УДК: 342.7(575.2)(04)
DOI 10.53473/16946324_2023_4

Тенизбек кызы Назира
ю.и.к., доценттин милдетин аткаруучу
Кыргыз Республикасынын эл аралык университети
Шергазиева Айдана Нурмаматовна
530500 – Юриспруденция багытынын
2–курсунун магистранты
Кыргыз Республикасынын эл аралык университети
Тенизбек кызы Назира
к.ю.н., и.о.доцента кафедры Международного,
предпринимательского право и политологии
Международный университет Кыргызской Республики
Шергазиева Айдана Нурмаматовна
Магистрант 2–курса,
направление 530500 Юриспруденция
Международный университет Кыргызской Республики
Tenizbek kyzy Nazira
PhD in Law, Acting Associate Professor
International University of the Kyrgyz Republic
mobile phone: +996 755 552227,
e-mail: nazira.tenizbekovna@mail.ru
Shergazieva Aidana Nurmamatovna
2nd year master's student, direction
International University of the Kyrgyz Republic
mobile phone: +996 706 020077,
e-mail: aidana.wergazieva@gmail.com

САНАРИПТЕШТИРҮҮ ДООРУНДАГЫ АДАМ УКУКТАРЫ: ЧАКЫРЫКТАР ЖАНА ПЕРСПЕКТИВАЛАР

ПРАВА ЧЕЛОВЕКА В ВЕК ЦИФРОВИЗАЦИИ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ

HUMAN RIGHTS IN THE AGE OF DIGITIZATION: CHALLENGES AND PROSPECTS

Аннотациясы: *Макалада санариптештирүүнүн азыркы коомдогу адам укуктарына тийгизген таасири каралат. Санариптик технологиянын, Интернеттин жана массалык маалыматтарды иштетүүнүн тез өнүгүшүнүн шартында, адам укуктары жаңы контекстте пайда болууда. Бул макалада жеке маалыматтардын купуялуулугу жана корголушу, сөз эркиндиги, маалыматка жетүү, санариптик теңсиздик жана киберкоопсуздук менен байланышкан чакырыктар талданат. Санариптик революцияга байланыштуу коом жана мыйзам чыгаруучулар туш болгон кыйынчылыктарга өзгөчө көңүл бурулат. Макала ошондой эле жаңы санариптик реалдуулукта адам укуктарын коргоо жана илгерилетүү боюнча стратегияларды жана көрсөтмөлөрдү сунуштайт. Изилдөөнүн жыйынтыктары санариптештирүү доорундагы адам укуктары үчүн заманбап чакырыктарды жана мүмкүнчүлүктөрдү түшүнүүгө салым кошот.*

Негизги сөздөр: *адам укуктары, санариптештирүү, маалыматтардын купуялуулугу, сөз эркиндиги, кибер коопсуздук, маалыматка жетүү, санариптик теңсиздик, адам укуктарынын заманбап чакырыктары жана мүмкүнчүлүктөрү, санариптештирүү доору.*

Аннотация: *В статье рассматривается влияние цифровизации на права человека в современном обществе. В свете быстрого развития цифровых технологий, интер-*

нета и массовой обработки данных, права человека оказываются в новом контексте. В данной статье анализируются вызовы, связанные с конфиденциальностью и защитой персональных данных, свободой слова, доступом к информации, цифровым неравенством и кибербезопасности. Особое внимание уделяется вызовам, с которыми сталкиваются общество и законодатели в связи с цифровой революцией. Статья также предлагает стратегии и рекомендации по защите и продвижению прав человека в новой цифровой реальности. Результаты исследования представляют собой вклад в понимание современных вызовов и возможностей для прав человека в эпоху цифровизации.

Ключевые слова: *права человека, цифровизация, конфиденциальность данных, свобода слова, кибербезопасность, доступ к информации, цифровое неравенство, современные вызовы и возможности прав человека, эпоха цифровизации.*

Abstract: *The article examines the impact of digitalization on human rights in modern society. In the light of the rapid development of digital technologies, the Internet and mass data processing, human rights find themselves in a new context. This article analyzes the challenges associated with confidentiality and protection of personal data, freedom of speech, access to information, digital inequality and cybersecurity. Particular attention is paid to the challenges faced by society and legislators in connection with the digital revolution. The article also offers strategies and recommendations for the protection and promotion of human rights in the new digital reality. The results of the study are a contribution to the understanding of modern challenges and opportunities for human rights in the era of digitalization.*

Keywords: *human rights, digitalization, data privacy, freedom of speech, cybersecurity, access to information, digital inequality, modern challenges and opportunities of human rights, the era of digitalization.*

В наше время цифровизация и информационно-коммуникационные технологии (ИКТ) играют все более важную роль в повседневной жизни человека. Это вызывает серьезные вопросы относительно того, как цифровизация влияет на права человека. Цифровизация включая сбор и анализ данных, интернет-связь, искусственный интеллект и автоматизацию, может как укреплять права человека, так и представлять угрозы для них.

В Кыргызской Республике, как и во многих других странах, цифровизация оказывает значительное воздействие на права человека. Стремительное внедрение технологий и доступ к интернету открывают новые возможности, но также вызывают опасения в отношении приватности, свободы слова и равенства.

Конфиденциальность и защита персональных данных. Цифровизация оказывает глубокое влияние на разнообразные аспекты жизни и приносит множество преимуществ, она также вызывает вопросы, связанные с конфиденциальностью данных, безопасностью и доступностью, но также может подвергать риску конфиденциальность и защиту персональных данных. Примером может служить деятельность крупных технологических компаний, которые собирают огромные объемы персональных данных пользователей без их явного согласия. В 2018 году компания Facebook была замешана в скандале с Cambridge Analytica, когда данные более 87 миллионов пользователей были несанкционированно использованы для политических целей [1]. Этот случай подчеркивает важность защиты персональных данных и конфиденциальности в цифровую эпоху.

Конфиденциальность и защита персональных данных является одним из важнейших аспектов прав человека, и в контексте современных цифровых технологий существуют как положительные, так и отрицательные стороны.

Положительные стороны права на конфиденциальность:

1. Защита личной сферы: право на конфиденциальность позволяет гражданам защищать свою личную сферу и управлять, какие данные о них собираются и использованы.
2. Свобода выражения: граждане чувствуют себя уверенно, что их личные данные не будут злоупотреблены, они могут свободно выражать свои мнения и идеи в онлайн-среде без опасений.

3. Безопасность и защита от преступности: правонфиденциальность обеспечивает защиту от незаконного доступа к личной информации, что способствует предотвращению кражи личных данных и мошенничества.

4. Свобода религии и убеждений: граждане могут свободно исповедовать свою религию и убеждения, не беспокоясь о нежелательном вмешательстве в их личные дела.

Отрицательные стороны права на конфиденциальность:

1. Злоупотребление преступниками: право на конфиденциальность может быть использовано преступниками для скрытия противоправной деятельности, включая киберпреступности и терроризм.

2. Ограничения в расследованиях: в ряде случаев, право на конфиденциальность может затруднить расследование преступлений, так как оно ограничивает доступ к информации.

3. Потенциальная угроза безопасности: в некоторых случаях, если информация о нарушении права на конфиденциальность становится известной (например, в случае утечки данных), это может привести к угрозе для безопасности личности.

4. Злоупотребление правом на анонимность: анонимность в интернете может быть использована для разжигания ненависти, кибербуллинга и распространения дезинформации.

Право на конфиденциальность является важным аспектом прав человека, и его соблюдение и балансирование с другими интересами, такими как безопасность и соблюдение закона, представляют сложные вызовы в цифровой эпохе. Необходим баланс между защитой конфиденциальности граждан и обеспечением безопасности общества.

Свобода слова. Цифровизация создает новые площадки для свободы слова, но также может сопровождаться цензурой и ограничениями. Примером является блокировка социальных сетей и интернет-ресурсов в различных странах для подавления политических дискуссий и свободы мнений. Китайская «Великая китайская брань» — это пример масштабной цензуры в сети, которая ограничивает доступ к многим информационным ресурсам и социальным сетям [2]. Свобода слова с учетом влияния цифровизации, предполагает, как положительные, так и негативные аспекты.

Положительные аспекты

Активное общественное обсуждение. Интернет и социальные сети стали мощными инструментами для общественного обсуждения и выражения мнений. Граждане активно обсуждают политические, социальные и экономические вопросы, что способствует развитию демократических процессов в стране.

Независимые СМИ и блогеры. В цифровую эпоху множество независимых СМИ и блогеров получили возможность донести информацию до широкой аудитории. Это дополняет традиционные СМИ и способствует разнообразию мнений и источников информации.

Активные дискуссии о правах человека. Активное движение за права человека и общественные инициативы, которые используют интернет для освещения и защиты прав граждан. Это включает в себя противодействие насилию в семье, защиту прав женщин и детей, и другие важные вопросы.

Негативные аспекты

Дезинформация и фейковые новости. В цифровую эпоху распространение дезинформации и фейковых новостей стало серьезной проблемой. Это может воздействовать на общественное мнение и политические решения, что ослабляет доверие к информации.

Угрозы журналистам и блогерам. Журналисты и блогеры иногда подвергаются угрозам из-за их профессиональной деятельности. Это создает атмосферу страха и самоцензуры.

Кибербезопасность. На сегодняшний день человечество сталкивается с проблемами общемировой безопасности: например, с природными и техногенными катастрофами, эпидемиями и вооруженными конфликтами. В связи с нарастающим темпом развития

цифрового общества перед человечеством предстала ещё одна проблема – кибербезопасность. Термин «кибербезопасность» представляет собой меры по защите персональных данных от несанкционированного доступа, копирования, изменения, воровства информации как отдельных граждан, так и частных компаний и даже государства.

В нашем мире практически каждая организация сталкивается с проблемой кибератаки, что наносит предельный ущерб государству, компаниям и, непосредственно, сотрудникам. То есть, вся информация о персональных данных пользователей, клиентов и работников аккумулируется у мошенников, что может привести к непоправимым последствиям для вышеперечисленных. Следовательно, перед пользователями стоит задача качественного и количественного повышения мер по контролю защиты информации. Такие действия приведут к снижению рисков возникновения потенциальных кибератак.

Также важно упомянуть о трёх важных элементах кибербезопасности: конфиденциальности, целостности и доступности данных, обеспечивающих информационную безопасность. В случае с конфиденциальностью данных, только пользователь с разрешённым доступом имеет возможность вносить какие-либо изменения. Изменения данных пользователями, наделёнными этими правами, обуславливает целостность данных. А доступность, в свою очередь, означает, что данные всегда доступны для авторизованных пользователей.

Проблема состоит в том, что при условии развития защиты от кибератак, сами методы и технологии кибератак так же непрерывно улучшаются. И нельзя сказать, что меры, предпринятые вчера по защите данных от кражи, сработают и сегодня. Кибератаки и киберугрозы стали частыми появлениями и принимают различные формы, например, вредоносные программы, социальная инженерия, фишинг, вирусы-вымогатели и многое другое.

Необходимо отметить актуальную на сегодняшний день тему– криптовалюты.

В частности, блокчейн-технология, может способствовать увеличению уровня кибербезопасности по причине децентрализации, использование токенов для безопасности, аутентификация и идентификация идр.

По информации директора «Лаборатории Касперского в Центральной Азии» по итогам 2021 года каждый 67-й житель Кыргызской Республики столкнулся с кибератаками и всего в прошлом году «Лаборатория Касперского» зафиксировала порядка 250 миллионов атак, направленных на пользователей. И существенная их доля, 42 процента, так или иначе была связана с атаками на финансовые институты [3].

1. Однако в Кыргызской Республике существуют соответствующие уголовные наказания за преступление против кибербезопасности в рамках главы 40 «Преступления против кибер-безопасности» Уголовного Кодекса Кыргызской Республики от 28 октября 2021 года № 127. [4]

Статьи, предусмотренные законом Кыргызской Республики за эти действия:

2. Статья 319 Уголовного Кодекса Кыргызской Республики «Несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи»;
3. Статья 320 Уголовного Кодекса Кыргызской Республики «Создание вредоносных программных продуктов
4. Статья 321 Уголовного Кодекса Кыргызской Республики «Кибер-саботаж»;
5. Статья 322 Уголовного Кодекса Кыргызской Республики «Массовое распространение электронных сообщений».

В целях рекомендации ниже составлена краткая информация Kaspersky о понятии кибербезопасности, которые помогут обезопасить от вредоносных кибератак.

1. Использовать антивирусные программы;
2. Использовать надежные пароли;
3. Обновлять программное обеспечение и операционную систему;
4. Не открывать почтовые вложения от неизвестных отправителей (они могут быть заражены вредоносным программным обеспечением);

5. Не переходить по ссылкам, полученным по почте от неизвестных отправителей или неизвестных веб-сайтов;
6. Избегать незащищенных сетей Wi-fi в общественных местах.

Обеспечение кибербезопасности цифровых инфраструктур и сервисов, которые активно создаются, является одним из важнейших вопросов в противостоянии подобным вызовам современности. Учитывая, что в последнее время наблюдаются хакерские атаки на государства и другие информационные системы, есть необходимость как поднять и развить это направление до качественного уровня. Актуальность работы связана с динамичными процессами в сфере международной и региональной безопасности, а также с последствиями военно-политических событий в мире.

Равенство. Цифровизация также может влиять на равенство. Например, в доступе к образованию и возможностям трудоустройства. В развивающихся странах, где доступ к технологиям ограничен, цифровое неравенство может усугубить социальное и экономическое неравенство. Один из способов борьбы с этой проблемой – развитие доступа к интернету и цифровой грамотности. Вопросы равенства в цифровом мире также актуальны для Кыргызской Республики. Доступ к высокоскоростному интернету и современным технологиям далеко не всегда равномерен по всей стране. Сельские районы и удаленные области могут страдать от ограниченного доступа к цифровым ресурсам, что создает цифровое неравенство.

Тем не менее, Кыргызская Республика занял второе место по скорости широкополосного Интернета среди стран Центральной Азии. Такие данные приводит британский портал Cable.co.uk. [5] Так, согласно мировому рейтингу, 1-е место в Центральной Азии по скорости Интернета занимает Узбекистан (131-е место в мировом рейтинге), 2-е – Кыргызская Республика (142-е место). За ними идут Республика Казахстан (155-е место) и Республика Туркменистан (206-е место). Самый медленный Интернет в Центральной Азии – в Республике Таджикистане (214-е место). В топ-5 стран с самым быстрым широкополосным Интернетом в мире вошли остров Джерси (Великобритания), Лихтенштейн, Макао, Исландия и Гибралтар.

Равенство остается важным аспектом прав человека, и влияние цифровизации создает как вызовы, так и возможности для его соблюдения. Важно обеспечивать равное участие всех граждан в цифровом мире, бороться с цифровым неравенством и дезинформацией, и защищать права на доступ к информации и участие в общественной жизни для всех.

Доступ к информации. С одной стороны, цифровизация увеличивает доступ к информации и знаний. С другой стороны, это может привести к информационной перегрузке и распространению дезинформации. Примером является проблема фейковых новостей, которые могут воздействовать на общественное мнение и даже политические решения. С одной стороны, интернет предоставляет доступ к обширным информационным ресурсам. Однако, как и в других странах, в Кыргызской Республике существует проблема распространения дезинформации и фейковых новостей, которые могут воздействовать на общественное мнение и политические процессы.

Цифровизация предоставляет Кыргызской Республике новые возможности для развития, но также представляет вызовы для защиты прав человека. Власти и общество должны работать совместно, чтобы разработать эффективные законы и механизмы контроля, которые обеспечат баланс между цифровым развитием и защитой прав и свобод человека. Фейковые новости и дезинформация стали проблемой в Кыргызской Республике, как и во многих других странах.

Таким образом, эти примеры подчеркивают важность разработки и реализации эффективных мер для защиты прав человека в условиях цифровой трансформации. Кыргызская Республика, как и многие другие страны, должна балансировать между использованием технологий для развития и защитой основных прав и свобод граждан.

Список использованной литературы:

1. Скандал с Facebook и Cambridge Analytica. **Режим доступа:** https
2. Интернет-цензура в Китайской Народной Республике. **Режим доступа:** https://ru.wikipedia.org/wiki/Интернет-цензура_в_Китайской_Народной_Республике;
3. Каждый 67-й житель Кыргызстана в 2021 году столкнулся с кибератаками. **Режим до- ступа:** https://theworldnews.net/kg-news/kazhdyi-67-i-zhitel-kyrgyzstana-v-nbsp-2021- godu-stolknulsia-s-nbsp-kiberatakami;
4. **Уголовный кодекс [Электронный ресурс]: закон Кыргызской Республики от 28 октября 2021 года № 68 (в ред. Законов Кыргызской Республики с изменениями и дополнениями по состоянию на 10 октября 2023 года № 186) // – Режим доступа: http://cbd.minjust.gov.kg/act/view/ru-ru/568 – Загл. с экрана.;**
5. Кыргызстан занял второе место в Центральной Азии по скорости Интернета. **Ре-жим..доступа:**https://kaktus.media/doc/488223_kyrgyzstan_zanial_vtoroe_mesto_v_centra lnoy_azii_po_skorosti_interneta.html;
6. **Основное выступление Верховного комиссара ООН по правам человека Мишель Бачелет. Японское общество, Нью-Йорк, 17 октября 2019 г.**
7. United Nations Human Rights Council. (2021). Annual Report of the United Nations High Commissioner for Human Rights and Reports of the Office of the High Commissioner and the Secretary-General. United Nations.
8. Предотвращение кибератак https://www.kaspersky.ru/resource-center/preemptive- safety/how-to-prevent-cyberattacks
9. https://www.cable.co.uk

Всероссийская научно-теоретическая конференция «Права человека в условиях цифровой трансформации общества и государства». / Сборник статей. Ростов-на-Дону – Таганрог. Издательство Южного федерального университета. 2021. Стр. 41-42.