Дата поступления рукописи в редакцию: 10.07.2026 г. DOI: 10.24412/2224-9133-2026-7-120-124
Дата принятия рукописи в печать: 31.07.2026 г.

АББУД Руслан Ратебович,
к.ю.н., старший преподаватель кафедры международного права Российского государственного университета правосудия имени В.М. Лебедева (г. Москва),
e-mail: ruslan625@yandex.ru

КИБЕРПРЕСТУПЛЕНИЯ В РАМКАХ МЕЖДУНАРОДНОГО КОММЕРЧЕСКОГО АРБИТРАЖА И СПОСОБЫ ИХ ПРЕДОТВРАЩЕНИЯ

Аннотация. *В настоящей статье автором анализируются отдельные виды киберпреступлений, способных нанести вред в контексте одной из процессуальных отраслей международного частного права – международный коммерческий арбитраж. Более того, киберпреступления могут нанести ущерб таким важным аспектам данного института, как конфиденциальность, беспристрастность и исполнимость решений. Скоротечное развитие цифровизации провоцирует новый всплеск кибератак в отношении международных третейских судов. Кроме того, с развитием систем ИИ, появилось такое киберпреступление, как модификация цифровых доказательств, что может сказаться крайне негативно на вынесение справедливого решения арбитром. Принятие своевременных мер защиты в данной сфере даст определенный толчок в части обеспечения должной информационной безопасности в части отправления правосудия.*

Статья состоит из трех разделов, включая аннотацию и заключение. Второй раздел посвящен анализу судебной практики в части совершения киберпреступлений в ходе процесса в международном коммерческом арбитраже и какими международно-правовыми механизмами, а также техническими средствами возможно предотвратить вышеназванную угрозу.

Ключевые слова: *киберпреступление, международный коммерческий арбитраж, системы ИИ, Нью-Йорская конвенция 1958 года, Руководство по использованию ИИ в международном арбитраже (2024).*

ABBUD R.R.,
PhD in law, Senior Lecturer Professor of the International Law Department at the Lebedev Russian State University of Justice (Moscow)

CYBERCRIMES IN THE FRAMEWORK OF INTERNATIONAL COMMERCIAL ARBITRATION AND WAYS TO PREVENT THEM

Annotation. *In this article, the author analyzes certain types of cybercrimes that can cause harm in the context of one of the procedural branches of private international law – international commercial arbitration. Moreover, cybercrimes can damage such important aspects of this institution as confidentiality, impartiality and enforceability of decisions. The rapid development of digitalization is provoking a new surge in cyber-attacks against arbitration courts. In addition, with the development of AI systems, cybercrime such as manipulation of digital evidence has appeared, which can have a very negative impact on the fair decision of the arbitrator. Taking timely protective measures in this area will give a definite boost in terms of ensuring proper information security.*

The article consists of three sections, including an abstract and a conclusion. The second section is devoted to the analysis of judicial practice regarding the commission of cybercrimes during the process in

international commercial arbitration and what international legal mechanisms, as well as AI systems, it is possible to prevent the above-mentioned threat.

Key words: *cybercrime, international commercial arbitration, AI systems, the 1958 New York Convention, Guidelines on the Use of AI in International Arbitration (2024).*

I.Киберпреступления в контексте международного арбитражного производства

В международном праве киберпреступление является преступлением международного характера, которое посягает как на внутригосударственный, так и на международный правопорядок. В узком смысле под киберпреступлением понимается любое противоправное деяние, осуществляемое посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных. Киберпреступление в широком смысле означает любое противоправное деяние, совершаемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное хранение, распространение информации посредством компьютерной системы или сети [7].

В эпоху стремительной цифровизации и развития сети «Интернет, практически не осталось той сферы, где киберпреступления не заявили о себе. По данным Международного союза электросвязи, текущий уровень киберугроз оценивается приблизительно в 2200 кибератак в мире ежедневно, при этом ежегодно количество кибератак в мире увеличивается на 80%. Схожие данные приводит и Роскомнадзор, указывая на то, что число компьютерных и DDoS-атак ежегодно увеличивается в среднем на 70%. Одной из самых массовых областей, по которой бьют киберпреступления – это экономический и финансовый сектор. Более того, кибератаки часто совершаются в отношении интеллектуальной собственности, а также на системы управления объектами жизнеобеспечения.

Судебная система также не является абсолютно защищенной и сохраняется риск представления поддельных доказательств в судах и арбитражах.

В деле «Libananco v. Turkey» истец ссылался на то, что Турция перехватывала корреспонденцию по электронной почте между кипрской компанией Libananco и адвокатом [4]. Турция получила доступ к документам, защищенным адвокатской тайной, после чего представила их в арбитраж. Однако, несмотря на обвинение кипрской компанией турецких властей в части незаконного перехвата конфиденциальной информации, Международный центр по урегулированию инвестиционных споров (далее – МЦУИС) в своем итоговом решении от 2 сентября 2011 года встал на позицию Турции, заявив, что прямой ущерб процессу не был доказан. В то же время МЦУИС подчеркнул, что несанкционированный перехват информации является нарушением процессуальной этики.

Таким образом, анализируя вышеназванный кейс, можно прийти к выводу о том, что совершение одной из сторон спора киберпреступления не влечет автоматического проигрыша, однако требует от арбитров внимательности в части обеспечения надлежащего процесса. В эпоху резкого развития информационных технологий, в международном коммерческом арбитраже представляется целесообразным закрепления «презумпции недопустимости» доказательств, полученных нелегитимным путем. Своевременный анализ системами ИИ цифровых следов позволит выявить фальсификацию документов. Более того, грамотное интегрирование систем ИИ в международное арбитражное производство позволит обеспечить достоверность доказательной базы, если идти по пути генерируя механизмов объективного контроля, способных предотвратить последствия киберпреступлений.

Еще одним ярким примером, где продемонстрировано совершение киберпреступления в отношении международного коммерческого арбитража служит кейс Sultan of Sulu v. Malaysia [5]. Спор проистекает из соглашения 1878 года между британскими колонистами и султаном Сулу об использовании принадлежащей ему территории на острове Борнео. В мае 2019 года Верховный суд Испании назначил на рассмотрение спора испанского арбитра Гонсало Стампа. В феврале 2022 года Стампа признал право наследников султана Сулу взыскать с Малайзии стоимость прав на территорию Северного Борнео, которая стала предметом территориальных уступок. Наследники должны были получить 14,92 млрд долларов. После такого решения Малайзия выдвинула против Стампы обвинение в превышении должностных полномочий.

Анализируя вышеназванное дело, действия арбитра можно квалифицировать, как мошенничество с использованием информационно-коммуникационной системы. Стампа эксплуатировал отсутствие синхронизации между цифровыми реестрами национальных судов Европейского союза (Испания, Франция). Выдав аннулированное решение за легитимное, он совершил киберпреступление против системы международного правосудия.

В эпоху активной цифровизации подобные

киберпреступления могут быть автоматизированы, что требует интегрирования технологий блокчейн-верификации в части каждого этапа арбитражного процесса, чтобы обеспечить надлежащую безопасность. Более того, если бы назначение арбитра фиксировалось в блокчейне, связанном с реестрами национальных судов, то в момент отстранения Стампы, в Мадриде, его цифровой ключ был бы автоматически отозван. Любое решение, подписанное арбитром после этого, системами помечалось – как недействительное.

Тем не менее, на сегодняшний день ведется дискуссия в части создания единой глобальной базы данных арбитражных решений. Суть заключается в следующем, что суд любого государства при получении требования об исполнении арбитражного решения должен иметь возможность зайти в защищенную базу данных и увидеть статус этого решения: «действует», «аннулировано», «оспорено». Это позволит исключить возможность обмана.

В деле Nigeria vs. P&ID Высокий суд Лондона постановил, что решение, которое было вынесено ранее в пользу компании P&ID должно быть аннулировано, так как противоречит публичному порядку [6]. В ходе рассмотрения дела выяснилось, что P&ID незаконно получала доступ к конфиденциальным цифровым данным Нигерии. Суд постановил, что незаконное получение доступа к конфиденциальным цифровым материалам другой стороны в деле является весомым аргументом в части отмены арбитражного решения. В контексте киберпреступлений данный кейс подтверждает, что любая форма несанкционированного завладения данными рассматривается судами как посягательство на публичный порядок, что делает окончательное решение в ходе арбитражного процесса юридически ничтожным.

В апреле 2024 года Центр арбитража и медиации Кремниевой долины опубликовал руководство по использованию ИИ в международном арбитраже (далее – Руководство ИИ) [2]. Данный документ предназначен для поддержки арбитражным институтов, арбитров, сторон и их представителей при использовании инструментов ИИ. Кроме того, Руководство ИИ устанавливает этические и процессуальные рамки применения ИИ. Главная его роль – минимизировать риски, сохраняя при этом эффективность арбитража. Руководство ИИ выполняет функцию soft law и является рекомендацией и ориентиром для международных коммерческих арбитражных судов. Более того, Руководство ИИ формирует новые требования к допустимости доказательств, а также устанавливает этический барьер против использования систем ИИ в качестве инструмента для киберпреступления, например генерирование фальшивых прецедентов или улик.

Таким образом, принятие Руководства ИИ стало значимым событием в области международного арбитражного производства. Устанавливая обязательство по обеспечению кибербезопасности при работе с системами ИИ и вводя запрет на делегирование полномочий арбитра алгоритмам систем ИИ, вышеназванный документ закладывает фундамент для защиты надлежащей правовой процедуры. Обязанность раскрытия использования систем ИИ, предусмотренная статьей 3 Руководством ИИ, выступает эффективным превентивным инструментом в отношении использования генеративных технологий в части дальнейшей фальсификации доказательств, тем самым обеспечивая целостность и легитимность арбитражного решения в условиях новых технологических вызовов.

Более того, к числу рекомендательных документов можно отнести Протокол о кибербезопасности в международном арбитраже (ICCA-NYC BAR-CPR Cybersecurity Protocol for International Arbitration) [3]. Данный Протокол содержит руководство по принятию мер, направленных на обеспечение информационной безопасности, которые стороны и арбитры могут принять при проведении виртуальных слушаний и подаче документов в электронном виде.

Оба документа носят рекомендательный характер, однако их принятие, безусловно, повышает уровень осведомленности участников арбитража и ставит вопросы справедливого и безопасного разрешения споров в центр внимания [8].

Кроме того, несмотря на свою историческую значимость, Нью-Йорская конвенция 1958 года о признании и приведении в исполнение иностранных арбитражных решений (далее – Нью-Йорская конвенция) демонстрирует технологическую слепоту в эпоху цифровизации и стремительного развития систем ИИ [1]. Тем не менее, статья 5 Нью-Йорская конвенции направлена на борьбу в том числе и против киберпреступлений. В частности, речь идет о публичном порядке, когда суды используют данный инструмент в части отказа в признании решения, основанного, например, на ложных цифровых доказательствах.

Заключение

На наш взгляд, в целях минимизации злоупотреблением полномочиями арбитрами, необходимо создать единый международный цифровой реестр и обязать государственные суды своевременно вносить данные об аннулировании арбитражных решений. Кроме того, отсутствие в Нью-Йорской конвенции положений о кибербезопасности и целостности электронных доказательств создает правовой вакуум, который вынуждает национальны суды расширительно толковать оговорку о публичном порядке. Принятия дополнительного протокола к Нью-Йорской конвенции

с чёткими правилами императивного характера (введение обязательной верификации цифровых подписей арбитров через международные реестры), и дальнейшей имплементации норм в национальную правовую систему государств, приведет к минимизации кибератак на систему международного арбитражного производства. А пока, главную роль в данной архитектуре безопасности играют нормы мягкого права, которые адаптируют классические постулаты международного частного права к цифровым вызовам современности.

Кроме того, эффективное противодействие киберпреступлениям в международном коммерческом арбитраже невозможно в рамках исключительно правового подхода. Необходима синергия: технические механизмы, например блокчейн-верификация или анализ системами ИИ цифровых доказательств позволят минимизировать риски представления поддельных доказательств в судах и арбитражах.

Таким образом, подводя итоги вышесказанному, киберпреступления перестали являться исключительно технической проблемой, превратившись в глобальный вызов для международного правосудия. Эффективная зашита международного коммерческого арбитража возможна при условии перехода от фрагментарных мер к комплексной системе цифровой защиты, сочетающей императивные нормы международного права с передовыми технологическими инструментами верификации данных.

Список литературы:

[1] Нью-Йорская конвенция 1958 года о признании и приведении в исполнение иностранных арбитражных решений. Доступ из СПС «Гарант».

[2] SVAMC Guidelines on the Use of Artificial Intelligence in Arbitration. – 2024. – P. 22.

[3] ICCA-NYC BAR-CPR Cybersecurity Protocol for International Arbitration. URL: https://www.arbitrationicca.org/publications/ICCA_Report_N6.html (дата обращения: 09.02.2026). – Текст: электронный.

[4] Libananco Holdings Co. Limited v. Republic of Turkey, ICSID Case No. ARB/06/8. // – URL: https://jusmundi.com/en/document/decision/en-libananco-holdings-co-limited-v-republic-of-turkey-decision-on-preliminary-issues-monday-23rd-june-2008/ (дата обращения: 09.02.2026). – Текст: электронный.

[5] Nurhima Kiram Fornan, Fuad A Kiram, Sheramar T Kiram, Permaisuli Kiram-Guerzon, Taj-Mahal Kiram-Tarsum Nuqui, Ahmad Narzad Kiram Sampang, Jenny KA Sampang and Widz-Raunda Kiram Sampang v. Malaysia. // – URL: https://jusmundi.com/en/document/decision/en-nurhima-kiram-fornan-fuad-a-kiram-sheramar-t-kiram-permaisuli-kiram-guerzon-taj-mahal-kiram-tarsum-nuqui-ahmad-narzad-kiram-sampang-jenny-ka-sampang-and-widz-raunda-kiram-sampang-v-malaysia-memorandum-order-of-the-united-states-district-court-for-the-district-of-delaware-thursday-3rd-july-2025/ (дата обращения: 09.02.2026). – Текст: электронный.

[6] Process and Industrial Developments Ltd. v. The Ministry of Petroleum Resources of the Federal Republic of Nigeria. // URL: https://jusmundi.com/en/document/decision/en-process-and-industrial-developments-ltd-v-the-ministry-of-petroleum-resources-of-the-federal-republic-of-nigeria-judgment-of-the-court-of-appeal-of-england-and-wales-2024-ewca-civ-790-friday-12th-july-2024/ (дата обращения: 09.02.2026). – Текст: электронный.

[7] Schjolberg, Stein. The history of cybercrime (third edition) / Stein Schjolberg. – 2020. – P. 25.

[8] Купчина Е.В. Разрешение споров в сфере интеллектуальной собственности международным арбитраже в условиях цифровизации: дис….канд.юрид. наук/ Купчина Е.В. – Москва, 2024. – 173 с.

References:

[1] 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards. Access from SPS "Garant.".

[2] SVAMC Guidelines on the Use of Artificial Intelligence in Arbitration. – 2024. – P. 22.

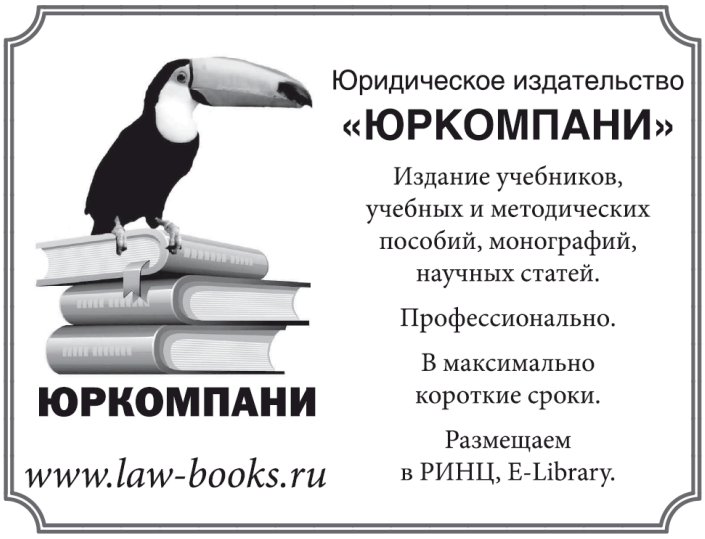
[3] ICCA-NYC BAR-CPR Cybersecurity Protocol for International Arbitration. URL: https://www.arbitrationicca.org/publications/ICCA_Report_N6.html (дата обращения: 09.02.2026). - Text: electronic.

[4] Libananco Holdings Co. Limited v. Republic of Turkey, ICSID Case No. ARB/06/8. // – URL: https://jusmundi.com/en/document/decision/en-libananco-holdings-co-limited-v-republic-of-turkey-decision-on-preliminary-issues-monday-23rd-june-2008/ (дата обращения: 09.02.2026). - Text: electronic.

[5] Nurhima Kiram Fornan, Fuad A Kiram, Sheramar T Kiram, Permaisuli Kiram-Guerzon, Taj-Mahal Kiram-Tarsum Nuqui, Ahmad Narzad Kiram Sampang, Jenny KA Sampang and Widz-Raunda Kiram Sampang v. Malaysia. // – URL: https://jusmundi.com/en/document/decision/en-nurhima-kiram-fornan-fuad-a-kiram-sheramar-t-kiram-permaisuli-kiram-guerzon-taj-mahal-kiram-tarsum-nuqui-ahmad-narzad-kiram-sampang-jenny-ka-sampang-and-widz-raunda-kiram-sampang-v-malaysia-memorandum-order-of-the-united-states-district-court-for-the-district-of-delaware-thursday-3rd-july-2025/ (дата обращения: 09.02.2026). - Text: electronic.

[6] Process and Industrial Developments Ltd. v. The Ministry of Petroleum Resources of the Federal Republic of

Nigeria. // URL: https://jusmundi.com/en/document/decision/en-process-and-industrial-developments-ltd-v-the-ministry-of-petroleum-resources-of-the-federal-republic-of-nigeria-judgment-of-the-court-of-appeal-of-england-and-wales-2024-ewca-civ-790-friday-12th-july-2024/ (дата обращения: 09.02.2026). - Text: electronic.

[7] Schjolberg, Stein. The history of cybercrime (third edition) / Stein Schjolberg. – 2020. – P. 25.

[8] E.V. Kupchina. Resolution of disputes in the field of intellectual property by international arbitration in the context of digitalization: dis.... Sciences/Kupchina E.V. - Moscow, 2024. - 173 s.