможны серьезные экономические и социальные последствия. Нарушение функционирования критической

инфраструктуры может привести к масштабным экономическим потерям и дестабилизации общественной жизни.

Важным аспектом обсуждаемой проблемы является также влияние киберугроз на политическую и информационную безопасность государств. В последние годы наблюдается активное использование цифровых технологий для распространения дезинформации, манипулирования общественным мнением и вмешательства в политические процессы. Такие явления представляют серьезную угрозу для демократических институтов и стабильности политических систем.

Кроме того, значительную роль в обеспечении кибербезопасности играет человеческий фактор. Многие кибератаки становятся возможными из-за недостаточного уровня цифровой грамотности пользователей, несоблюдения элементарных правил информационной безопасности или использования слабых систем защиты. В этой связи важным направлением повышения уровня кибербезопасности является развитие образовательных программ, направленных на формирование культуры безопасного поведения в цифровой среде.

Еще одним важным аспектом обсуждения является необходимость развития правового регулирования в сфере кибербезопасности. Быстрое развитие цифровых технологий требует постоянного обновления нормативно-правовой базы, регулирующей вопросы защиты информации, борьбы с киберпреступностью и обеспечения безопасности информационных систем. Эффективное правовое регулирование должно учитывать как национальные особенности развития информационного общества, так и международные стандарты в области кибербезопасности.

Следует также отметить важность сотрудничества между государственным и частным сектором. Значительная часть цифровой инфраструктуры находится в управлении частных компаний, поэтому обеспечение кибербезопасности невозможно без активного участия

бизнеса. Формирование эффективных механизмов государственно-частного партнерства способствует повышению уровня защиты информационных систем и развитию инновационных технологий безопасности.

Таким образом, результаты исследования подтверждают, что кибербезопасность представляет собой сложную междисциплинарную проблему, требующую комплексного подхода. Эффективное противодействие киберугрозам возможно только при сочетании технологических, организационных, правовых и образовательных мер.

**Заключение**

Проведенное исследование позволило проанализировать актуальность проблемы кибербезопасности в современном обществе и выявить основные тенденции ее развития. Результаты исследования показывают, что в условиях глобальной цифровизации кибербезопасность становится одним из ключевых факторов устойчивого функционирования современного общества.

Современный этап развития информационных технологий характеризуется стремительным ростом объемов цифровой информации, расширением использования интернет-технологий и формированием глобального киберпространства. Эти процессы способствуют развитию новых форм экономической и социальной деятельности, однако одновременно создают дополнительные риски, связанные с уязвимостью информационных систем.

Одним из наиболее значимых факторов актуализации проблемы кибербезопасности является рост масштабов киберпреступности. Кибератаки, направленные на получение конфиденциальной информации, нарушение функционирования информационных систем или нанесение экономического ущерба, становятся все более распространенными. Это требует разработки эффективных механизмов

защиты информационных ресурсов и повышения уровня устойчивости цифровой инфраструктуры.

Особое значение имеет обеспечение безопасности критической информационной инфраструктуры, от функционирования которой зависит стабильность экономики и государственного управления. Современные государства должны уделять особое внимание разработке национальных стратегий кибербезопасности и созданию специализированных институтов, занимающихся мониторингом и предотвращением киберугроз.

Не менее важным направлением обеспечения кибербезопасности является развитие международного сотрудничества. Поскольку большинство киберугроз носит транснациональный характер, эффективная борьба с киберпреступностью требует координации усилий государств, международных организаций и частного сектора. Развитие международных стандартов и механизмов обмена информацией о киберугрозах способствует повышению уровня глобальной цифровой безопасности.

Также необходимо уделять значительное внимание развитию человеческого капитала в сфере информационной безопасности. Повышение уровня цифровой грамотности населения, подготовка квалифицированных специалистов и развитие образовательных программ в области кибербезопасности являются важными условиями формирования устойчивой системы защиты информационного пространства.

В перспективе дальнейшая цифровизация общества будет сопровождаться появлением новых технологических решений, таких как искусственный интеллект, интернет вещей и квантовые вычисления. Эти технологии открывают новые возможности для развития экономики и общества, однако одновременно создают новые вызовы в области

кибербезопасности. В связи с этим научные исследования в данной сфере будут приобретать все большее значение.

Таким образом, проблема кибербезопасности является одной из наиболее актуальных проблем современного мира. Ее эффективное решение требует комплексного подхода, объединяющего технологические инновации, правовое регулирование, международное сотрудничество и развитие культуры безопасного использования цифровых технологий.

Перспективы дальнейших исследований связаны с разработкой новых методов защиты информационных систем, анализом социальных аспектов цифровой безопасности и формированием эффективных механизмов противодействия киберугрозам в условиях глобального информационного общества.

**Список литературы**

Castells, M. (2010). *The rise of the network society*. Wiley-Blackwell.

Deibert, R. (2013). *Black code: Surveillance, privacy, and the dark side of the Internet*. McClelland & Stewart.

Kshetri, N. (2021). *Cybercrime and cybersecurity in the global south*. Palgrave Macmillan.

Lopatyn, V. N. (2016). *Information security of Russia*. Moscow.

Nye, J. (2017). Deterrence and dissuasion in cyberspace. *International Security*.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Wellman, B. (2001). Physical place and cyberplace: The rise of personalized networking. *International Journal of Urban and Regional Research*.