“ADOLAT”
MILLIY HUQUQIY AXBOROT MARKAZI
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=382

2026-yil
8-son
avgust
ISSN 3093-8546

Киберрабство как новая форма эксплуатации: научный анализ, кейс-стади и правовые перспективы

Комила Рашидова,
самостоятельный соискатель
Университета общественной безопасности Республики Узбекистан
e-mail: kamilarash27@gmail.com

Аннотация. Maqola jamiyatning raqamli transformatsiyasi sharoitida yuzaga kelayotgan, hali yetarlicha o‘rganilmagan shaxsni ekspluatatsiya qilishning yangi shakli, ya’ni kiberqullik (cyberslavery) hodisasiga bag‘ishlangan. Maqolada kiberqullikni ta’riflashning normativ, kriminologik va etik yondashuvlari, shuningdek uni mustaqil huquqiy kategoriya sifatida tan olish borasidagi ilmiy bahslar ko‘rib chiqiladi. Janubi-Sharqiy Osiyodagi onlayn firibgarlik fermalari, sextortion, gold farming va Afrikadagi mayning fermalarida bolalar mehnatidan foydalanish kabi keys-stadilar asosida huquqni qo‘llash muammolari, jumladan jinoyatlarning transchegaraviy xususiyati va raqamli dalillarni to‘plashdagi qiyinchiliklar tahlil qilinadi. Muallif xalqaro huquqiy tartibga solishni isloh qilish, jumladan raqamli ekspluatatsiya shakllari to‘g‘risida maxsus konvensiya ishlab chiqish va raqamli ombudsmenlar institutini yaratish bo‘yicha takliflar ilgari suradi.

Калит сўзлар. kiberqullik, odam savdosi, majburiy mehnat, raqamli ekspluatatsiya, inson huquqlari, kiberxavfsizlik, Budapesht konvensiyasi, firibgarlik fermalari, sextortion.

Аннотация. Статья посвящена феномену киберрабства (cyberslavery) как новой, недостаточно исследованной форме эксплуатации личности, возникающей в условиях цифровой трансформации общества. Рассматриваются нормативный, криминологический и этический подходы к определению киберрабства, а также научная полемика о его квалификации в качестве самостоятельной правовой категории. На основе кейс стади, включающих онлайн скам фермы Юго Восточной Азии,sextortion,goldfarmingи детский труд на майнинговых фермах, анализируются правоприменительные вызовы, включая трансграничный характер преступлений и сложность сбора цифровых доказательств. Автор формулирует предложения по реформированию международно правового регулирования, включая разработку специализированной конвенции о цифровых формах эксплуатации и создание института цифровых омбудсменов.

Ключевые слова. киберрабство, торговля людьми, принудительный труд, цифровая эксплуатация, права человека, кибербезопасность,

Будапештская конвенция, скам-фермы, sextortion.

Annotation. This article addresses the phenomenon of cyber slavery as a new and insufficiently studied form of exploitation of the individual, emerging in the context of the digital transformation of society. The article examines normative, criminological, and ethical approaches to defining cyber slavery, as well as the scholarly debate regarding its qualification as an independent legal category. Drawing on case studies, including online scam farms in Southeast Asia, sextortion, gold farming, and child labour at cryptocurrency mining sites in Africa, the article analyzes law enforcement challenges, including the cross-border nature of the crimes and the difficulty of collecting digital evidence. The author formulates proposals for reforming international legal regulation, including the development of a specialized convention on digital forms of exploitation and the creation of a digital ombudsman institution.

Keywords. cyber slavery, human trafficking, forced labour, digital exploitation, human rights, cybersecurity, Budapest Convention, scam farms, sextortion.

Введение:

Феномен киберрабства (cyber slavery) является одной из наиболее острых социальных и правовых проблем цифровой эпохи. Под киберрабством понимается систематическое использование информационно коммуникационных технологий для принуждения, контроля или обмана человека с целью его эксплуатации [1]. Это явление интегрирует элементы классического рабства, торговли людьми и киберпреступности, формируя междисциплинарную исследовательскую проблему, которая затрагивает международное право, социологию, кибербезопасность и этику.

По данным Walk Free Foundation, общее число людей, находящихся в условиях современного рабства, превышает 50 миллионов человек, из которых растущая доля подвергается цифровым формам эксплуатации [2]. Цифровизация усиливает трансграничный характер проблемы: вербовка, контроль и принуждение могут осуществляться из другой юрисдикции, что создает серьезные вызовы для национальных правовых систем и требует выработки согласованных международных подходов.

Целью настоящей статьи является комплексный анализ феномена киберрабства через призму теоретических подходов, научной полемики и практических кейсов, а также формулирование предложений по совершенствованию правового регулирования данной сферы.

Методологическую основу исследования составляют сравнительно-правовой, формально-юридический и системный методы анализа, позволяющие сопоставить положения действующих международных конвенций с фактическими проявлениями киберрабства,

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

зафиксированными в правоприменительной практике различных государств. Использование кейс-стади в качестве самостоятельного метода исследования обусловлено тем, что теоретические конструкции киберрабства, при всей их научной значимости, нуждаются в проверке на конкретном эмпирическом материале, отражающем реальные механизмы цифрового принуждения.

Актуальность настоящего исследования определяется тем обстоятельством, что стремительное развитие цифровых платформ, алгоритмов автоматизированного принятия решений и трансграничных финансовых сервисов создает принципиально новые возможности для эксплуатации личности, которые зачастую остаются вне поля зрения традиционных механизмов уголовно-правовой и гражданско-правовой защиты. В этой связи представляется необходимым системное осмысление киберрабства как самостоятельного, хотя и тесно связанного с классическими формами эксплуатации, правового феномена.

Теоретические основы и концептуальные подходы:

1.1. Нормативно-правовая рамка:

Запрет рабства и подневольного состояния закреплен во множестве международно-правовых документов, включая статью 4 Европейской конвенции о защите прав человека и основных свобод [3], статью 8 Международного пакта о гражданских и политических правах [4], Конвенцию Международной организации труда №29 о принудительном труде [5], а также Протокол о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее, известный как Палермский протокол [6]. Однако ни один из этих документов напрямую не упоминает цифровые формы эксплуатации, поскольку они были приняты до наступления эпохи повсеместной цифровизации общественных отношений.

Gallagher указывает, что интерпретация указанных норм должна расширяться, чтобы охватывать вербовку и эксплуатацию, осуществляемые через сеть Интернет, поскольку буквальное толкование традиционных определений рабства не всегда позволяет квалифицировать современные цифровые формы принуждения [7, С.45-52]. Современные исследователи выделяют три концептуальных подхода к определению киберрабства. Нормативный подход рассматривает киберрабство как расширение понятия торговли людьми в соответствии с Палермским протоколом [7, С.58-61]. Криминологический подход рассматривает киберрабство как вид организованной преступности, акцентируя внимание на технологиях принуждения и онлайн рекрутинге [8, С.112-118]. Этический подход связывает данный феномен с концепцией «капитализма слежки», в рамках которой личные данные и цифровое поведение человека становятся объектом

эксплуатации [9, С.20-27].

1.2. Социологический и криминологический анализ.

Киберрабство сочетает в себе черты как классического рабства, так и цифрового контроля поведения личности. Bryant выделяет три ключевых компонента данного явления. Первый компонент, принуждение, включает угрозы физического или цифрового характера, в частности утечку персональных данных и DDoS атаки в отношении жертвы или ее близких [8, С.120-124]. Второй компонент, ограничение свободы, состоит в невозможности покинуть онлайн платформу или прекратить участие в определенной деятельности без причинения существенного ущерба жертве [8, С.125-128]. Третий компонент, извлечение выгоды, охватывает экономическую, сексуальную или иную форму эксплуатации, получаемую эксплуататором за счет жертвы [8, С.129-133].

1.3. Этическое измерение.

Zuboff связывает киберрабство с концепцией «капитализма слежки», при которой данные пользователей систематически собираются и используются в качестве инструмента манипуляции их поведением [9, С.30-38]. В данном контексте научная полемика приобретает дополнительное измерение: возникает вопрос о том, является ли согласие пользователя на обработку его персональных данных подлинно добровольным волеизъявлением либо оно фактически навязано асимметрией переговорных позиций между цифровой платформой и пользователем.

Научная полемика:

Вопрос о признании киберрабства самостоятельной правовой категорией вызывает существенные разногласия в академическом сообществе. Представители широкой школы, в частности Bales, считают, что даже относительно мягкие формы цифрового контроля над трудом работников, включая гиг экономику и платформенные рейтинговые системы, следует рассматривать в качестве одной из форм эксплуатации, ограничивающей свободу выбора личности [10, С.14-22].

Представители узкой школы, к которым относится Gallagher, настаивают на сохранении строгих юридических критериев рабства, включающих насилие, реальную угрозу и отсутствие добровольности со стороны потерпевшего [7, С.65-70]. По мнению данных авторов, чрезмерное расширение понятия «рабство» способно размыть его юридические границы и, как следствие, снизить эффективность правоприменения в отношении наиболее тяжких форм эксплуатации.

Гибридный подход, предложенный Latonero, заключается в разделении «жесткого» киберрабства, то есть принудительного труда в скам фермах и аналогичных структурах, и «мягкой» цифровой эксплуатации, охватывающей манипулятивные практики цифровых корпораций [11, С.8-13]. Данная классификация представляется методологически

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

продуктивной, поскольку позволяет дифференцировать степень тяжести различных форм цифрового принуждения и, соответственно, определять адекватные правовые последствия для каждой из них.

Особую остроту научная полемика приобретает при обсуждении статуса цифровых трудовых платформ: одни исследователи расценивают их как форму киберэксплуатации, тогда как другие рассматривают их в качестве составной части легитимной цифровой экономики. Представляется, что разрешение данного спора требует выработки четких количественных и качественных критериев, позволяющих отграничивать законную гибкую занятость от скрытых форм цифрового принуждения.

Кейс-стади:

Для иллюстрации многообразия проявлений киберрабства целесообразно рассмотреть несколько показательных кейсов, документированных в научной и журналистской литературе.

Первый кейс касается онлайн скам ферм в Камбодже и Мьянме. Согласно данным агентства Reuters, тысячи трудовых мигрантов были обманным путем вовлечены в трудовую деятельность в колл центрах, где под угрозой физического насилия их принуждали совершать онлайн мошенничества в отношении граждан третьих стран [12]. Отдельные жертвы, по имеющимся сведениям, продавались между различными лагерями, что содержит все признаки классической торговли людьми, дополненной цифровым инструментарием совершения преступлений.

Второй кейс связан с явлением sextortion в Соединенных Штатах Америки. Согласно исследованию Latonero, охватившему порядка трех тысяч случаев, жертвы, преимущественно несовершеннолетние, подвергались цифровому шантажу с требованием предоставления интимных материалов либо денежных выплат, а отказ от выполнения указанных требований влек угрозу публикации компрометирующих данных [11, С.25-31]. Данный случай убедительно подтверждает, что контроль над персональными цифровыми данными может выступать самостоятельным и весьма эффективным инструментом принуждения.

Третий кейс охватывает практику «gold farming» в игровой индустрии, распространенную в ряде государств Азии, при которой работники трудятся по двенадцать шестнадцать часов в сутки, добывая внутриигровую валюту с целью ее последующей перепродажи, что сочетает экономическую эксплуатацию с технологической зависимостью от игровой платформы.

Четвертый кейс связан с использованием детского труда на майнинговых фермах в ряде государств Африки, в частности в Демократической Республике Конго, где, согласно журналистским расследованиям, дети привлекаются к

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

обслуживанию энергетического оборудования, обеспечивающего функционирование ферм по добыче криптовалют, что представляет собой сочетание классической эксплуатации детского труда с современной цифровой технологической средой.

Правоприменительные аспекты и вызовы:

Правоприменительная практика в сфере противодействия киберрабству сталкивается с рядом системных сложностей. Прежде всего, трансграничный характер соответствующих преступлений существенно ограничивает юрисдикцию отдельных государств, поскольку организаторы преступной деятельности, серверная инфраструктура и жертвы зачастую находятся в разных странах, что затрудняет проведение расследования и привлечение виновных к ответственности.

Кроме того, доказательная база по делам о киберрабстве, как правило, находится в цифровом формате и требует применения специализированных методов кибер криминалистики, включая анализ метаданных, блокчейн аналитику и OSINT методы сбора открытой информации, что предполагает наличие у правоохранительных органов соответствующей технической компетенции. Наконец, идентификация жертв киберрабства существенно осложнена тем обстоятельством, что многие из них не осознают себя жертвами принуждения, воспринимая свое положение как временную или вынужденную, но добровольно принятую работу.

Совет Европы рекомендует расширить сферу действия Будапештской конвенции о киберпреступности за счет включения в нее положений о киберэксплуатации [13]. Международная организация труда, в свою очередь, настаивает на разработке новых международных стандартов, учитывающих специфику цифрового принудительного труда и позволяющих государствам эффективно противодействовать данному явлению на национальном уровне [14].

Статистический обзор:

Согласно данным Международной организации труда, порядка 27,6 миллиона человек в мире находятся в условиях принудительного труда, из которых приблизительно 3,3 миллиона подвергаются эксплуатации именно через цифровые каналы [14]. При этом более 50% выявленных жертв составляют лица в возрасте от 18 до 30 лет, что свидетельствует об особой уязвимости данной возрастной группы в условиях развития цифровой экономики и активного использования ею социальных сетей и онлайн платформ занятости.

Согласно докладу Управления Организации Объединенных Наций по наркотикам и преступности, наблюдается устойчивый рост числа зарегистрированных случаев торговли людьми, сопряженных с использованием информационно коммуникационных технологий, что подтверждает

актуальность выработки специализированных правовых механизмов противодействия киберрабству [15].

Международный и национальный опыт противодействия киберрабству:

Международный опыт противодействия торговле людьми и смежным формам эксплуатации демонстрирует постепенное признание необходимости адаптации существующих правовых механизмов к цифровой среде. В частности, Интерпол развивает специализированные подразделения по борьбе с киберпреступностью, ориентированные на выявление трансграничных схем цифрового принуждения, а также осуществляет обмен оперативной информацией между правоохранительными органами государств-членов в рамках операций, направленных на пресечение деятельности скам-ферм в Юго-Восточной Азии.

Республика Узбекистан также предпринимает последовательные меры по противодействию торговле людьми и смежным формам эксплуатации. Закон Республики Узбекистан «О противодействии торговле людьми» устанавливает правовые и организационные основы предупреждения данного вида преступлений, защиты и реабилитации потерпевших, а также международного сотрудничества компетентных органов в указанной сфере. Национальные программы противодействия торговле людьми предусматривают меры по повышению информированности населения о рисках трудовой миграции, в том числе о случаях обманного вовлечения граждан в деятельность зарубежных колл-центров и скам-ферм, ставших источником значительного числа задокументированных случаев киберрабства в отношении трудовых мигрантов из государств Центральной Азии.

Представляется, что национальный опыт Узбекистана в области профилактики торговли людьми может быть эффективно дополнен специализированными механизмами противодействия именно цифровым формам эксплуатации, включая разработку методических рекомендаций для правоохранительных органов по выявлению признаков цифрового принуждения, обучение сотрудников консульских учреждений распознаванию типичных схем вербовки трудовых мигрантов через интернет-платформы, а также развитие межведомственного взаимодействия с провайдерами цифровых услуг в целях оперативного выявления и блокирования соответствующих преступных схем.

Сравнительный анализ национальных практик государств Европейского союза также представляет значительный интерес. Ряд государств-членов Европейского союза в рамках имплементации второго дополнительного протокола к Будапештской конвенции о киберпреступности предусмотрели расширенные полномочия

правоохранительных органов по трансграничному доступу к электронным доказательствам, что существенно повышает эффективность расследования преступлений, связанных с цифровой эксплуатацией [13]. Указанный опыт заслуживает внимания при разработке соответствующих механизмов на уровне национального законодательства Республики Узбекистан и иных государств Центральной Азии.

Предложения по реформированию:

На основании проведенного анализа представляется целесообразным сформулировать следующие предложения по совершенствованию правового регулирования в сфере противодействия киберрабству.

Во-первых, необходима разработка международно-правового определения киберрабства и его последующая интеграция в существующие международные конвенции, в частности в Палермский протокол и Конвенции Международной организации труда, что позволит устранить существующий пробел в квалификации цифровых форм эксплуатации [6; 5].

Во-вторых, целесообразно создание единого международного реестра киберэксплуатации, позволяющего систематизировать данные о выявленных кейсах, обеспечить обмен информацией между компетентными органами различных государств и повысить эффективность трансграничного расследования соответствующих преступлений.

В-третьих, представляется перспективным развитие института цифровых омбудсменов и независимых институтов мониторинга прав человека в цифровой среде, наделенных полномочиями по приему жалоб от потенциальных жертв киберрабства и оперативному реагированию на выявленные случаи эксплуатации.

В-четвертых, следует рассмотреть возможность возложения на цифровые платформы обязанности по проведению должной осмотрительности в отношении рисков цифровой эксплуатации пользователей, включая внедрение технических механизмов раннего выявления признаков принуждения и контроля.

В-пятых, необходимо развитие программ повышения цифровой грамотности населения, в особенности молодежи, а также разработка специализированных программ защиты и реабилитации лиц, пострадавших от киберрабства.

Наконец, особого внимания заслуживает вопрос о роли частного сектора в противодействии киберрабству. Значительная часть цифровой инфраструктуры, используемой для совершения преступлений, связанных с цифровым принуждением, включая платежные системы, мессенджеры и рекламные платформы, находится в собственности и под управлением частных компаний. В этой связи возложение на

такие компании обязанности по выявлению и пресечению подозрительной активности, а также по сотрудничеству с правоохранительными органами в рамках расследования конкретных дел представляется необходимым элементом комплексной стратегии противодействия киберрабству.

Заключение:

Проведенное исследование позволяет сделать вывод о том, что киберрабство представляет собой сложный и многоаспектный феномен, сочетающий правовые, технические и социальные измерения. Существующая международно-правовая база, разработанная преимущественно во второй половине двадцатого века, лишь опосредованно охватывает цифровые формы эксплуатации, что создает существенные пробелы в правовом регулировании данной сферы.

Для эффективного противодействия киберрабству необходим комплексный подход, включающий разработку международно-правового определения данного явления и его интеграцию в существующие конвенции, создание механизмов трансграничного расследования и цифровой криминалистики, повышение цифровой грамотности населения и разработку программ защиты потенциальных жертв, а также этическое регулирование деятельности цифровых платформ с целью исключения скрытых форм эксплуатации.

Таким образом, научная полемика вокруг феномена киберрабства стимулирует формирование новой парадигмы защиты прав человека в цифровую эпоху, требующей согласованных усилий государств, международных организаций, бизнеса и гражданского общества.

Список литературы:

1. Davidson J. Online Exploitation and Human Trafficking. Berlin: Springer, 2020. 210 p.

2. Walk Free Foundation. Global Slavery Index 2023. https://www.walkfree.org/global-slavery-index/

3. Европейская конвенция о защите прав человека и основных свобод от 4 ноября 1950 года, ст. 4. [European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, Article 4.]

4. Международный пакт о гражданских и политических правах от 16 декабря 1966 года, ст. 8. [International Covenant on Civil and Political Rights, 16 December 1966, Article 8.]

5. Конвенция Международной организации труда №29 о принудительном труде, 1930 год. [ILO Convention No. 29 concerning Forced Labour, 1930.]

6. Протокол о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее, дополняющий Конвенцию ООН против транснациональной организованной преступности (Палермский протокол), 2000 год. [Protocol to Prevent, Suppress and Punish Trafficking in

Persons, Especially Women and Children, Supplementing the United Nations Convention against Transnational Organized Crime (Palermo Protocol), 2000.]

7. Gallagher A.T. The International Law of Human Trafficking. Cambridge: Cambridge University Press, 2020. 570 p.

8. Bryant R. Critical Criminology and Digital Exploitation. London: Routledge, 2021. 240 p.

9. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019. 704 p.

10. Bales K. Understanding Modern Slavery. Berkeley: University of California Press, 2021. 260 p.

11. Latonero M. Sextortion and Digital Coercion. New York: Data and Society Research Institute, 2018. https://pubmed.ncbi.nlm.nih.gov/31789977

12. Reuters. What Are Southeast Asia's Scam Centres and Why Are They Being Dismantled? 4 March 2023. https://www.reuters.com/world/asia-pacific/what-are-southeast-asias-scam-centres-why-are-they-being-dismantled-2025-03-04/

13. Council of Europe. Second Additional Protocol to the Convention on Cybercrime, 2021. https://www.coe.int/en/web/cybercrime/second-additional-protocol

14. International Labour Organization. Global Estimates of Modern Slavery: Forced Labour and Forced Marriage. Geneva: ILO Publications, 2022. https://www.ilo.org/publications/major-publications/global-estimates-modern-slavery-forced-labour-and-forced-marriage

15. United Nations Office on Drugs and Crime. Global Report on Trafficking in Persons. Vienna: UNODC, 2022. https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf