УДК 34

КИБЕРБЕЗОПАСНОСТЬ ЦИФРОВОГО АРБИТРАЖА В РОССИИ

Маркина А.А.,[1]

Студент,

Калужский государственный университет им. К.Э. Циолковского

Калуга, Россия

Русяев М.С.,

Студент,

Калужский государственный университет им. К.Э. Циолковского

Калуга, Россия

Аннотация: статья посвящена актуальным вопросам кибербезопасности в условиях цифровизации арбитражного процесса в Российской Федерации. Авторы анализируют вызовы, связанные с возрастанием числа кибератак, и их потенциальное влияние на конфиденциальность споров, целостность данных и доверие к институту арбитража. В работе рассматривается определение информационной безопасности согласно Доктрине РФ и подчеркивается особое значение защиты конфиденциальных сведений в арбитражном разбирательстве, в том числе споров, связанных с интеллектуальной собственностью. Отмечается, что электронные

[1] ***Научный руководитель – Александров Андрей Юрьевич,*** к.ю.н., доцент, доцент кафедры юриспруденции Института истории и права Калужского государственного университета имени К. Э. Циолковского, Калуга, Россия

Scientific supervisor – Alexandrov Andrey Yuryevich, *PhD, Associate Professor of the Department of Jurisprudence, Institute of History and Law, Kaluga State University named after K. E. Tsiolkovsky, Kaluga, Russia*

коммуникации являются основным вектором киберугроз, и повсеместное использование незащищенных каналов связи, таких как обычная электронная почта, значительно повышает уязвимость участников процесса. Статья предлагает конкретные методы борьбы с кибератаками, включая применение сквозного шифрования, многофакторной аутентификации, современных систем мониторинга трафика, регулярного обновления ПО и использования защищенных каналов связи.

Ключевые слова: арбитражный процесс, цифровизация арбитражного процесса, электронное правосудие, кибербезопасность, информационные технологии.

CYBERSECURITY OF DIGITAL ARBITRATION IN RUSSIA

Markina A.A.,

Student,

Kaluga State University named after Prince E. N. Tsiolkovsky

Kaluga, Russia

Rusyaev M.S.,

Student,

Kaluga State University named after K.E. Tsiolkovsky

Kaluga, Russia

Annotation: The article is devoted to topical issues of cybersecurity in the context of digitalization of the arbitration process in the Russian Federation. The authors

analyze the challenges associated with the increasing number of cyber attacks and their potential impact on dispute confidentiality, data integrity, and trust in the institution of arbitration. The paper examines the definition of information security according to the Doctrine of the Russian Federation and emphasizes the special importance of protecting confidential information in arbitration proceedings, including disputes related to intellectual property. It is noted that electronic communications are the main vector of cyber threats, and the widespread use of unsecured communication channels, such as regular e-mail, significantly increases the vulnerability of participants in the process. The article suggests specific methods to combat cyber attacks, including the use of end-to-end encryption, multi-factor authentication, modern traffic monitoring systems, regular software updates, and the use of secure communication channels.

Keywords: arbitration process, digitalization of the arbitration process, electronic justice, cybersecurity, information technology.

Стремительный рост компьютерных технологий в различных сферах человеческой деятельности, с одной стороны, позволил обеспечить высокие достижения в этих сферах, а с другой стороны, стал источником самых непредсказуемых и вредных для человеческого общества последствий. Кибербезопасность остаётся ключевым вызовом для цифрового арбитража, учитывая конфиденциальность рассматриваемых споров. Недостаточность правовых гарантий защиты данных усиливает уязвимость участников процесса. Эти факторы требуют пересмотра традиционных процессуальных подходов в условиях цифровой среды.

В Доктрине информационной безопасности Российской Федерации дается определение информационной безопасности. Под информационной

безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [1].

Арбитражное разбирательство по традиции ценится за высокий уровень конфиденциальности, который позволяет сторонам защищать коммерческую тайну и деловую информацию от публичного распространения. Тем не менее, в современном цифровом поле, когда кибератаки становятся все более распространенными, арбитраж представляет собой площадку для возможного кибернападения. Обмен закрытой информацией в ходе арбитражного процесса, в случае утечки, может привести к существенному коммерческому ущербу, повлиять на рыночную стоимость акций, корпоративные стратегии и даже государственную политику. Особенно уязвимы в этом отношении споры, связанные с интеллектуальной собственностью, поскольку информация о таких объектах имеет решающее значение в условиях конкуренции [2, с.469]. Цифровая среда арбитражного процесса создает уникальные риски несанкционированного доступа к конфиденциальным данным участников. Уязвимости в информационных системах могут быть использованы злоумышленниками для хищения персональных данных, коммерческой тайны и иных охраняемых сведений. Особую опасность представляют атаки на каналы передачи электронных документов и базы данных арбитражных учреждений. Реализация таких угроз способна оказать влияние на уровень доверие к институту цифрового арбитража в целом. Последствия утечки конфиденциальной информации в арбитражном процессе могут носить системный характер. Компрометация полученных в ходе кибератаки данных ставит под угрозу принципы равенства сторон и справедливого

разбирательства. Кроме того, нарушения безопасности могут повлечь юридическую ответственность арбитражных учреждений согласно законодательству о защите персональных данных. Это обуславливает необходимость разработки многоуровневых механизмов защиты на всех этапах судопроизводства.

Основными векторами распространения киберугроз в арбитраже являются электронные коммуникации. Юристы и клиенты часто обмениваются информацией, обсуждают стратегии и передают доказательства, заключения экспертов и свидетельские показания по электронной почте [3, с.47]. Подготовка документов нередко производится на электронных платформах, принадлежащих сторонним дата-провайдерам. Снижение рисков кибератак и сохранение конфиденциальности требуют понимания угроз и принятия соответствующих мер. Каждый участник арбитражного процесса, имеющий доступ к информации, должен неукоснительно соблюдать политику безопасности. Ответственность за безопасность ложится не только на IT-отделы, но и на каждого сотрудника [4, с.90]. Несмотря на это, суды нередко продолжают использовать незащищенные почтовые сервисы. Даже в условиях многомиллионных исков адвокаты и стороны споров зачастую пренебрегают безопасными каналами связи, используя обычную электронную почту. Электронная почта, будучи одним из наиболее популярных средств коммуникации, не является безопасным каналом. История интернета помнит времена, когда информация передавалась в открытом виде. Несмотря на развитие технологий шифрования и систем паролей, каждое письмо проходит через множество серверов и сетей, каждая из которых представляет собой потенциальную уязвимость. Хакер, получивший доступ к одному из таких узлов, может перехватить или даже модифицировать электронную корреспонденцию.

Примером небезопасности электронной почты служит вирус Petya, распространившийся в 2017 году через фишинговые письма, что продемонстрировало уязвимость пользователей перед мошенническими схемами. Наиболее актуальными методами борьбы с кибератаками, совершаемыми по электронной почте можно назвать использование специализированных облачных платформ, разработанных с учетом требований безопасности для юридической сферы, с надежным шифрованием и контролем несанкционированного доступа. Не менее важно повышение квалификации участников арбитражного судопроизводства основам кибербезопасности, методам распознавания фишинга, социальной инженерии, другим угрозам.

В цифровом арбитраже наиболее применимы следующие принципы кибербезопасности: конфиденциальность (защита информации от несанкционированного доступа), целостность (обеспечение защиты информации от несанкционированного изменения или удаления), доступность (обеспечение доступа авторизованным пользователям в любое время), прослеживаемость (возможность отследить изменения документа). Как следствие, можно предложить законодательно закрепить следующие методы борьбы с кибератаками в цифровом арбитраже: применение сквозного шифрования для всех каналов передачи данных (в т.ч. электронная почта, системы видеоконференцсвязи, платформы для обмена документами), многофакторная аутентификация, использование современных систем мониторинга трафика для обнаружения и предотвращения несанкционированных вторжений, регулярное обновление программного обеспечения и использование защищенных каналов связи. С точки зрения организационных и процессуальных мер наиболее актуальными выступают разработка четких регламентов и политики информационной безопасности,

проведение регулярных аудитов безопасности и тестирования на проникновение (с привлечением сторонних экспертов), сертификация и аккредитация используемых в цифровом арбитраже платформ с целью проверки на соответствие стандартам безопасности.

Таким образом, вопросы кибербезопасности и защиты конфиденциальных данных приобретают первостепенное значение. Несанкционированный доступ к информации, утечки и атаки могут не только нанести ущерб отдельным участникам процесса, но и подорвать доверие к судебной системе в целом. Требуется создание многоуровневых систем защиты, гармонизация национальных и международных стандартов, а также постоянное совершенствование мер безопасности в ответ на развивающиеся угрозы. Только комплексный и проактивный подход позволит в полной мере реализовать потенциал цифровизации, минимизировав при этом сопутствующие риски и обеспечив подлинное торжество правосудия в цифровую эпоху. Обеспечение соответствия систем цифрового арбитража наивысшим стандартам информационной безопасности представляет собой сложную задачу. Разнообразие нормативных требований, требует адаптации платформ под конкретные юрисдикции. Некоторое несовершенство национальных законодательств в части регулирования кибербезопасности усложняет унификацию защитных мер. При этом отсутствие единых подходов к сертификации арбитражных платформ снижает эффективность сотрудничества. Ключевой проблемой остается гармонизация технических и организационных мер защиты информации с процессуальными нормами. Внедрение сквозного шифрования и многофакторной аутентификации часто конфликтует с требованиями доступности правосудия. Необходимость обеспечения прозрачности процедур затрудняет применение закрытых криптографических протоколов.

Библиографический список

1. Доктрина информационной безопасности Российской Федерации / [Электронный ресурс] // МИД России : [сайт]. — URL: https://www.mid.ru/ru/foreign_policy/official_documents/1539546/ (дата обращения: 30.03.2026).

2. Kupchina, E. IP Dispute resolution thought International Commercial Arbitration: US experience / E. Kupchina, O. Kuznetsova, K. Chilingaryan // Proceedings of INTCESS 2019 - 6th International Conference on Education and Social Sciences, 46 February 2019, Dubai, U.A.E. - Dubai, 2019. -P. 468-472.

3. Курышова, Я. С. Интеллектуальная собственность и кибератаки. Интеллектуальная собственность: от надежной защиты к эффективному управлению : сб. ст. XI Междунар. науч.-практ. конф., г. Екатеринбург, 30-31 октября 2015 г. / Я. С. Курышова. - Екатеринбург : Изд-во Урал. гос. экон. ун-та, 2015. - 99 с.

4. Inshakova, A. O. Classification criteria: defending the specific features of corporate conflicts / A. O. Inshakova, V. V. Dolinskaya, E. E. Frolova // "Conflict-Free" Socio-Economic Systems: Perspectives and Contradictions Bingley. - West Yorkshire, 2019. -P. 89-99.