ZAMONAVIY HUQUQSHUNOSLIKNING AKTUAL MUAMMOLARI

XVII-RESPUBLIKA ILMIY-AMALIY KONFERENSIYA

YAKUNLARI BO'YICHA ILMIY ISHLAR TO'PLAMI

Issue - 5(2025) Available at www.uznauka.uz

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ГРАЖДАНСКО-ПРАВОВОЙ ЗАЩИТЫ ОТ КИБЕРАТАК В УЗБЕКИСТАНЕ

Ёркинова Сангина Яҳё кизи

Студентка магистратуры Ташкентского государственного юридического университета по направлению «Международный арбитраж и разрешение споров»

Аннотация: *в тезисе рассматриваются особенности гражданско-правовой ответственности за ущерб, причинённый кибератаками, включая пробелы в законодательстве Узбекистана и международный опыт в данной области. Исследуются правовые подходы США и стран ЕС, механизмы компенсации и страхования цифрового вреда, а также выдвигаются предложения по адаптации отечественного законодательства к цифровым вызовам.*

Ключевые слова*: кибератаки; гражданско-правовая ответственность; цифровой вред; Узбекистан; компенсация ущерба; персональные данные; кибербезопасность; цифровые доказательства.*

PROBLEMS AND PROSPECTS OF DEVELOPMENT OF CIVIL LEGAL PROTECTION AGAINST CYBER-ATTACKS IN UZBEKISTAN

Yorkinova Sangina Yahyo kizi

Master's student of Tashkent State University of Law in the direction of "International arbitration and dispute resolution"

Abstract: *the thesis examines the features of civil liability for damage caused by cyber-attacks, including gaps in the legislation of Uzbekistan and international experience in this area. The legal approaches of the USA and EU countries, mechanisms for compensation and insurance of digital harm are studied, and proposals are put forward for adapting domestic legislation to digital challenges.*

Keywords: *cyber-attacks; civil liability; digital harm; Uzbekistan; compensation for damage; personal data; cybersecurity; digital evidence.*

В современную эпоху цифровизации информационные технологии стали неотъемлемой частью повседневной жизни, а киберпространство – полем как для инноваций, так и для угроз. Одной из наиболее серьёзных проблем, с которыми сталкивается глобальное сообщество, являются умышленные действия, направленные на нарушение конфиденциальности, целостности и доступности данных. Эти атаки могут быть нацелены как на государственные институты, так и на частные компании или отдельных граждан, причиняя вред имуществу, репутации и правам личности.

По мере роста зависимости общества от цифровых инфраструктур усиливается и уязвимость этих систем. Атаки могут парализовать работу государственных порталов, вывести из строя банковские системы или спровоцировать утечку персональных данных. При этом жертвы таких атак сталкиваются с трудностями получения компенсации, особенно в правовых системах, где нормы о гражданско-правовой ответственности не учитывают специфику цифрового вреда. Учитывая трансграничный характер киберпреступлений и техническую сложность их расследования, возникает насущная необходимость адаптировать гражданское законодательство к реалиям цифровой эпохи.

Одной из центральных проблем в этой сфере является отсутствие эффективных механизмов гражданско-правового возмещения ущерба, причинённого в результате кибератак. В отличие от уголовного преследования хакеров, которое часто осложняется трансграничностью и

анонимностью нарушителей, гражданское право должно обеспечивать защиту интересов пострадавших и восстановление их нарушенных имущественных и неимущественных прав. Однако действующая система законодательства во многих странах, включая Республику Узбекистан, пока не предлагает комплексного и действенного инструментария для таких случаев. Возмещение вреда в гражданском праве основывается на статье 985 Гражданского кодекса Республики Узбекистан. Однако нормы о компенсации не адаптированы к специфике цифрового вреда, где затруднено установление причинителя, оценка ущерба и причинно-следственной связи. В Законе «О кибербезопасности»[1] отсутствует регламентация гражданской ответственности, а нормы о защите персональных данных носят фрагментарный характер. Это существенно ограничивает возможности потерпевших лиц в получении компенсации.

На этом фоне интерес представляет международный опыт. В США широко используются коллективные иски (class actions), а также модели киберстрахования. Известное дело ‘Equifax breach’ продемонстрировало возможность компенсации нематериального вреда миллионам пострадавших. **В ЕС** действует статья 82 GDPR, гарантирующая **компенсацию вреда от утечек данных**. Судебная практика ЕС допускает как моральный, так и материальный ущерб, а также возлагает ответственность на операторов данных, не обеспечивших должную защиту.

Ключевой проблемой в киберделиктах остаётся **доказательство**. Часто невозможно определить конкретного виновника, особенно если атака

[1] Закон Республики Узбекистан от 15.04.2022 г. № ЗРУ–764 «О кибербезопасности» // Эл. ресурс: https://lex.uz/docs/5960609.

осуществлена анонимно или трансгранично. В таких случаях международная доктрина предлагает презумпции вины организаций, владеющих данными. Кроме того, в ряде стран учитывается соблюдение ИТ-стандартов безопасности (например, ISO/IEC 27001) как критерий добросовестности.

В условиях растущих киберугроз Узбекистан предпринимает шаги к совершенствованию нормативного регулирования. Показательно, что в апреле 2025 года в Узбекистане принято Постановление Президента Республики Узбекистан **«О мерах, направленных на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий»**[2], усиливающий ответственность за киберпреступления. Согласно постановлению, банки и платёжные организации, не обеспечившие должный уровень защиты, обязаны компенсировать причинённый кибератакой материальный ущерб. Более того, за предоставление своих карт или SIM-карт мошенникам граждане могут нести административную и уголовную ответственность. Также предусмотрено развитие механизмов раннего выявления финансовых махинаций, в том числе с использованием цифровых инструментов мониторинга. Это свидетельствует о переходе к концепции распределённой ответственности и усилении превентивных мер защиты цифровых прав.

Ещё одним из ключевых барьеров для эффективной реализации гражданско-правовой ответственности за кибератаки является **сложность**

[2] Постановление Президента Республики Узбекистан от 30.04.2025 г. № ПП-153 «О мерах, направленных на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий» // Эл. ресурс: https://lex.uz/docs/7511168.

доказывания цифрового вреда. Это обусловлено как техническими, так и правовыми факторами, ограничивающими возможности потерпевших.

Во-первых, затруднён процесс **идентификации источника вреда**. Хакерские атаки часто осуществляются с использованием цепочек прокси-серверов, анонимных сетей (Tor, VPN), заражённых устройств третьих лиц (botnet) и поддельных доменов, что усложняет установление причинителя вреда (ответчика). В такой ситуации традиционная модель ответственности, базирующаяся на принципе индивидуализации ответчика, становится малоприменимой.

Во-вторых, в делах о цифровом вреде возникает трудность в **установлении причинно-следственной связи** между действием нарушителя и наступившим ущербом. Часто невозможно доказать, что именно конкретная атака привела к утечке данных или нарушению права. Особенно это характерно для так называемых «цепных атак», где вред возникает как совокупный результат нескольких связанных инцидентов.

В-третьих, остро стоит проблема **определения размера ущерба**, особенно нематериального. Утрата контроля над личными данными, вторжение в частную жизнь, стресс, утрата деловой репутации – всё это трудно поддаётся точной денежной оценке. В мировой практике (например, дела ‘Lloyd v Google’ в Великобритании и ‘Schrems v Facebook’ в ЕС) суды всё чаще признают сам факт утечки персональных данных как достаточный для компенсации морального вреда, даже при отсутствии прямых финансовых потерь.

Кроме того, в гражданском процессе до сих пор отсутствует полноценный правовой **режим обращения с цифровыми доказательствами**, особенно полученными с помощью технической экспертизы, логов, скриншотов, аудита серверов и систем. Недостаточная цифровая грамотность участников процесса, в том числе судей и адвокатов, также снижает эффективность защиты пострадавших.

Таким образом, обеспечение действенного доказывания цифрового вреда требует как институциональных реформ, так и внедрения специальных процессуальных норм, учитывающих специфику кибератак и цифровых технологий.

Исходя из вышеизложенного, для повышения эффективности гражданско-правовой защиты пострадавших от кибератак в Узбекистане целесообразно обеспечить формирование комплексного подхода, который охватывает как материально-правовые нормы, так и процессуальные механизмы. В частности, необходимо внести дополнения в Гражданский кодекс Республики Узбекистан, чётко закрепив положения о деликтной ответственности за причинение цифрового вреда, включая как материальный, так и моральный ущерб, возникший в результате кибератак, утечек персональных данных или вмешательства в частную жизнь. В настоящее время правовая конструкция вреда, причинённого кибердействиями, в национальном законодательстве остаётся не до конца определённой, что создаёт правовую неопределённость и препятствует компенсации пострадавшим.

Следующим шагом должно стать установление обязательных стандартов киберзащиты для операторов персональных данных и критической цифровой инфраструктуры. Это включает внедрение систем сертификации информационных технологий, проведение регулярных аудитов на предмет информационной безопасности, а также установление ответственности за несоблюдение минимальных технических и организационных требований. Подобная практика уже реализована, например, в рамках Регламента GDPR в Европейском союзе, где операторы несут ответственность за недостаточную защиту данных.

Кроме того, с целью финансовой устойчивости и защиты интересов граждан, необходимо законодательно внедрить механизмы обязательного киберстрахования для ключевых отраслей, таких как финансовые учреждения, телекоммуникационные компании, государственные информационные системы и поставщики электронных услуг. Это позволит застраховать риски, связанные с нарушением конфиденциальности, доступности и целостности данных, а также обеспечить компенсацию ущерба в случаях массовых инцидентов.

Не менее важным направлением является упрощение порядка принятия и оценки цифровых доказательств в гражданском судопроизводстве. Следует признать допустимыми электронные документы, отчёты логов, технические заключения IT-специалистов и материалы, зафиксированные с помощью автоматизированных средств. Для этого потребуется адаптировать нормы Гражданского процессуального кодекса, в частности, касающиеся письменных доказательств и заключений экспертов.

Наконец, необходимо разработать процессуальные нормы, обеспечивающие возможность коллективной защиты прав пострадавших от кибератак – например, через внедрение института групповых исков (class actions). Это особенно актуально в ситуациях, когда вред причиняется массово – как в случаях утечек баз данных или атак на цифровую экосистему государственного уровня. Такие механизмы успешно используются в США, Канаде и отдельных странах Европы, способствуя не только восстановлению нарушенных прав, но и превентивному воздействию на операторов.

Таким образом, развитие цифрового права требует комплексного подхода к регулированию ущерба от кибератак, основанного на лучших международных практиках и адаптированного к национальной правовой системе. Применение международных подходов и активизация внутренней реформы позволят Республике Узбекистан эффективно защищать интересы граждан и бизнеса в цифровой среде, формируя справедливую модель ответственности в условиях технологической трансформации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Гражданский кодекс Республики Узбекистан.
2. Закон Республики Узбекистан «О кибербезопасности».
3. Regulation (EU) 2016/679 (General Data Protection Regulation), Art. 82.

4. Studer E., de Werra J. Civil Liability in Case of Cyber-Attacks. Expert Focus, 2017.

5. Walton B. Low-Intensity Cyber Attacks and Liability. Yale Law Journal, 2018.

6. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. NATO, 2017.

7. Equifax Case Materials, US Federal Trade Commission Reports.

8. ISO/IEC 27001:2022 Information Security Management Systems.

9. UN GGE Reports on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021.