www.volsu.ru

DOI: https://doi.org/10.15688/lc.jvolsu.2020.2.19

UDC 347.918.2
LBC 67.410.14

Submitted: 12.03.2020
Accepted: 03.04.2020

CYBERSECURITY IN THE INTERNATIONAL COMMERCIAL ARBITRATION FOR INTELLECTUAL PROPERTY DISPUTES [1]

Ekaterina V. Kupchina

Peoples' Friendship University of Russia, Moscow, Russian Federation

Introduction: in the paper the author considers such a complex and multi-level issue as cybersecurity in the international commercial arbitration, including when considering disputes related to the intellectual property violations. The rapidly developing areas of information technology dictate the need for rapid and adequate measures in this area. Modern approaches based on the risk assessment in each arbitration by the participants of the arbitration, as a result of which the arbitrators have the right to take measures based on the circumstances of each individual case, have become a subject of discussion in the modern scientific community. Although the significance of cybersecurity risks may vary from one case to another, the threat of a cyber attack occurs in almost every international arbitration. The **purpose** of the research is achieved by solving a number of tasks: to identify the most frequent cases of violation of the rights of legal rights holders; to highlight the problem of confidentiality of arbitration disputes. The **methodology** is based on a theoretical approach to the study of the arbitration rules, as well as a number of national sources and other normative acts. Based on the analysis of the theoretical data obtained, the author provides examples of the most frequent cases of violation of the confidentiality of arbitration proceedings, as well as highlights some modern approaches to solving this problem. The **results** of the research can be used in determining the key goals and objectives of the procedural nature, improving the functioning of judicial and non-judicial organizations, law enforcement, research, and teaching activities, in particular, lectures and seminars on private international law, arbitration, copyright and patent law. **Conclusions:** the increased awareness of participants of the international commercial arbitration about the ways of information storage and information security promotes the development of the institution of arbitration proceedings, increases the degree of confidence of the parties in the procedures for dispute resolution.

Key words: intellectual property, international commercial arbitration, cybersecurity, cyber attacks, privacy.

Citation. Kupchina E.V. Cybersecurity in the International Commercial Arbitration for Intellectual Property Disputes. *Legal Concept*, 2020, vol. 19, no. 2, pp. 129-135. (in Russian). DOI: https://doi.org/10.15688/lc.jvolsu.2020.2.19

УДК 347.918.2
ББК 67.410.14

Дата поступления статьи: 12.03.2020
Дата принятия статьи: 03.04.2020

КИБЕРБЕЗОПАСНОСТЬ В МЕЖДУНАРОДНОМ КОММЕРЧЕСКОМ АРБИТРАЖЕ ПРИ РАССМОТРЕНИИ ИНТЕЛЛЕКТУАЛЬНЫХ СПОРОВ [1]

Екатерина Валентиновна Купчина

Российский университет дружбы народов, г. Москва, Российская Федерация

Введение: в настоящей статье автором рассматривается такой сложный и многоуровневый вопрос, как кибербезопасность в международном коммерческом арбитраже, в том числе при рассмотрении споров, касающихся нарушений в сфере интеллектуальной собственности. Быстро развивающиеся сферы информационных технологий диктуют необходимость принятия быстрых и адекватных мер в указанной области. Современные подходы, основанные на оценке риска, при каждом арбитражном разбирательстве участника-

ми арбитража, в результате которых арбитры имеют право принимать меры, основанные на обстоятельствах каждого отдельного случая, стали предметом для дискуссий в современном научном сообществе. Несмотря на то что значение рисков кибербезопасности может варьироваться от одного случая к другому, угроза кибератаки возникает практически в каждом международном арбитраже. **Цель** настоящего исследования достигается путем решения ряда задач: выявить наиболее частые случаи нарушения прав законных правообладателей; осветить проблему конфиденциальности арбитражных споров. **Методология** основывается на теоретическом подходе к исследованию арбитражных регламентов, а также ряда национальных источников и иных нормативных актов. На основе анализа полученных теоретических данных в настоящей работе автором приводятся примеры наиболее частых случаев нарушения конфиденциальности арбитражного разбирательства, а также освещаются некоторые современные подходы к решению данной проблемы. **Результаты** исследования могут быть использованы при определении ключевых целей и задач процессуального характера, совершенствовании функционирования судебных и внесудебных организаций, правоприменительной, научно-исследовательской деятельности, а также в учебно-преподавательской деятельности, в частности, при лекциях и семинарских занятиях по курсам международного частного права, арбитражного процесса, авторского и патентного права. **Выводы:** увеличение степени осведомленности участников международного коммерческого арбитража о способах хранения информации, а также обеспечения информационной безопасности способствует развитию института арбитражного судопроизводства, повышает степень доверия со стороны участников к процедурам рассмотрения споров.

Ключевые слова: интеллектуальная собственность, международный коммерческий арбитраж, кибербезопасность, кибератаки, конфиденциальность.

Цитирование. Купчина Е. В. Кибербезопасность в международном коммерческом арбитраже при рассмотрении интеллектуальных споров // Legal Concept = Правовая парадигма. – 2020. – Т. 19, № 2. – С. 129–135. – DOI: https://doi.org/10.15688/lc.jvolsu.2020.2.19

Введение

Интеллектуальная собственность будучи объектом хозяйственного оборота обладает способностью более быстрого, по сравнению с другими объектами, распространения как внутри страны, так и за ее пределами. Вопросы правового регулирования отношений, связанных с интеллектуальной собственностью, как никакие другие, должны рассматриваться в международном контексте.

Наиболее распространенной альтернативой судебного разбирательства в спорах, связанных с интеллектуальной собственностью, является посредничество и арбитраж. В свою очередь, среди двух указанных процедур арбитраж представляет собой наиболее удобную и простую форму урегулирования споров.

При рассмотрении интеллектуальных споров международным арбитражем существует ряд преимуществ. Стороны могут договориться о рассмотрении спора в одном арбитражном форуме, что позволяет избежать получения противоречивых результатов. При рассмотрении спора в арбитраже стороны могут осуществлять контроль над процедурой рассмотрения дела, имеют возможность выбрать применимое право, язык разбирательства и т. д. Стороны могут выбрать арбитров, особенно это касается ситуаций, когда арбитр должен обладать специальными знаниями в конкретной области, по поводу которой ведется спор (бизнес, право, наука и т. д.). Также у арбитров имеются широкие процессуальные полномочия. Например, при рассмотрении спора о нарушении авторского права при создании программного обеспечения арбитр может обязать ответчика приобрести лицензию [3, с. 54].

Одним из ключевых преимуществ арбитража по праву считается высокая степень конфиденциальности при рассмотрении спора. Стороны могут принять меры по предотвращению публичного распространения коммерческой тайны и деловой информации. Однако в современном цифровом мире все больше распространяется такое явление, как кибератаки, и с этой точки зрения арбитраж является крайне привлекательным для хакеров. В рамках арбитражного процесса участники обмениваются информацией, которая носит закрытый характер. В случае попадания данных в недобросовестные руки это может потенциально нанести коммерческий ущерб, повлиять на цены акций, корпоративные стратегии или даже государственную политику.

Особенно негативные последствия разглашения информации могут быть при рассмотрении споров, связанных с охраной интеллектуальных прав, так как информация о характере и содержании охраняемых объектов имеет важнейшее значение в современной конкурентной среде [10, с. 469].

Киберугрозы в сфере интеллектуальной собственности

Вопросы информационной безопасности и защиты данных тесно связаны, в основном потому, что во всем мире усиливается регулирование и обработка персональных данных. Для законодательства и нормативных актов о защите данных характерно, среди прочего, обязательство лиц, обрабатывающих личные данные, применять разумные меры информационной безопасности [5, с. 17].

Применительно к объектам интеллектуальной собственности можно выделить несколько групп нарушений, возникающих в киберпространстве:

– незаконный доступ, получение и раскрытие сведений, составляющих коммерческую тайну (ноу-хау), государственную тайну;

– несанкционированное вмешательство в базы данных, изменение или блокировка сведений в составе баз данных и иной цифровой информации;

– распространение в сети Интернет персональных данных физического или юридического лица;

– нарушение авторских или смежных прав путем несанкционированного копирования или скачивания информации;

– незаконное использование товарных знаков, наименований юридических лиц или других средств индивидуализации, в том числе доменных имен [2, с. 48].

Большинство споров, вытекающих из перечисленных выше нарушений прав на интеллектуальную собственность, подлежит рассмотрению в международном коммерческом арбитраже.

Правилами большинства арбитражей, рассматривающих споры в сфере интеллектуальной собственности, специально регламентированы положения о конфиденциальности. Например, Арбитражный регламент ВОИС в ст. 54 определяет «конфиденциальную информацию» как любую информацию, независимо от того, в какой форме она выражена, а именно:

– находится во владении стороны;

– является недоступной для общественности;

– представляет коммерческую, финансовую или промышленную значимость;

– считается конфиденциальной стороной, обладающей информацией [11].

Повсеместный переход на цифровые технологии и обмен информацией в электронном виде создает благоприятные условия для кибератак. Почти любая организация становится уязвимой в таких условиях. Безопасность данных арбитражного разбирательства не является исключением в этом контексте [6, с. 4436]. Как только происходит отправка данных в электронном виде, отправитель больше не может контролировать или обеспечивать свою безопасность. Представляется возможным выделить некоторые группы участников арбитража, которые являются наиболее незащищенными:

– юридические фирмы, оказывающие услуги в международном коммерческом арбитраже;

– адвокаты;

– арбитры;

– непосредственно сами стороны арбитражного разбирательства;

– третьи лица, обладающие информацией о любом из вышеперечисленных участников, включая экспертов, свидетелей и поставщиков услуг.

Основные источники распространения киберугроз

Как правило, обмен информацией между юристами и клиентами, а также обсуждение вопросов и стратегий арбитражного разбирательства происходят по электронной почте. Заявления, большинство доказательств, а также экспертные заключения и показания свидетелей также зачастую передаются в электронном виде. Проверка и подготовка документов регулярно осуществляется на электронных платформах хостинга данных, которые обычно принадлежат сторонним поставщикам услуг.

С целью минимизирования рисков кибератак и сохранения конфиденциальности требуется понимание угрозы и принятие адекватных мер [4, с. 47]. Основная задача заключается в обеспечении того, чтобы все субъекты, которые так или иначе имеют отношение к арбитражному разбирательству и соприкасаются с информацией, в первую очередь соблюдали корпоративную политику безопасности и сохранения информации. Несомненно, за безопасность информации отвечает не только команда специалистов по информационным технологиям – это каждый человек в организации [7, с. 90]. Однако, как показывает практика, арбитры продолжают использовать обычные веб-службы электронной почты, такие как Gmail или Yahoo. При многомилионных исках в международном коммерческом арбитраже адвокаты продолжают общаться с помощью незашифрованной электронной почты, не говоря уже о самих сторонах, которые не стремятся к использованию безопасных интернет-каналов для обмена информацией.

Наряду с мессенджерами электронная почта является самой популярной формой общения в мире. Чтобы понять, почему электронная почта является не безопасным способом обмена информацией, нужно вспомнить, что еще несколько десятилетий назад использование сети Интернет было весьма ограничено и все, что передавалось, было открыто и доступно. Несомненно, за прошедшее время был сделан значительный рывок в сфере обеспечения конфиденциальности и безопасного общения, создана система паролей и шифрования передаваемых данных. Однако факт остается фактом: каждое электронное письмо находится во многих местах одновременно. Исходным источником является устройство отправителя (смартфон, планшет, компьютер), и до того, как электронное письмо поступит на устройство получателя, оно проходит через множество промежуточных сетей, серверов, маршрутизаторов и коммутаторов, которыми зачастую управляют разные администраторы. Каждый подобный промежуточный узел является отдельной уязвимой точкой для несанкционированных вторжений. Хакер, который проникает в любое из этих мест, может получить доступ и даже изменить содержимое электронных писем, которые проходят через него.

В качестве примера того, что электронная почта является небезопасным способом общения и обмена информацией можно привести случай взлома компьютеров, который произошел в 2017 году. Как известно, 27 июня 2017 г. ряд компаний по всему миру подвергся кибератаке вируса под названием «Petya». Заражение компьютеров происходило через фишинговые письма (фишинг – вид интернет-мошенничества, когда под видом писем от имени популярных брендов злоумышленники получают доступ к конфиденциальным данным пользователей). Специалисты утверждают, что вирус использовал поддельную электронную подпись Microsoft.

В последнее время стороны в международном коммерческом арбитраже все чаще используют альтернативные облачные сервисы для хранения и обмена информацией, такие как Box, Dropbox и подобные им платформы. Но, как и в случае с электронной почтой, эти сервисы не разрабатывались как специальные и не обеспечивают надлежащего уровня безопасного хранения данных. Многие такие платформы заявляют о праве собственности на всю загружаемую информацию, что делает возможным использовать и делиться такой информацией в любых открытых целях. Кроме того, администраторы и разработчики облачных сервисов имеют полный доступ к передаваемой информации. Информация о мерах безопасности, используемых большинством таких платформ, является не доступной для пользователей. Также при загрузке информации в облачное хранилище, как правило, не допускается ее шифрование.

Меры по обеспечению конфиденциальности в международном коммерческом арбитраже

Как же участникам международного коммерческого арбитража можно обезопасить себя и обеспечить максимальный уровень конфиденциальности?

С целью адекватной оценки безопасного ведения арбитражного разбирательства и снижения рисков кибератак совместно с Международным советом по международному

коммерческому арбитражу (International Council for Commercial Arbitration – ICCA), Нью-Йоркской ассоциацией адвокатов (New York City Bar Association) и Международным институтом предотвращения и разрешения конфликтов (International Institute for Conflict Prevention and Resolution – CPR) был разработан ICCA-NYC BAR-CPR Cybersecurity Protocol for International Arbitration (далее – Протокол) [8, с. 5].

По мнению авторов, цель создания Протокола для международного коммерческого арбитража имеет двоякое значение. Во-первых, Протокол призван обеспечить основу для определения разумных мер информационной безопасности для отдельных арбитражных вопросов. Эта структура включает процедурное и практическое руководство для оценки рисков безопасности и определения доступных мер, которые могут быть реализованы.

Во-вторых, Протокол направлен на повышение осведомленности об информационной безопасности в международных арбитражах. Это включает в себя следующие положения:

– риски информационной безопасности в арбитражном процессе, в которые входят риски как кибербезопасности, так и физической безопасности;

– важность информационной безопасности для поддержания доверия пользователей к общему арбитражному режиму;

– подчеркнутая важная роль лиц, участвующих в арбитраже и способствующих эффективному снижению рисков;

– некоторые легкодоступные меры информационной безопасности, применимые для улучшения повседневной практики безопасности [8, с. 6].

Данный документ носит рекомендательный характер, однако его принятие, безусловно, повышает уровень осведомленности и ставит вопросы кибербезопасности в центр внимания, предоставляя некоторые практические рекомендации для повседневного применения различных правил.

Сфера информационных технологий в плане обеспечения безопасности обмена и хранения информации в процессе арбитражного разбирательства также не стоит на месте [1, с. 7; 9, с. 90]. К счастью для арбитров, специалистов-практиков и их клиентов, разрыв между текущей (небезопасной) практикой и потребностью в конфиденциальности заполняется отраслью легальных технологий. Например, специально разработанная для юридической отрасли платформа TransCEND, которая позволяет арбитрам, сторонам и их консультантам безопасно хранить, передавать и редактировать конфиденциальные документы из любой точки мира.

Поскольку такие платформы изначально разрабатываются с упором на безопасность, функции, обеспечивающие конфиденциальность, являются многогранными и их почти невозможно обойти. В первую очередь использование данной платформы предполагает многофакторную аутентификацию для доступа к базе данных. Это означает, что каждый загруженный файл инкапсулируется в защитный экран для предотвращения перехвата данных и несанкционированного извлечения или распространения контента. Кроме того, с помощью средств управления доступом на платформе сторона, загружающая документ, может контролировать объем доступа, который они предоставляют своим контрагентам (или самим арбитрам). Например, при подаче особо важных документов через платформу, доступ принимающих сторон может быть ограничен возможностью просмотра содержимого через платформу при отключении возможности редактировать, распечатывать, загружать или отправлять документ по электронной почте другим лицам. Даже возможность сделать «скриншот» может быть отключена.

Вывод

Повсеместная оцифровка всех процессов в международных коммерческих арбитражах диктует условия, при которых институциональные правила и руководства должны будут идти в ногу со временем. Необходимо строго учитывать и обеспечивать соответствующие меры кибербезопасности, которые подходят в каждом конкретном случае, и то, как будет распределена ответственность между заинтересованными сторонами в арбитражном процессе при реализации этих мер. Все участники арбитража должны быть макси-

мально осведомлены о том, как они получают и хранят данные, а также о технических сложностях и расходах, связанных с различными мерами кибербезопасности. Коммерческая чувствительность данных, а также индивидуальные обязательства сторон по защите информации обусловливают пропорциональность любой конкретной меры кибербезопасности. Знание технологических, организационных и процедурных вариантов, доступных для повышения кибербезопасности, будет способствовать содержательному обсуждению многих необходимых мер кибербезопасности в арбитраже и предоставит убедительные основания для трибуналов вынести соответствующий порядок в случае несогласия сторон.

ПРИМЕЧАНИЕ

[1] Работа выполнена при финансовой поддержке гранта Президента РФ № НШ-2668-2020.6 «Национально-культурные и цифровые тренды социально-экономического и политико-правового развития Российской Федерации в XXI веке».

This work was financially supported by the Grant of the President of the Russian Federation No. НШ-2668-2020.6 "National-Cultural and Digital Trends in the Socio-Economic, Political and Legal Development of the Russian Federation in the 21st Century".

СПИСОК ЛИТЕРАТУРЫ

1. Иншакова, А. О. Право и информационно-технологические преобразования общественных отношений в условиях индустрии 4.0 / А. О. Иншакова // Legal Concept. – 2019. – Т. 18, № 4. – С. 6–17.

2. Карцхия, А. А. Кибербезопасность и интеллектуальная собственность. Ч. 2 / А. А. Карцхия // Вопросы кибербезопасности. – 2014. – № 2 (3). – С. 46–50.

3. Купчина, Е. В. Споры в области интеллектуальной собственности в практике лондонского международного арбитражного суда / Е. В. Купчина // Евразийский юридический журнал. – М., 2016. – № 4. – С. 54–56.

4. 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.

5. Мир в цифровую эпоху: политика, право и экономика в XXI веке / А. Ю. Мамычев, Д. А. Петрова, Я. В. Гайворонская [и др.]. – М. : ООО «Издательский Центр РИОР», 2020. – 216 с.

6. Digital technologies as a driver of intellectual stratification of human resources: Socio-economic inequality / E. P. Rusakova, M. N. Dudin, O. F. Shakhov, M. S. Shakhova, Yu. S. Sizova // International Journal of Recent Technology and Engineering. – 2019. – Vol. 8, No. 2. – P. 4436–4440.

7. 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.

8. ICCA-NYC BAR-CPR Cybersecurity Protocol for International Arbitration (2020). – Electronic text data. – Mode of access: https://www.arbitration-icca.org/publications/ICCA_Report_N6.html (accessed 8 April 2020). – Title from screen.

9. Frolova, E. E. Information security of Russia in the digital economy: the economic and legal aspects / E. E. Frolova, T. A. Polyakova, M. N. Dudin, E. P. Rusakova, P. A. Kucherenko // Journal of Advanced Research in Law and Economics. – 2018. – Vol. 9, No. 1. – P. 89–95.

10. 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, 4–6 February 2019, Dubai, U.A.E. – Dubai, 2019. – P. 468–472.

11. WIPO Arbitration Rules (Effective from January 1, 2020). – Electronic text data. – Mode of access: https://www.wipo.int/amc/en/arbitration/rules/#cond2 (accessed 03 April 2020). – Title from screen.

REFERENCES

1. Inshakova A.O. Pravo i informatsionno-tekhnologicheskiye preobrazovaniya obshchestvennykh otnosheniy v usloviyakh industrii 4.0 [Law and Information and Technological Transformations of Public Relations in the Conditions of Industry 4.0]. *Legal Concept*, 2019, vol. 18, no. 4, pp. 6-17.

2. Kartskhiya A.A. Kiberbezopasnost i intellektualnaya sobstvennost. Ch. 2 [Cybersecurity and Intellectual Property]. *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2014, no. 2 (3), pp. 46-50.

3. Kupchina E.V. Spory v oblasti intellektualnoy sobstvennosti v praktike londonskogo mezhdunarodnogo arbitrazhnogo suda [Intellectual Property Disputes in the Practice of the London

International Arbitration Court]. *Evraziyskiy yuridicheskiy zhurnal* [Eurasian Law Journal]. Moscow, 2016, no. 4, pp. 54-56.

4. Kuryshova Ya.S. *Intellektualnaya sobstvennost i kiberataki. Intellektualnaya sobstvennost: ot nadezhnoy zashchity k effektivnomu upravleniyu: sb. st. XI Mezhdunar. nauch.-prakt. konf., g. Ekaterinburg, 30–31 oktyabrya 2015 g.* [Intellectual Property and Cyber Attacks]. Ekaterinburg, Izd-vo Ural. gos. ekon. un-ta, 2015. 99 p.

5. Mamychev A.Yu., Petrova D.A., Gayvoronskaya Ya.V., Miroshnichenko O.I. [i dr.]. *Mir v tsifrovuyu epokhu: politika. pravo i ekonomika v XXI veke* [The World in the Digital Age: Politics, Law and Economics of the XXI Century]. Moscow, OOO «Izdatelskiy Tsentr RIOR», 2020. 216 p.

6. Rusakova E.P., Dudin M.N., Shakhov O.F., Shakhova M.S., Sizova Yu.S. Digital Technologies As a Driver of Intellectual Stratification of Human Resources: Socio-Economic Inequality. *International Journal of Recent Technology and Engineering*, 2019, vol. 8, no. 2, pp. 4436-4440.

7. Inshakova A.O., Dolinskaya V.V., Frolova E.E. Classification Criteria: Defending the Specific Features of Corporate Conflicts. *"Conflict-Free" Socio-Economic Systems: Perspectives and Contradictions Bingley*. West Yorkshire, 2019, pp. 89-99.

8. *ICCA-NYC BAR-CPR Cybersecurity Protocol for International Arbitration (2020)*. URL: https://www.arbitration-icca.org/publications/ICCA_Report_N6.html (accessed 8 April 2020).

9. Frolova E.E., Polyakova T.A., Dudin M.N., Rusakova E.P., Kucherenko P.A. Information Security of Russia in the Digital Economy: The Economic and Legal Aspects. *Journal of Advanced Research in Law and Economics*, 2018, vol. 9, no. 1, pp. 89-95.

10. Kupchina E., Kuznetsova O., Chilingaryan K. IP Dispute Resolution Thought International Commercial Arbitration: US Experience. *Proceedings of INTCESS 2019 – 6th International Conference on Education and Social Sciences, 4–6 February 2019, Dubai, U.A.E.* Dubai, 2019, pp. 468-472.

11. *WIPO Arbitration Rules (Effective from January 1, 2020)*. URL: https://www.wipo.int/amc/en/arbitration/rules/#cond2 (accessed 03 April 2020).

Information About the Author

Ekaterina V. Kupchina, Senior Lecturer, Department of Civil Law and Procedure and Private International Law, Peoples' Friendship University of Russia, Miklukho-Maklaya St., 6, 117198 Moscow, Russian Federation, belousova_ev@pfur.ru, https://orcid.org/0000-0003-1318-3654

Информация об авторе

Екатерина Валентиновна Купчина, старший преподаватель кафедры гражданского права и процесса и международного частного права, Российский университет дружбы народов, ул. Миклухо-Маклая, 6, 117198 г. Москва, Российская Федерация, belousova_ev@pfur.ru, https://orcid.org/0000-0003-1318-3654