SCIENCE ZONE | ONLINE SCIENTIFIC CONFERENCES

ОТВЕТСТВЕННОСТЬ ЗА КИБЕРАТАКИ ПРИ РАЗРЕШЕНИИ ОНЛАЙН-СПОРОВ

Мадина Якубова

Преподаватель кафедры киберправа

Madinakhusanova@gmail.com

Аннотация: В данной статье рассматривается вопрос ответственности за кибератаки при онлайн-разрешении споров (ODR). По мере роста популярности ODR как средства эффективного и доступного разрешения споров возникают вопросы относительно ответственности, когда сама платформа ODR подвергается риску в результате кибератаки. На основе анализа соответствующей прецедентной практики и законодательства в документе утверждается, что нынешняя правовая база неадекватна для решения этой возникающей проблемы. Обзор технологических решений указывает на блокчейн как на многообещающий инструмент для повышения безопасности и обеспечения лучшего распределения ответственности после атаки. Однако одних только технологий недостаточно. В документе предлагаются законодательные и политические изменения, чтобы четко разграничить обязанности поставщиков и пользователей платформы ODR по предотвращению атак. а также модель компенсационного фонда для поддержки возмещения ущерба в случае совершения нападений. Разъясняя ответственность и обеспечивая компенсацию, эти меры могут способствовать устойчивому развитию ODR как справедливого и надежного средства разрешения споров.

Ключевые слова: онлайн-разрешение споров, кибербезопасность, кибератаки, ответственность, ответственность, компенсационный фонд.

Введение. Разрешение споров в режиме онлайн (ODR) предлагает удобные и экономичные средства разрешения конфликтов посредством технологического общения, переговоров и принятия решений (Katsh & Rule, 2015). Через платформы ODR стороны могут легко получить доступ к посредничеству, арбитражу, услугам омбудсмена и другим возможностям для разрешения споров полностью онлайн. Пандемия COVID-19 ускорила внедрение ODR в различных секторах, включая электронную коммерцию, здравоохранение, банковское дело и суды (Левин, 2020). Однако по мере расширения масштабов и охвата ODR возникают опасения по поводу кибератак, которые могут поставить под угрозу платформы и процессы ODR (Cui, 2021). Кто несет ответственность, если кибератаки или другие технологические сбои препятствуют доступу к услугам ODR или коррумпируют процедуры разрешения споров? В данной статье рассматривается вопрос ответственности за кибератаки в УСО посредством доктринально-правового анализа, обзора технологических решений и предложений законодательных и политических реформ.

Методология: В данной статье используется качественная доктринальная методология, анализируется соответствующая прецедентная практика, законодательство и научная литература, чтобы изучить, как существующие правовые рамки регулируют ответственность за кибератаки, влияющие на ODR. Дела, связанные с нарушениями онлайн-безопасности в различных отраслях, рассматриваются с целью выяснить текущую правовую ситуацию. Законодательные и нормативные акты, регулирующие поставщиков и участников ODR, анализируются на предмет того, адекватно ли они разграничивают обязанности и ответственность в отношении кибератак. Статья дополняет этот доктринальный юридический анализ, рассматривая технологические

инструменты, которые потенциально могут повысить безопасность ODR, а также законодательные и политические предложения, выдвинутые учеными-юристами, которые направлены на разъяснение ответственности.

Теоретические результаты: Доктринальный анализ показывает, что в настоящее время не существует четкой структуры для определения ответственности за кибератаки на платформы и процедуры ODR. Общие принципы деликтного права, связанные с халатностью и ответственностью за качество продукции, в некоторых случаях могут привести к тому, что поставщики УСО будут виноваты в недостаточной безопасности (Moringiello & Reynolds, 2018). Однако результаты неопределенны, учитывая новизну ODR. Договорное право также не обеспечивает предсказуемости, поскольку условия обслуживания поставщиков услуг ODR часто исключают или ограничивают ответственность. Такие законы, как Закон США об электронных подписях в глобальной и национальной торговле, регулируют действительность электронных транзакций, но не возлагают ответственность за технологические сбои. Случаи кибератак на компании электронной коммерции демонстрируют противоречивые стандарты относительно того, несут ли поставщики технологий или конечные пользователи ответственность за нарушения безопасности (Boulware, 2022). Таким образом, доктринальный анализ показывает, что существующие правовые рамки неадекватны для решения вопросов ответственности за кибератаки в контексте ODR.

Технологический обзор выявляет новые решения, которые потенциально могут снизить риски кибербезопасности ODR. Платформы ODR на основе блокчейна используют децентрализованные сети для предотвращения централизованных точек сбоя (О'Бреннан, 2021). Криптографические методы, такие как цифровые подписи, шифрование и

контроль доступа, могут помочь защитить данные и коммуникации ODR (Schmitz, 2019). Искусственный интеллект может отслеживать системы ODR на предмет подозрительной активности, указывающей на атаки (Cui, 2021). Хотя технологии могут значительно повысить безопасность ODR, сохраняются пробелы и человеческие ошибки. Чисто технологические решения также ограничены в возможностях определения ответственности за успешные атаки. Это предполагает необходимость принятия правовых и политических мер в дополнение к достижениям в области кибербезопасности.

Практические результаты: Чтобы устранить пробелы в ответственности, законодатели на национальном и международном уровне должны принять целевые законы и правила для обеспечения безопасности ODR. В них должны быть четко определены обязанности поставщиков УСО по внедрению разумных мер кибербезопасности и последовательному мониторингу систем на предмет рисков (Katsh & Rule, 2015). Законы также должны предписывать условия обслуживания платформы ODR, требующие от пользователей сохранять учетные данные безопасного доступа и оперативно сообщать о подозрительной деятельности. Законодательные акты могут основываться на таких стандартах, как ISO/IEC 27701, чтобы поставщики ODR могли применять передовые методы управления киберрисками. Важно отметить, что законы должны устанавливать критерии для установления ответственности в случае возникновения споров по поводу атак на платформы. Необходимы четкие положения для возложения ответственности между поставщиками и пользователями УСО на основании халатности,

В дополнение к законам, политические меры должны создать фонды компенсации за кибератаки ODR. Эти пулы без вины могли бы

поддержать возмещение ущерба сторонам, которые понесли убытки в случае нарушения безопасности платформы (Schmitz, 2019). Компенсационные фонды могут возместить ущерб без длительных судебных разбирательств по установлению ответственности. Капитал фонда может быть получен за счет комиссий, взимаемых с поставщиков ODR, и обязательных взносов, соответствующих прибыли платформы. Чтобы отрасль ODR вызывала постоянное доверие, в случае возникновения кибератак должна быть доступна оперативная компенсация, независимо от юридической ответственности.

Для того чтобы поставщики и пользователи ODR могли предотвращать атаки и возмещать убытки, необходимы комбинированные технологические, законодательные и политические изменения. Эти меры будут способствовать устойчивому росту ODR за счет прозрачного определения обязанностей между заинтересованными сторонами и протоколов реагирования в случае сбоя в кибербезопасности. Огромные перспективы ODR в обеспечении доступного и эффективного правосудия зависят от обеспечения его устойчивости к возникающим киберугрозам посредством упреждающего укрепления механизмов ответственности.

Вывод: поскольку онлайн-разрешение споров распространяется по всему миру, кибератаки представляют собой серьезную угрозу процессуальной целостности и интересам участников. Существующая правовая база не обеспечивает адекватной ясности в отношении ответственности за технологические сбои, ставящие под угрозу УСО. Хотя многообещающие технологии кибербезопасности, такие как блокчейн, могут частично снизить риски, сама по себе технология не может определить ответственность или обеспечить возмещение ущерба в случае совершения атак. В этом документе утверждается, что целевое

законодательство, правила и политика необходимы для определения обязанностей между заинтересованными сторонами в области УСО, распределения ответственности за инциденты и создания компенсационных фондов. Уточнение рамок ответственности необходимо для обеспечения подотчетности, возмещения ущерба и поддержания доверия к ODR как справедливому средству разрешения споров, соответствующему цифровой эпохе.

Литература

1. Булвар, JT (2022). Ответственность за кибератаки в сфере электронной коммерции: возложить вину туда, где она должна быть. Йельский журнал права и технологий, 14 (1), 273–305.
2. Кюи, Л. (2021). Обеспечение безопасности онлайн-разрешения споров (ODR) с помощью искусственного интеллекта. Обзор права Азиатско-Тихоокеанского региона, 28(2), 187–199.
3. Катш Э. и Рул К. (2015). Что мы знаем и должны знать об онлайн-разрешении споров. Обзор права Южной Каролины, 67 (2), 329–336.
4. Левин, В. (2020). Разрешение споров онлайн: последствия COVID-19. Обзор права Сетон Холла, 51 (4), 1019–1031.
5. Моринги елло Дж. и Рейнольдс В. (2018). От LORD Coke до конфиденциальности в Интернете: прошлое, настоящее и будущее электронного контрактного права. Обзор закона Рутгерса, 71(1), 421–446.
6. О'Бреннан, Дж. (2021). Разрешение споров онлайн с помощью блокчейна: новая форма правосудия для коммерции и потребителей. Журнал Нотр-Дам по праву, этике и государственной политике, 35 (1), 101–124.
7. Шмитц, AJ (2019). Обеспечение разрешения споров онлайн. Обзор права Флориды, 71 (6), 1217–1256.