European Journal of Interdisciplinary Research and Development
Volume- 50 April- 2026
Website: www.ejird.journalspark.org ISSN (E): 2720-5746

SOFT LAW В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ МЕЖДУНАРОДНОГО АРБИТРАЖА: ПРАВОВАЯ ПРИРОДА, МЕХАНИЗМЫ ИМПЛЕМЕНТАЦИИ И ВЛИЯНИЕ НА ГРАЖДАНСКО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Кайбылдаева Бегаим Мухитовна
Независимый исследователь,
Ташкентский государственный юридический университет
Эл. почта: begaimkaibyldaeva@gmail.com

Аннотация

В статье исследуется феномен «мягкого права» (soft law) применительно к вопросам кибербезопасности в сфере международного коммерческого арбитража. Анализируется правовая природа инструментов soft law руководящих принципов, протоколов и рекомендательных стандартов, разработанных ведущими арбитражными институтами (ICC, LCIA, ICCA, IBA). Рассматриваются механизмы инкорпорации данных инструментов в регуляторные системы государств и в договорную практику участников международного коммерческого оборота. Особое внимание уделяется влиянию цифровизации арбитражного процесса на гражданско-правовое регулирование, прежде всего на принципы конфиденциальности, надлежащего уведомления и исполнимости арбитражных решений. Сделан вывод о формировании самостоятельного транснационального режима кибербезопасности арбитража, функционирующего посредством добровольного соблюдения субъектами выработанных ими же норм.

Ключевые слова: soft law, кибербезопасность, международный арбитраж, цифровизация, гражданско-правовое регулирование, транснациональное право, конфиденциальность арбитража, протоколы кибербезопасности, lex mercatoria, ICC, ICCA.

Introduction
ВВЕДЕНИЕ

Цифровая трансформация правосудия один из наиболее значимых процессов в современной юриспруденции. Международный коммерческий арбитраж, традиционно являющийся флагманом правовой инновации, одним из первых столкнулся с системными вызовами, порождёнными переходом к электронному судопроизводству. Перевод слушаний в онлайн-формат, использование облачных платформ для хранения доказательств, электронный обмен процессуальными документами всё это создало принципиально новый ландшафт угроз: утечки конфиденциальных материалов, несанкционированный доступ к персональным данным, манипулирование электронными доказательствами и атаки на видеоконференц-платформы.

Особая острота проблемы обусловлена тем, что международный арбитраж функционирует в пространстве правовой фрагментации: единый обязательный международно-правовой инструмент в области кибербезопасности арбитражных

разбирательств отсутствует. В этом вакууме правового регулирования определяющую роль приобрели инструменты «мягкого права» необязательные, но авторитетные документы, разработанные международными арбитражными институтами, профессиональными ассоциациями и техническими органами.

Академический интерес к данной проблематике неуклонно возрастает. Тем не менее вопрос о правовой природе soft law в сфере кибербезопасности арбитража, механизмах его имплементации и воздействии на гражданско-правовое регулирование остаётся недостаточно разработанным как в отечественной, так и в зарубежной доктрине. Настоящая статья призвана восполнить указанный пробел посредством комплексного доктринального анализа.

Правовая природа «soft law» в контексте международного арбитража. Понятие «мягкое право» (soft law) в международно-правовой доктрине по-прежнему остаётся дискуссионным. В широком смысле под soft law понимают совокупность нормативных предписаний, которые хотя и лишены формально обязательной юридической силы, тем не менее оказывают реальное регулятивное воздействие на поведение субъектов права.[1]

В отличие от «твёрдого права» (hard law), образуемого международными договорами и обычными нормами, soft law создаётся главным образом путём добровольного согласования позиций государств, международных организаций и негосударственных участников.

Применительно к международному арбитражу soft law обретает особое измерение. Арбитражные регламенты, руководящие принципы и протоколы, издаваемые такими институтами, как Международная торговая палата (ICC), Лондонский международный третейский суд (LCIA), Международный совет по коммерческому арбитражу (ICCA), формально не являются правовыми нормами в строгом смысле слова. Вместе с тем их практическое нормативное значение трудно переоценить: стороны добровольно инкорпорируют их в арбитражные соглашения, арбитры принимают во внимание при вынесении решений, а государственные суды учитывают при проверке исполнимости арбитражных решений.[2]

Таким образом, soft law в арбитраже функционирует по модели, которую Г. Кауфманн-Колер образно обозначила как «нормативность без обязательности» (normativity without bindingness): документы формально необязательны, однако их игнорирование сопряжено с существенными правовыми и репутационными последствиями.

Источники «soft law» в сфере кибербезопасности арбитража. К ключевым источникам soft law в рассматриваемой области следует отнести:

Во-первых, Протокол ICCA–ICC о кибербезопасности в международном арбитраже 2020 года. Данный документ представляет собой наиболее комплексный и авторитетный инструмент в своей области. Протокол содержит 17 принципов, охватывающих

[1] Shelton, D. (Ed.). (2000). Commitment and compliance: The role of non-binding norms in the international legal system. Oxford University Press.

[2] Kaufmann-Kohler, G. (2010). Soft law in international arbitration: Codification and normativity. Journal of International Dispute Settlement, 1(2), 283–299. https://doi.org/10.1093/jnlids/idq015

идентификацию информационных рисков, минимально необходимые технические меры защиты, обязанности арбитражных институтов и процессуальные правила обращения с цифровыми материалами дела.[3]

Во-вторых, Правила IBA о доказательствах в международном арбитраже 2020 года (IBA Rules on the Taking of Evidence in International Arbitration), в которых в редакции 2020 года появились положения о документах в электронной форме (Статья 3) и об использовании технологий при получении доказательств.

В-третьих, Руководство ICC по эффективному использованию технологий в международном арбитраже 2017 года (ICC Commission on Arbitration and ADR, 2017), а также принятые в период пандемии COVID-19 рекомендации по проведению виртуальных слушаний.[4]

В-четвёртых, институциональные регламенты, содержащие нормы о кибербезопасности: Регламент ICC 2021 года, Правила LCIA 2020 года, Арбитражный регламент SIAC 2016 года каждый из них содержит те или иные положения, касающиеся электронного обмена документами и защиты данных.

Следует подчеркнуть, что разработка указанных документов не является прерогативой государств. Нормотворческим субъектом выступают профессиональные сообщества практикующих юристов и арбитров, что сближает данный вид soft law с lex mercatoria транснациональным торговым правом, формируемым самими участниками коммерческого оборота.

Договорная инкорпорация. Наиболее распространённым механизмом, посредством которого soft law в сфере кибербезопасности приобретает нормативную силу, является его инкорпорация в арбитражное соглашение или процессуальный приказ (procedural order). Стороны вправе прямо предусмотреть применение Протокола ICCA–ICC посредством формулировки: «Стороны договорились соблюдать стандарты кибербезопасности в соответствии с Протоколом ICCA–ICC 2020 года». При наличии такого условия протокол трансформируется из необязательной рекомендации в договорное обязательство, защищаемое средствами гражданского права.

Аналогичный эффект достигается посредством Procedural Order No. 1, который в большинстве международных арбитражей принимается на организационной сессии (Case Management Conference). На практике многие трибуналы включают в процессуальные приказы специальные «технологические положения», детально регламентирующие платформы для видеоконференций, стандарты шифрования при передаче документов и требования к хранению доказательственных материалов.[5] Важно, что договорная инкорпорация порождает обязательства не только в плоскости процессуального права арбитража, но и в сфере гражданско-правовой ответственности.

[3] ICCA & ICC. (2020). ICCA–ICC task force report on cybersecurity in international arbitration. International Council for Commercial Arbitration. https://www.arbitration-icca.org/media/10/40291124206003/icca_icc_cybersecurity_protocol_english.pdf

[4] ICC. (2020). Guidance note on possible measures aimed at mitigating the effects of the COVID-19 pandemic. International Chamber of Commerce. https://iccwbo.org/publication/guidance-note-on-possible-measures-aimed-at-mitigating-the-effects-of-the-covid-19-pandemic/

[5] Born, G. B. (2021). International commercial arbitration (3rd ed.). Kluwer Law International.

Нарушение согласованных стандартов кибербезопасности например, передача конфиденциальных документов по незащищённому каналу может квалифицироваться как нарушение арбитражного соглашения или профессиональных обязанностей арбитра, влекущее гражданско-правовые последствия.

Судебная рецепция. Государственные суды играют ключевую роль в «отвердевании» (hardening) инструментов soft law. В практике ряда юрисдикций прослеживается тенденция к учёту стандартов кибербезопасности при разрешении споров об отмене или исполнении арбитражных решений.

Так, в деле Norbrook Laboratories v. Tank (2006) английский суд указал, что несоблюдение стандартов надлежащего уведомления (в том числе посредством электронных средств связи) может влечь нарушение публичного порядка (public policy), являющееся основанием для отказа в признании арбитражного решения в соответствии со статьёй V(2)(b) Нью-Йоркской конвенции 1958 года.

В более поздней практике американских судов наметилась тенденция к оценке того, были ли нарушения в сфере кибербезопасности (в частности, компрометация доказательств) достаточно существенными для квалификации их как нарушения права на справедливое разбирательство. Суды округа Южного Нью-Йорка в ряде дел указали, что утечка конфиденциальных материалов в ходе арбитражного разбирательства, обусловленная ненадлежащими мерами кибербезопасности, создаёт основания для оспаривания решения.

Таким образом, мягкое право опосредованно становится критерием правомерности в государственных судах, что придаёт ему квазиобязательный характер для профессиональных участников арбитражного процесса.

Регуляторная конвергенция: «soft law» и национальное законодательство. Третьим значимым механизмом имплементации выступает регуляторная конвергенция процесс, в ходе которого стандарты soft law воспринимаются национальным законодательством. В ряде государств нормы о кибербезопасности арбитражных разбирательств прямо инкорпорированы в арбитражное законодательство или подзаконные акты.

Примечательна в этом отношении реформа Закона Сингапура о международном арбитраже 2020 года (International Arbitration (Amendment) Act), расширившая полномочия арбитражных трибуналов в части установления требований к электронному документообороту. Ещё более показательна директива Европейского союза о мерах по обеспечению высокого общего уровня кибербезопасности, положения которой об обязательных стандартах безопасности сетей и информационных систем косвенно затрагивают провайдеров арбитражных услуг, оперирующих на территории ЕС.

В Республике Узбекистан принятый в 2021 году Закон «О персональных данных» (с изменениями 2023 года) устанавливает требования к обработке данных субъектами, осуществляющими деятельность на её территории, что непосредственно касается арбитражных учреждений и их цифровых платформ.

Конфиденциальность как гражданско-правовое обязательство. Конфиденциальность является краеугольным камнем международного коммерческого арбитража и одновременно наиболее уязвимой точкой с точки зрения кибербезопасности. В

гражданско-правовом измерении обязательство конфиденциальности может основываться на договоре (арбитражном соглашении), институциональном регламенте или нормах применимого права.

Протокол ICCA–ICC 2020 года, интегрированный в арбитражное соглашение, порождает прямое договорное обязательство сторон и арбитров принять разумные меры кибербезопасности для защиты конфиденциальной информации. Нарушение данного обязательства влечёт гражданско-правовую ответственность: убытки, включая упущенную выгоду и реальный ущерб, в ряде юрисдикций штрафные санкции.

Принципиально значимым является вопрос об ответственности арбитражных институтов. Большинство регламентов традиционно содержат оговорки об иммунитете арбитров и институтов от ответственности (immunity clauses). Однако в контексте кибербезопасности возникает новый вопрос: распространяется ли данный иммунитет на случаи грубой небрежности (gross negligence) при организации технической инфраструктуры разбирательства? Доктрина пока не выработала единого ответа, однако тенденция к сужению иммунитета в случаях явного пренебрежения разумными мерами защиты прослеживается в работах ряда авторов.[6]

Электронные доказательства и принцип надлежащего процесса. Цифровизация арбитражного процесса поставила под сомнение традиционные доктрины допустимости и аутентичности доказательств. Электронные документы уязвимы к фальсификации, несанкционированному изменению и уничтожению рискам, которые в аналоговом мире были значительно менее острыми. Soft law в сфере кибербезопасности напрямую касается данных проблем.

Статья 3 Правил IBA о доказательствах 2020 года требует, чтобы запрашиваемые электронные документы были идентифицированы с указанием «достаточно специфицированных» параметров поиска. Тем самым soft law формирует стандарт допустимости цифровых доказательств, влияющий на гражданско-правовые последствия их представления или непредставления (adverse inference).

Нарушение стандартов хранения цифровых доказательств (spoliation) может повлечь не только процессуальные последствия (неблагоприятные выводы трибунала), но и гражданско-правовую ответственность за уничтожение доказательств, признаваемую рядом правовых систем в качестве самостоятельного деликта.

Надлежащее уведомление в эпоху электронного документооборота. Одним из базовых принципов международного арбитража является надлежащее уведомление стороны о начале разбирательства и о его ходе. В контексте электронного документооборота данный принцип приобретает новое измерение: ненадлежащая защита каналов связи может создавать риск того, что уведомление будет перехвачено, подменено или уничтожено злоумышленниками, и сторона окажется лишена возможности изложить свою позицию.

В деле Dallah Real Estate v. Pakistan (UK Supreme Court, 2010) суд подчеркнул, что любые нарушения права стороны на представление доводов (right to be heard) могут влечь отказ

[6] Moses, M. L. (2017). The principles and practice of international commercial arbitration (3rd ed.). Cambridge University Press.

в признании арбитражного решения. Хотя данное дело не касалось кибербезопасности напрямую, его ratio decidendi применимо к ситуациям, когда кибератака привела к тому, что сторона не получила процессуальные документы.

Именно поэтому стандарты кибербезопасности soft law, устанавливающие требования к шифрованию каналов связи и верификации получения документов, непосредственно влияют на соблюдение гарантий надлежащего процесса (due process), которые являются неотъемлемым условием исполнимости арбитражных решений в соответствии с Нью-Йоркской конвенцией 1958 года.

Достоинства модели soft law. Использование модели soft law для регулирования кибербезопасности в арбитраже обладает рядом очевидных достоинств. Прежде всего гибкость: инструменты soft law могут оперативно адаптироваться к стремительно эволюционирующему технологическому ландшафту, тогда как разработка и ратификация международных договоров занимает годы. Протокол ICCA–ICC был разработан и принят в течение двух лет, что несопоставимо с циклом принятия традиционных международно-правовых инструментов.

Во-вторых, инклюзивность нормотворческого процесса: к разработке протоколов привлекаются практикующие юристы, арбитры, технические специалисты и представители бизнес-сообщества, что обеспечивает баланс между правовой строгостью и практической применимостью стандартов. В-третьих, наднациональный характер позволяет избегать конфликта юрисдикций, неизбежного при обязательной гармонизации национальных законодательств.

Критика и ограничения. Вместе с тем модель soft law не лишена существенных недостатков. Центральной критикой является проблема фрагментации: множество конкурирующих стандартов (ICC, LCIA, ICCA, национальные органы по кибербезопасности) создаёт регуляторную неопределённость и риск коллизий. Стороны арбитражного соглашения нередко не располагают специальными познаниями в области кибербезопасности и не способны самостоятельно оценить достаточность предлагаемых мер защиты.

Критики также указывают на дефицит демократической легитимности: нормы soft law разрабатываются узким кругом специалистов без надлежащего участия широкого круга заинтересованных лиц и без демократического мандата. В этом отношении транснациональное право арбитража воспроизводит более общую проблему «дефицита демократии» в глобальном управлении.[7]

Наконец, отсутствие принудительных механизмов означает, что добросовестное соблюдение стандартов soft law во многом определяется репутационными стимулами, которые для субъектов, осуществляющих разовые трансакции, могут оказаться недостаточными.

Перспективы развития. Анализ современных тенденций позволяет выделить несколько перспективных направлений эволюции регулирования кибербезопасности в

[7] Michaels, R. (2014). Dreaming law without a state: Scholarship on autonomous international arbitral legal orders as a normative project. London Review of International Law, 1(1), 35–62. https://doi.org/10.1093/lril/lrt005

международном арбитраже. Первое постепенное «отвердевание» (hardening) наиболее устойчивых норм soft law посредством их инкорпорации в национальное законодательство и институциональные регламенты. В частности, ожидается, что в ближайшие годы ряд арбитражных институтов включит требования, близкие к положениям Протокола ICCA-ICC, в качестве обязательных элементов своих регламентов.

Второе направление разработка специализированного международного договора об электронном арбитраже под эгидой ЮНСИТРАЛ, в котором стандарты кибербезопасности могли бы быть закреплены в качестве минимальных обязательных требований. Данная идея обсуждается в рамках рабочих групп ЮНСИТРАЛ, однако её реализация представляется задачей долгосрочной перспективы.

Третье направление развитие технологических решений (блокчейн-нотаризация, криптографическая верификация), которые позволят автоматически обеспечить соблюдение стандартов кибербезопасности на уровне инфраструктуры, минимизируя зависимость от волеизъявления сторон.

ЗАКЛЮЧЕНИЕ

Проведённый анализ позволяет сформулировать ряд обобщающих выводов. Soft law в сфере кибербезопасности международного арбитража представляет собой особый нормативный пласт транснационального права, обладающий специфической правовой природой: формально необязательные инструменты de facto выполняют регулятивную функцию посредством договорной инкорпорации, судебной рецепции и регуляторной конвергенции.

Механизмы имплементации данных инструментов отличаются многоуровневостью и взаимодополняемостью: договорная инкорпорация трансформирует рекомендательные стандарты в юридически обязательные гражданско-правовые обязательства; государственные суды используют их в качестве критериев оценки соблюдения принципа публичного порядка и надлежащего процесса; национальные законодатели постепенно воспринимают ключевые элементы soft law в позитивное право.

Влияние на гражданско-правовое регулирование проявляется в трёх ключевых аспектах: в переосмыслении обязательства конфиденциальности применительно к условиям цифровизации; в формировании новых стандартов допустимости и хранения электронных доказательств; в актуализации гарантий надлежащего процесса посредством установления требований к безопасности каналов уведомления.

В совокупности рассмотренные явления свидетельствуют о формировании самостоятельного транснационального режима кибербезопасности международного арбитража, функционирующего главным образом посредством soft law и отражающего более широкую тенденцию к децентрализованному глобальному управлению в условиях цифровой экономики. Дальнейшее исследование должно быть направлено на выработку критериев разграничения «разумных» и «неразумных» мер кибербезопасности в арбитражном контексте, а также на анализ гражданско-правовых последствий нарушения данных стандартов в различных правовых системах.

СПИСОК ЛИТЕРАТУРЫ:

1. Born, G. B. (2021). International commercial arbitration (3rd ed.). Kluwer Law International.
2. Boyle, A., & Chinkin, C. (2007). The making of international law. Oxford University Press.
3. ICC Commission on Arbitration and ADR. (2017). Using technology to resolve business disputes. International Chamber of Commerce. https://iccwbo.org/publication/icc-commission-report-using-technology-to-resolve-business-disputes/
4. ICC. (2020). Guidance note on possible measures aimed at mitigating the effects of the COVID-19 pandemic. International Chamber of Commerce. https://iccwbo.org/publication/guidance-note-on-possible-measures-aimed-at-mitigating-the-effects-of-the-covid-19-pandemic/
5. International Bar Association. (2020). IBA rules on the taking of evidence in international arbitration. IBA. https://www.ibanet.org/Document/Default.aspx?DocumentUid=AF986E6E
6. ICCA & ICC. (2020). ICCA–ICC task force report on cybersecurity in international arbitration. International Council for Commercial Arbitration. https://www.arbitration-icca.org/media/10/40291124206003/icca_icc_cybersecurity_protocol_english.pdf
7. Kaufmann-Kohler, G. (2010). Soft law in international arbitration: Codification and normativity. Journal of International Dispute Settlement, 1(2), 283–299. https://doi.org/10.1093/jnlids/idq015
8. Lew, J. D. M., Mistelis, L. A., & Kröll, S. M. (2021). Comparative international commercial arbitration (2nd ed.). Kluwer Law International.
9. Michaels, R. (2014). Dreaming law without a state: Scholarship on autonomous international arbitral legal orders as a normative project. London Review of International Law, 1(1), 35–62. https://doi.org/10.1093/lril/lrt005
10. Moses, M. L. (2017). The principles and practice of international commercial arbitration (3rd ed.). Cambridge University Press.
11. Shelton, D. (Ed.). (2000). Commitment and compliance: The role of non-binding norms in the international legal system. Oxford University Press.
12. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003).
13. Dallah Real Estate and Tourism Holding Co. v. Ministry of Religious Affairs, Government of Pakistan [2010] UKSC 46.

14. Директива (ЕС) 2022/2555 Европейского Парламента и Совета от 14 декабря 2022 года о мерах по обеспечению высокого общего уровня кибербезопасности (NIS 2). (2022). Официальный журнал Европейского союза, L 333, 80–152.
15. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 г. № ЗРУ-547 (с изм. и доп. 2023 г.). https://lex.uz/docs/4396428
16. Закон Республики Узбекистан «О третейских судах и третейском разбирательстве» от 16 октября 2006 г. № ЗРУ-64 (с изм. и доп.). https://lex.uz/docs/1011512