ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

УДК 341.6

АНАЛИЗ ВЛИЯНИЯ КИБЕРУГРОЗ НА МЕЖДУНАРОДНОЕ ИНВЕСТИЦИОННОЕ ПРАВО

Нұрғазиева Диана Азизбекқызы
dianangurgazieva4@gmail.com
Студент 1 курса 7М04202- «Международное право» ЕНУ им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – Ж.Т. Искакова

В последние годы мы стали свидетелями роста кибератак, которые могут быть направлены на организации, правительства и даже на индивидуальных пользователей. Эти атаки могут затронуть критическую инфраструктуру, финансовые системы и технологические компании, что может привести к значительным экономическим потерям и ущербу для бизнеса. Только в 2023 году, по данным компании IT Governance, в мире произошло 8,2 млрд утечек данных в результате кибератак [1]. В современном мире международные инвестиции в значительной степени зависят от технологии и онлайн-систем, что делает их уязвимыми для киберугроз.

Согласно данным ООН, общий ущерб мировой экономике от кибератак к 2025 году достигнет 10 трлн долларов. Согласно докладам Международной организации по ценным бумагам (IOSCO) и научно-исследовательскому отделу Всемирной федерации бирж ценных бумаг ежегодный ущерб от кибератак для каждый из бирж-жертв составляет около 1 млн долларов. Согласно опросу, проведенному вышеперечисленными учреждениями 53% бирж участников стали жертвами нападения в 2023 году [2].

Эти положения дают основания для проведения комплексного исследования в в рамках научной статьи.

Цель - провести анализ влияния киберугроз на правовые аспекты международных инвестиций. В рамках достижения данной цели были поставлены следующие **задачи**:

- Рассмотреть международно-правовое определение киберугроз и их виды
- Рассмотреть проблемы, возникающие в контексте киберугроз для международного инвестиционного права.

Объект - воздействие киберугроз на международное инвестиционное право.

Предмет исследования: аспекты влияния киберугроз на международное инвестиционное право.

Материальная база исследования состоит из международно-правовых документов в области кибербезопасности и международного инвестиционного права, а также научных трудов в области кибербезопасности, статистики и материалов СМИ о киберпреступлениях, связанных с инвестиционными активами.

Методы исследования включают в себя общенаучные и частноөнаучные методы, как анализ, абстрагирование, синтез и т.д.

Международно-правовое определение киберугроз и их виды

Исследователь Каратаева Л.Р. в своей работе «Информационная безопасность vs кибербезопасность: проблемы определения» указывает, что «кибербезопасность» это «информационная безопасность в компьютерной сфере, которая обеспечивает устойчивость в условиях информационного противоборства» [3]. Она подчеркивает, что в данном определении главным становится информационно-технический компонент.

Схожей позиции придерживаются исследователи Бородакий Ю.В. и Добродеев А.Ю., определяя кибербезопасность как «свойство или состояние системы сохранять надежность и функциональную устойчивость в условиях современного противоборства» [4].

Профессор Технологического института Стивенс и независимый консультант Правительства США по вопросам кибербезопасности Jennifer L. Bayuk и Директор национального офиса по кибербезопасности Joseph Weiss предлагают понимать под кибербезопасностью «возможность контролировать доступ к сетевым системам и к информациям, содержащимся в них» [5].

Paul Rohmeyer профессор Технологического университета Стивенс и эксперт в области кибербезопасности Jeffrey Schmidt, предлагают понимать под «кибербезопасностью» состояние защищенности глобальной сети интернет [5].

Из представленных доктринальных положений можно сделать вывод о том, что кибербезопасность представляет собой совокупность мер и технологий, направленных на обеспечение защиты информационных систем и данных в условиях информационного противоборства. В определениях выделяется информационно-технический компонент, что подчеркивает важность использования современных технологий и методов для обеспечения безопасности. Некоторые исследователи сосредотачивают внимание на защите глобальной сети интернет как ключевого аспекта кибербезопасности. Кроме того, понимание кибербезопасности не ограничивается только академическими исследованиями. Международные правовые документы также вносят свой вклад в определение этого понятия.

В рекомендациях Международного Союза Электросвязи X.1205 МСЭ-Т «кибербезопасность» определяется как «набор средств, стратегий, принципов обеспечения безопасности, мер по обеспечению безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, практического опыта, страхования, технологий, которые могут быть использованы для защиты киберпространства» [4].

В Концепции «Киберщит Казахстан» 2017 «кибербезопасность» определяется как «состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационная безопасность в сфере информатизации» [6].

В Глобальной стратегии по киберпространству 2021, принятой Генеральной Ассамблеей ООН, кибербезопасность рассматривается как важный аспект обеспечения международного мира и безопасности. В данном контексте кибербезопасность определяется как «обеспечение стабильности и защиты информационных и коммуникационных технологий от киберугроз» [7]. Этот подход выходит за рамки технических аспектов и включает в себя также аспекты международных отношений, права и политики. Данный документ, как и большинство резолюций ООН, посвященных данной сфере, имеет характер «мягкого права».

В рамках ООН вопросы «кибербезопасности» являются составной частью вопросов «информационной безопасности», по поводу которой международное сообщество все еще не выработало единого подхода в понимании. Как считают исследователи Крутских А. и Шакиров О., ни работа группы правительственных экспертов, ни труды рабочей группы открытого состава ООН, занимающихся вопросами информационной безопасности, не принесли значительных сдвигов в решении данной проблемы [8].

Таким образом, ключом к определению «кибербезопасности» становится «киберпространство». В стандарте в области кибербезопасности ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности», «киберпространство» определяется как «комплекс среды и, как следствие в результате взаимодействия людей, программного обеспечения и услуг в Интернете с помощью технологий, устройств и сетей, подключенных к ней, которых не существует в любой физической форме» [4]. Обсуждение кибербезопасности требует не только понимания технических аспектов, но и учета международно-правовых норм и документов, которые влияют на формирование стратегий и политики в области

кибербезопасности, что подчеркивает важность комплексного подхода к рассмотрению этой проблемы

В ходе анализа научных работ различных исследователей, серий резолюций ООН «Достижения в области информатизации и телекоммуникации», «Создание глобальной культуры кибербезопасности» были выделены такие виды киберугроз как кибервойна, кибершпионаж, киберпреступления, кибертерроризм [9].

Киберпреступления - любое противоправное действие, совершенное в киберпространстве (нарушение права свободы слова, совести и религии в интернете, онлайн-мошенничества, кража персональных данных и т.д.). В резолюциях ООН по глобальной культуре кибербезопасности, где под данным термином понимаются международно-противоправные деяния с использованием икт, которые угрожают международной безопасности и безопасности отдельных государств [9].

Кибер-конфликты/кибервойны - общее название для конфликтов, которые включают в себя технологии икт как средства или цели [9].

Кибертерроризм - в рамках резолюций ГАООН по достижениям в сфере информатизации и телекоммуникации, под данным термином понимается использование террористами киберпространства для совершения международно-противоправных действий [10].

Кибершпионаж - шпионаж, совершаемый суверенным государством в отношении другого суверенного государства в киберпространстве [9].

Следовательно, **киберугрозы** можно рассматривать как деяния, нарушающие целостность киберпространства и угрожающие как международной, так и национальной безопасности. Подобные угрозы представляют собой различные формы кибератак, направленных на причинение вреда государственным, корпоративным или частным субъектам.

Одним из важных аспектов в контексте современного мирового порядка является кибербезопасность инвестиционных объектов. Инвестиционные объекты, такие как биржи, фондовые рынки, финансовые институты и предприятия, становятся мишенями для кибератак из-за их значимости для экономики и финансового рынка.

Согласно исследованию «Опрос инвесторов 2018» 41% инвесторов выразили обеспокоенность киберугрозами и обозначили их в качестве одного из главных угроз для бизнеса. Согласно исследованию, CGI и Oxford Economics была установлена "существенная связь между серьезным кибератакой и динамикой курса акций компании". Исследование показало, что цены на акции падают в среднем на 1,8% на постоянной основе в результате кибератак. Автор исследования подводит итог, что стоимость акции 2013-2017 годы упала на 52, 4 млрд долларов [10].

Инвестиционные активы иностранных компаний также становятся объектами киберпреступлений. Так, компания австралийская компания DP World, имеющий иностранных инвесторов, подверглась кибератаке в результате которой была парализована информационная инфраструктура компании. Согласно оценке экспертов, результатом этого стали рост цен на товары, транспортируемые компанией [11].

10 декабря 2021 года шведский производитель Volvo Cars заявила, что одно из его файловых хранилищ подверглось кибератаке. Хакерам удалось похитить данные исследований и разработок. 3 января 2023 года стало известно о том, что неизвестный злоумышленник (или группа киберпреступников) выставил на продажу на одном из хакерских форумов конфиденциальные данные, украденные у автопроизводителя Volvo [12].

Таким образом, мы видим, что кибератаки представляют серьезные угрозы для успешной и эффективной деятельности инвесторов. Показательным представляется судебный иск IRA Financial Trust против Trust Company 2021. IRA Trust Fund представляет собой специальный вид пенсионных счетов в США, позволяющих инвестировать средства в различные финансовые инструменты. Gemini, криптовалютная биржа, выбрана IRA для защиты криптоактивов клиентов. Однако, переход на API Gemini ослабил безопасность,

создав единственную точку отказа и уязвимость для хакеров. Хакеры, получив мастер-ключ, осуществили множество транзакций, переведя миллионы долларов активов клиентов на один счет и выведя их. Gemini не обнаружила эти переводы, игнорируя системы защиты от мошенничества. Согласно претензиям IRA Financial Trust компания Gemini, позиционирующая себя как «самая надежная» на рынке, не смогла обеспечить надлежащую кибербезопасность активов, тем самым нарушив свои обязательства. Дело все еще не получила своего судебного разрешения, но несмотря на это данный кейс очень показателен в плане демонстрации ущерба, который могут нанести киберугрозы объектам инвестирования [13].

Одной из немаловажных вызовов для международного инвестиционного права, связанных с киберугрозами, в том числе становится обеспечение конфиденциальности и прав интеллектуальной собственности. Кибератаки могут привести к утечке конфиденциальной информации, включая коммерческие секреты и интеллектуальную собственность, что может негативно сказаться на инвестиционных сделках и отношениях между странами.

Более того киберугрозы увеличивают риск для инвесторов и могут привести к сокращению инвестиций в страны, страдающие от кибератак. Согласно исследованиям Comparitech наименее кибербебезопасными странами оказались Таджикистан, Бангладеш, Китай, Вьетнам, Алжир, Индия, Бразилия, Казахстан, Узбекистан, Эквадор и Морокко, Россия, Шри-ланка, Кыргызстан и т.д., что в данном контексте говорит о снижении инвестиционной привлекательности данных стран для зарубежных инвесторов [14].

Исследования и реальные случаи кибератак показывают, что киберугрозы становятся всё более серьезной угрозой для инвесторов и компаний. Отсутствие адекватной кибербезопасности может привести к серьезным последствиям, включая снижение стоимости акций и ущерб для бизнеса. Кейс IRA Financial Trust против Trust Company 2021 выделяет важность не только принятия мер по защите от киберугроз, но и постоянного мониторинга и обновления систем безопасности. Это подчеркивает необходимость активного внедрения современных технологий и стратегий для защиты инвестиционных активов от потенциальных кибератак.

Подводя итоги, на основе анализа международно-правовых документов, можно сделать вывод, что «киберугрозы» это деяния, нарушающие целостность киберпространства, где под «киберпространством» следует понимать «комплекс среды и, как следствие в результате взаимодействия людей, программного обеспечения и услуг в Интернете с помощью технологий, устройств и сетей, подключенных к ней, которых не существует в любой физической форме».

В целом можно выделить несколько типов современных киберугроз: кибервойна, кибершпионаж, киберпреступления, кибертерроризм.

На основе анализа выводов и статистики различных финансовых учреждений мы убедились в широкой распространенности киберпреступлений в инвестиционной сфере, а также в больших масштабах наносимого ущерба. Также был рассмотрен судебный иск IRA financial trust против Gemini, суть которого заключалась в том, что вторая компания не предоставила адекватные меры безопасности, согласно заключенному договору. Несмотря на то, что оба юридических лица в данном деле зарегистрированы в США и данный иск не носит международного характера, это, однако, не отрицает той вероятности, что аналогичные дела могут быть возбуждены против иностранных инвесторов или при их участии, что говорит о серьезных угрозах и вызовах для международного инвестиционного права.

В ходе исследования были выделены несколько проблемных аспектов, возникающих в контексте киберугроз для международного инвестиционного права.

Во-первых, по сей день отсутствуют международно-правовых механизмы регулирования киберпространства на уровне ООН(имеющие обязательную юридическую силу). Так ни группа правительственных экспертов ООН, ни рабочая группа открытого

состава ООН не пришли к единому пониманию термина «информационной безопасности», что осложняет дальнейшую работу по кодификации киберпространства.

Во-вторых, киберугрозы становятся серьезным вызовом для международного инвестиционного права, особенно в контексте обеспечения конфиденциальности и защиты прав интеллектуальной собственности. Потенциальные кибератаки могут привести к утечке чувствительной информации, включая коммерческие секреты и интеллектуальные активы, что негативно сказывается на инвестиционных отношениях между странами.

В-третьих, увеличение риска для инвесторов из-за киберугроз может снизить интерес к инвестициям в страны, страдающие от таких атак. Недавнее исследование показало, что страны с низким уровнем кибербезопасности, такие как Таджикистан, Бангладеш, Китай, Вьетнам и другие, могут стать менее привлекательными для зарубежных инвесторов. Это создает реальную угрозу для экономического развития и международного инвестиционного сотрудничества этих стран.

Список использованных источников

1. Мировая экономика страдает из-за кибератак [Электронный ресурс].- Режим доступа: https://limex.com/ru/profile/213608641/7089898/full/ .- Дата обращения: 04.03.2024.
2. Отчет: кибератаки на биржи ценных бумаг могут нанести серьезный ущерб рынку [Электронный ресурс].- Режим доступа: https://www.securitylab.ru/news/442499.php. -Дата обращения: 04.03.2024.
3. Каратаева Л.Р. Информационная безопасность vs кибербезопасность: проблемы определения // Казахстан-Спектр, №1, 2014, С. 5-13.
4. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века // Вопросы кибербезопасности, №1, 2013, С.2-9.
5. Jennifer L. Bayuk Jason Healey Paul Rohmeyer Marcus S.Sachs Jeffrey Schmidt Joseph Weiss Cyber security policy Guidebook. - A John Wiley & Camp; Sons, Inc., Publication, 2022, 267 p.
6. Об утверждении концепции кибербезопасности («Киберщит Казахстан») [Электронный ресурс].- Режим доступа: https://adilet.zan.kz/rus/docs/P1700000407 . - Дата обращения: 02.03.2024.
7. Глобальная стратегия по кибербезопасности ООН 2021 [Электронный ресурс].- Режим доступа: https://www.un.org/counterterrorism/cybersecurity / - Дата обращения: 02.03.2024.
8. Шакиров О. Широкий киберконсенсус [Электронный ресурс].- Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/shirokiy-kiberkonsensus/ - Дата обращения: 02.03.2024.
9. Крутских А.В. Международная информационная безопасность: Теория и практика: В трех томах. Том 2: Сборник документов (на русском языке). – М.: «Аспект Пресс», 2019, 784с.
10. Инвесторы назвали кибератаки главной угрозой для бизнеса [Электронный ресурс].- Режим доступа: https://forbes.kz/process/technologies/investoryi_nazvali_kiberataki_glavnoy_ugrozoy_dlya_biznesa. - Дата обращения: 02.03.2024.
11. DP World [Электронный ресурс].- Режим доступа: https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:DP_World/ - Дата обращения: 05.03.2024.
12. Volvo Cars [Электронный ресурс].- Режим доступа: http://surl.li/rryzv Дата обращения: 05.03.2024.
13. Complaint [Электронный ресурс].- Режим доступа: https://www.documentcloud.org/documents/22054489-ira-v-gemini-complaint - Дата обращения: 05.03.2024.

14. Paul Bischof Which countries have the worst (and best) cybersecurity? Global rankings Режим доступа: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/ - Дата обращения: 06.03.2024.

УДК 341.6

«КОДИФИКАЦИЯ МЕЖДУНАРОДНОГО ЧАСТНОГО ПРАВА: РОЛЬ И ДЕЯТЕЛЬНОСТЬ КОМИССИИ МЕЖДУНАРОДНОГО ПРАВА ООН»

Шалгымбаева Алина Нурлановна
alinas0901@gmail.com
Магистрант 1 курса образовательной программы «7М04202» Международное право
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – Е. М. Абайдельдинов

В данной научной статье рассматривается важность кодификации международного частного права и роль, которую играет в этом процессе Комиссия международного права Организации Объединенных Наций. Автор анализирует исторические основы, функции и активности Комиссии в контексте разработки и утверждения стандартов международного частного права. Основываясь на актуальных документах и литературных источниках, статья выделяет значимость усилий Комиссии для обеспечения стабильности и предсказуемости в международных отношениях, а также ее вклад в укрепление правового порядка в мировом масштабе.

Международное частное право играет ключевую роль в регулировании отношений между субъектами различных юрисдикций. В условиях глобализации и увеличения трансграничных взаимодействий важно иметь унифицированные правовые нормы для разрешения споров и обеспечения справедливости. Кодификация международного частного права становится необходимостью для создания единого правового пространства и обеспечения защиты интересов всех участников международных отношений.

Современный этап развития МЧП представляется чрезвычайно благоприятным для научного исследования феномена кодификации в связи с наличием большого объема нового и мало изученного нормативно-правового материала.

Как отмечает К.К.Рашидов, ускорение процессов кодификации в международном частном праве объясняется такими факторами, как усиление влияния транснациональных компаний в системе международных экономических отношений, усиление участия государств в экономических отношениях, активный процесс уникации.

Другое мнение по вопросу кодификации связано с вопросом определенности, реализуемой кодификацией, и, по мнению ученых, выступающих против кодификации, определенность, реализуемая кодификацией, существенно ограничивает свободу выбора правовой системы, а следовательно, и действие принципа справедливости, на которую должен опираться суд при разрешении коллизионного права. Они утверждают, что четкое законодательное регулирование лишает судью возможности учитывать реальную ситуацию в каждом отдельном случае и проявлять необходимую гибкость. Это рассуждение справедливо применительно к странам общего права. Представители доктрины общего права выдвигают точку зрения, что строгое определение коллизионных привязок не обеспечивает всестороннюю оценку дела и, как следствие, справедливый результат. По мнению