

**12.00.10- МЕЖДУНАРОДНОЕ ПРАВО
ЗАЩИТА ПРАВ ЧЕЛОВЕКА В ЦИФРОВОМ ПРОСТРАНСТВЕ**

Мамбеткаримова Мадина Жандос кизи ¹

¹ *Ташкентский государственный юридический университет
Факультет Публичного права 4-курс студент
E-mail: mtambetkarimova03@gmail.com
Тел.: (+99890)660-11-88*

**ИНФОРМАЦИЯ
О СТАТЬЕ**

АННОТАЦИЯ:

**ИСТОРИЯ
СТАТЬИ:**

*Received: 31.01.2025
Revised: 01.02.2025
Accepted: 02.02.2025*

**КЛЮЧЕВЫЕ
СЛОВА:**

*цифровизация,
конфиденциальность,
интернет,
персональные данные.
Право на частную
жизнь,
киберпреступность,
General Data
Protection Regulation
(GDPR).*

в статье рассматриваются ключевые аспекты защиты прав человека в цифровом пространстве, учитывая быстрые темпы цифровизации, глобальную распространённость интернета и рост использования информационных технологий. Особое внимание уделяется вопросам конфиденциальности, защиты персональных данных, свободы выражения мнений и доступа к информации. Также анализируются правовые и этические аспекты, связанные с противодействием киберпреступности и регулированием цифровых платформ. Изучается международный и национальный опыт правового регулирования цифрового пространства, предлагаются направления для улучшения существующих механизмов защиты прав человека.

ВВЕДЕНИЕ. Современное общество стремительно движется в сторону цифровизации, охватывая все сферы жизни: от повседневных коммуникаций и образования до глобальных экономических процессов и правосудия. Расширение интернета и информационных технологий принесло значительные выгоды, но одновременно создало новые вызовы для защиты прав человека. Вопросы

конфиденциальности, безопасности персональных данных, а также угрозы киберпреступности и цифрового неравенства стали предметом активных дискуссий на национальном и международном уровнях.

Одним из основных прав, которое особенно уязвимо в цифровом мире, является право на частную жизнь. В цифровом пространстве личные данные собираются и анализируются с бешеной скоростью и объемом. Пользователи сети часто не осознают, какие данные о них собираются и как они могут быть использованы. Нарушения права на частную жизнь могут происходить как со стороны частных компаний, занимающихся сбором данных для коммерческих целей, так и со стороны правительств, использующих эти данные для слежки.

А также обычные люди снимают и опубликует видео и фото личного характера без разрешения пользователей на таких платформах, как Instagram , YouTube, или TikTok, тем самым нарушая личные границы и право на частную жизнь граждан, особенно в этом случае страдают медийные личности такие как актеры, певцы и блогеры, они свободно не могут находиться в общественных местах без грима и в обычных нарядах, папарацци их снимают на видео и фото и выкладывают в сети интернет что в последствии эти знаменитости получают оскорбительные комментарий по поводу внешности и одежды от людей и не только и как результат от такого негативного давления от пользователей страдают психика этих личностей.

Цифровое пространство также стало платформой для выражения мнений и общения. Интернет дает людям возможность делиться своими идеями, обмениваться информацией и участвовать в общественных дискуссиях. Однако свобода выражения мнений в цифровом пространстве часто сталкивается с цензурой, ограничениями со стороны платформ социальных сетей и государственным вмешательством. Во многих странах правительство пытается контролировать содержание, распространяемое в интернете, что приводит к ограничениям свободы слова и подавлению инакомыслия, с одной стороны государству можно понять, есть сведения которые относятся к государственному тайну и никто не гарантирует что он не всплывет в общественное признание и его присутствие в сети интернет опасно для самого государства.

Правовое регулирование цифрового пространства находится на стадии активного развития. Многие государства и международные организации работают над созданием комплексных нормативных актов, направленных на защиту прав человека в интернете. Важную роль в этом процессе играют международные документы, такие как Международный пакт о гражданских и политических правах (МПГПП), который

устанавливает принципы защиты прав на свободу слова, частную жизнь и справедливое судебное разбирательство, применимые и в цифровой сфере [1].

GDPR стал значительным шагом в области защиты персональных данных, установив строгие требования к обработке данных и предоставив гражданам больше контроля над своей информацией. Примеры других национальных инициатив включают в себя Закон о защите конфиденциальности в интернете в США, а также законопроекты в России и Китае, направленные на регулирование цифровых платформ. [2]

А также в Узбекистане есть ряд законов и нормативных актов, которые касаются регулирования цифрового пространства, защиты персональных данных и обеспечения кибербезопасности. Ниже перечислены некоторые ключевые законы и правовые акты, связанные с цифровым пространством в Узбекистане:

1. Закон «О защите персональных данных» (2021):

Этот закон регулирует сбор, хранение, обработку и защиту персональных данных граждан. Он требует, чтобы организации получали согласие граждан на обработку их данных и обеспечивали их безопасность. Закон также предусматривает ответственность за нарушения в сфере обработки данных. [3]

2. Закон «Об информатизации» (2003):

Закон регулирует вопросы использования информационных систем и ресурсов, включая развитие инфраструктуры и обеспечение доступа к цифровым технологиям. Он определяет принципы государственной политики в сфере информатизации и регулирует деятельность государственных органов и частных компаний в этом направлении. [4]

3. Закон «О кибербезопасности» (2022):

Принят для обеспечения безопасности в цифровом пространстве. В нём прописаны меры по предотвращению киберугроз, защите критической инфраструктуры и обеспечению защиты данных. Также он направлен на борьбу с киберпреступностью и создание условий для безопасного использования цифровых технологий. [5]

4. Закон «О защите информации» (1993, с изменениями):

Определяет основные правила защиты информации в государственных и частных структурах. Закон регулирует сбор, обработку и хранение информации, а также предусматривает меры по обеспечению её конфиденциальности и целостности. [6]

5. Концепция развития “Цифрового Узбекистана – 2030”:

Это стратегическая программа, направленная на цифровизацию различных секторов экономики и государственной сферы. Она предполагает развитие информационно-коммуникационных технологий (ИКТ), внедрение цифровых услуг и повышение уровня цифровой грамотности населения. [7]

6. Нормативные акты по регулированию интернета и социальных сетей:

Эти законы и нормативные акты направлены на создание безопасного и регулируемого цифрового пространства в стране, а также на защиту прав граждан в этой сфере.

Несмотря на это, проблем достаточно хватает в этой сфере и ниже будем рассмотреть проблем с возможными решениями как говорится новые проблемы требуют новые решения.

Развитие цифровых технологий также породило новые угрозы для прав человека. Взлом аккаунтов и утечки данных, становятся повседневными явлениями.

Более того, государственные и частные структуры могут использовать цифровые средства для массового наблюдения, что подрывает право на частную жизнь, большинство.

В некоторых странах наблюдается усиление контроля над интернетом со стороны государства. Блокировка ресурсов, ограничение доступа к информации и уголовные преследования за выражение мнения в интернете — всё это нарушает основные права человека. Международное сообщество должно выработать более чёткие механизмы реагирования на такие нарушения.

Мнения учёных:

Эксперт по цифровой безопасности Даниэль Солове отмечает, что развитие технологий требует новых подходов к пониманию права на частную жизнь. Он утверждает, что традиционные концепции конфиденциальности устарели в условиях постоянного сбора данных, и необходимо переосмыслить подходы к защите личной информации. В его трудах подчёркивается, что права на частную жизнь должны учитывать риски, связанные с искусственным интеллектом и большими данными. [8]

Юрген Хабермас, известный философ и теоретик общественной сферы, подчеркивает, что цифровые технологии радикально изменили пространство для дискуссий, что, с одной стороны, расширило доступ к информации, но, с другой стороны, создало новые формы манипуляции общественным мнением. Хабермас считает, что необходимо более чёткое регулирование алгоритмов, управляющих

распространением информации в социальных сетях, чтобы избежать дискриминации и манипуляций. [9]

Исследователи, такие как Мануэль Кастель указывают на то, что цифровое неравенство не только отражает экономические различия между регионами, но и создает барьеры для равного доступа к информации, возможностям работы и обучения. Он подчёркивает необходимость включения проблемы цифрового разрыва в повестку дня глобального развития, а также активное участие правительств в обеспечении доступа к цифровым технологиям для всех слоёв населения. [10]

Кейт Кроуфорд, исследователь в области искусственного интеллекта и цифровых технологий, утверждает, что алгоритмы, которыми управляются цифровые платформы, часто воспроизводят предвзятости и дискриминацию, существующие в обществе. Она подчёркивает важность создания нормативных стандартов для контроля за прозрачностью и справедливостью работы алгоритмов, а также необходимость привлечения независимых экспертов к их оценке. [11]

Брус Шнайер, эксперт по кибербезопасности, в своих работах указывает на растущие угрозы со стороны киберпреступности и вмешательства государств в частную жизнь граждан. Шнайер утверждает, что общество недооценивает угрозы, связанные с массовым наблюдением и утечками данных, и предлагает разработку более строгих мер защиты цифровых прав, а также усиление контроля над государственными органами, занимающимися наблюдением. [12]

Цифровое пространство стало новым полем для реализации прав человека, но вместе с этим принесло новые вызовы и угрозы. Государства, международные организации и цифровые платформы должны работать совместно, чтобы разработать эффективные механизмы защиты прав человека в интернете, обеспечивая баланс между безопасностью и свободой. Перспективы развития правовой базы включают создание более жёстких стандартов защиты данных, контроль над алгоритмами и усиление международного сотрудничества в борьбе с киберпреступностью.

Список использованной литературы:

1.Международный пакт о гражданских и политических правах (МПГПП) – ООН, https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

(Принят резолюцией 2200 А (XXI) Генеральной Ассамблеи от 16 декабря 1966 года)

2. General Data Protection Regulation (GDPR) – Официальный текст закона. <https://gdpr-info.eu/> (дата создания 04.05.2016)

3. Закон «О защите персональных данных» <https://lex.uz/docs/4396428> (закон принят в 15.01.2021 г.)

4. Закон «Об информатизации» <https://lex.uz/docs/82956> (закон принят в 11.12.2003 г):

5. Закон «О кибербезопасности» <https://lex.uz/uz/docs/5960609> (закон принят в 15.04. 2022):

6. Закон «О защите информации» <https://lex.uz/docs/98845> (07.05.1993, с изменениями):

7. Концепция развития «Цифрового Узбекистана- 2030» <https://lex.uz/docs/5031048> (Указ Президента Республики Узбекистан, от 05.10.2020 г. № УП-6079)

8. Даниэль Солове автор книги «On privacy and Technology» <https://www.danielsolove.com/on-privacy-and-technolgy/> (планирует выпускать 2025 году)

9. Юрген Хабермас, эссе <https://ijoc.org/index.php/ijoc/article/download/23674/4813> (дата выпуска 2023)

10. Мануэль Кастель, книга «Beyond the Digital Divide: Contextualizing the Information Society»

<https://www.brookings.edu/articles/fixing-the-global-digital-divide-and-digital-access-gap/> (дата выхода 24.09.2018.)

11. Кейт Кроуфорд, книга «Power, Politics and the Planetary Costs of Artificial Intelligence» <https://www.radicalai.org/atlas-of-ai> (год выпуска 06.04. 2021 г)

12. Брус Шнайер, книга «Data and Goliath» https://www.schneier.com/news/archives/2015/06/surveillance_bulk_da.html (дата выпуска 24.03.2015)