ТӘУЕЛСІЗДІК ЖЫЛДАРЫ ҚАЗАҚСТАН

РУХАНИ ЖАҢҒЫРУ

Фараби оқулары

Қазақстан 2050

ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛЬ-ФАРАБИ
AL-FARABI KAZAKH NATIONAL UNIVERSITY

ХАЛЫҚАРАЛЫҚ ҚАТЫНАСТАР ФАКУЛЬТЕТІ
ФАКУЛЬТЕТ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ
FACULTY OF INTERNATIONAL RELATIONS

«ФАРАБИ ӘЛЕМІ»

атты студенттер мен жас ғалымдардың
халықаралық ғылыми конференция
МАТЕРИАЛДАРЫ
Алматы, Қазақстан, 6-8 сәуір 2021 жыл

МАТЕРИАЛЫ
международной научной конференции
студентов и молодых ученых
«ФАРАБИ ӘЛЕМІ»
Алматы, Казахстан, 6-8 апреля 2021 года

MATERIALS
International Scientific Conference
of Students and Young Scientists
«FARABI ALEMI»
Almaty, Kazakhstan, April 6-8, 2021

СОВРЕМЕННОЕ СОСТОЯНИЕ КИБЕРБЕЗОПАСНОСТИ И РЕГЛАМЕНТАЦИЯ ТРЕБОВАНИЙ К ЕЁ ОСУЩЕСТВЛЕНИЮ В ИНДИИ

Бисалиев Марлен,
магистрант 1 курса специальности «Международное право»
Казахского национального университета им. аль-Фараби
Научный руководитель: д.ю.н., профессор Шакиров К.Н.,

Введение. Развитие новых технологий, особенно в сфере IT-технологий, создают проблемы в новых областях национальной безопасности и государственной политики. В связи с этим государства на уровне национального и международного права разрабатывают законодательные и правоприменительные механизмы для борьбы с данной угрозой.

Целями субъектов кибератак являются организации и лица из самых разных сфер, таких, как правительственные учреждения, банки, военные организации, частные компании, сектор образования, научно-исследовательские структуры, дипломатические представительства, представители оппозиции и т.п.

Международно-правовое сотрудничество государств в сфере борьбы с киберпреступностью пока ограничено, но считается важным. В частности, подобное сотрудничество представляется особенно необходимым, чтобы позволить государствам создать единую правовую основу для законного привлечения и развития новейших информационных технологий, исключения любого противоправного технологического вмешательства во внутренние дела стран и установление ответственности за любую попытку покушения на их кибербезопасность.

Теоретическое обоснование. О том, что в направлении установления международной кибербезопасности предпринимаются определённые усилия свидетельствуют приводимые ниже факты.

Шесть стран (Казахстан, Россия, Таджикистан, Узбекистан, Кыргызстан, Китай) в рамках Шанхайского общества сотрудничества (ШОС) подписали «Правила поведения в области обеспечения международной информационной безопасности». Правила обязывают государства-участников использовать приемлемые системы защиты информации, не иметь средств информационного оружия и источников угрозы от них. Документ был подан в 2015 году в ООН и ратифицирован шестью государствами.

Организация исламского сотрудничества (ОИС) одобрила и приняла Резолюцию о «Сотрудничестве групп реагирования на компьютерные чрезвычайные ситуации (OIC-CERT) между странами-членами ОИС». Резолюция была одобрена на 35-й сессии Совета министров иностранных дел встречи ОИС в Кампале, Уганда, 18-20 июня 2008 г., Резолюция № 3/35-INF. OIC-CERT открыта для частного сектора и специалистов по информационной безопасности всех стран-членов ОИС. Цель состоит в том, чтобы способствовать беспрепятственному сотрудничеству и взаимодействию между группами реагирования и профессионалами в области информационной безопасности среди участников для достижения целей OIC-CERT, а именно:

- укрепление отношений между CERT в странах-членах ОИС;
- улучшение обмена информацией в области кибербезопасности;
- предотвращение и/или сокращение киберпреступлений;
- содействие образовательным и просветительским программам;
- содействие совместным исследованиям и разработкам технологий;
- предоставление кибернетических каналов связи между странами-членами.

В Стратегии ОДКБ от 2016 года подчеркивается, что формирование безопасного информационного пространства государств-членов ОДКБ является основной стратегической целью информационной безопасности ОДКБ, что, несомненно, включает в себя также киберпространство. При этом, согласно Стратегии, ОДКБ должна предпринять следующий комплекс действий для обеспечения комплексной информационной безопасности государств-членов:

- формирование системы информационной безопасности государств-членов ОДКБ;
- развитие межгосударственной информационной безопасности;
- межведомственное сотрудничество в области информационной безопасности;
- модернизация механизмов противодействия угрозам в информационном пространстве;
- проведение совместных мероприятий по противодействию и нейтрализации угроз в информационно-коммуникационной сфере ОДКБ;
- взаимодействие в вопросах обеспечения международной информационной безопасности;

- разработка согласованных правил поведения в информационном пространстве и продвижение их на международный уровень;
- разработка условий для создания основы для согласованной информационной политики.

Статья XXI ГАТТ допускает ряд «исключений безопасности» из обязательств ВТО. До недавнего времени это исключение использовалось нечасто не только потому, что стороны не хотели подвергать интересы национальной безопасности проверке урегулирования споров, но отчасти из-за опасений, что это исключение может создать очень большую дыру в торговой системе.

Комиссия ВТО 2019 года по делу России и Украины четко дала понять, что исключение в отношении национальной безопасности ГАТТ не является самооценкой и что комиссии будут делать объективную оценку того, имели ли место такие квалифицирующие события, как «чрезвычайная ситуация в международных отношениях». Эта оценка усложняется в контексте кибербезопасности, поскольку исключения для национальной безопасности и общие положения об исключениях в ВТО и в соглашениях о свободной торговле размываются из-за увеличения кибер-рисков со стороны государственных и негосударственных субъектов. Меры по устранению кибер-рисков становятся все более общими для экономики. Для установления границ потребуется общее глобальное определение области кибербезопасности.

Дискуссия. Международный арбитраж – это механизм, к которому частные стороны и государственные организации чаще всего прибегают для разрешения трансграничных споров. Арбитражные решения признаются эквивалентными судебным решениям и могут приводиться в исполнение в 160 юрисдикциях в соответствии с Нью-Йоркской конвенцией 1958 года. Республика Казахстан присоединилась к Нью-Йоркской конвенции 1958 года в 1995 году. В связи с глобализацией мировой экономики и преимуществами международного арбитража, включая возможность принудительного исполнения, нейтралитет, эффективность, гибкость и конфиденциальность – за последние несколько десятилетий он продемонстрировал экспоненциальный рост.

Кибер-апелляционный трибунал Индии был создан в соответствии с Законом об информационных технологиях под эгидой Контролера удостоверяющих органов (Controller Of Certifying Authorities) в Индии. Первый и единственный кибер-апелляционный трибунал в стране был учрежден Центральным правительством Индии в соответствии с положениями, содержащимися в разделе 48 (1) Закона об информационных технологиях 2000 года.

Центральное правительство также должно указать в уведомлении, указанном в подразделе (1), вопросы и места, в отношении которых кибер-апелляционный трибунал может осуществлять юрисдикцию.

Кибер-апелляционный трибунал в целях выполнения своих функций в соответствии с Законом об информационных технологиях от 2000 года, те же полномочия, которые наделены Гражданским судом в соответствии с Гражданским процессуальным кодексом 1908 года. Однако применяется процедура, установленная Гражданским процессуальным кодексом 1908 года, но в то же время трибунал руководствуется принципами естественного права.

Первоначально в состав трибунала входило только одно лицо — Председатель, который назначался Центральным правительством. После этого в 2008 году в Закон были внесены поправки, согласно которым раздел 49, который предусматривает состав Кибер-апелляционного суда, был изменен.

Согласно измененному разделу, трибунал должен состоять из председателя и такого количества других членов, какое Центральное правительство может назначить путем уведомления в официальном вестнике. Выбор председателя и членов трибунала производится Центральным правительством в консультации с Главным Судьей Индии.

Любое лицо, пострадавшее из-за приказа Контролера или судебного следователя, назначенного в соответствии с Законом об информационных технологиях 2000 года, может подать апелляцию в трибунал в течение 45 дней с момента получения копии приказа Контролера или судебного следователя.

Центральное правительство может путем уведомления в Официальном вестнике назначить Контролера сертифицирующих органов, а также заместителей и помощников контролеров, чья квалификация, опыт и условия службы могут быть предписаны Правительством, для выполнения функций, предусмотренных в разделе 18 Закона. Закон дает Центральному правительству право назначать должностное лицо не ниже уровня директора правительства Индии или аналогичное должностное лицо правительства штата в качестве судебного должностного лица для расследования того, нарушило ли какое-либо лицо какие-либо положения Закона. Закон или любое правило, постановление, распоряжение или приказ, принятый в нем, в соответствии с которым он обязан

выплатить штраф или компенсацию. Судебный чиновник, назначенный в соответствии с Законом, может осуществлять юрисдикцию для вынесения решения по делам, в которых требование о возмещении ущерба или ущерба не превышает 50 миллионов рупий. В отношении иска о возмещении ущерба или ущерба, превышающего 50 миллионов рупий, юрисдикция передается компетентному суду.

Заключение. Создание кибер-апелляционного трибунала может иметь положительный результат. Механизмы правового регулирования могут быть повышены путем повышения осведомленности общественности и властей, а также путем привлечения компетентных кадров. Важно улучшить технологические возможности, чтобы справиться с возникшей ситуацией кибербезопасности. Необходимо поддерживать целостность, конфиденциальность и аутентификацию каналов и процессов связи. В отношении определенных видов правонарушений существует потребность в более быстром принятии решений в определенных судах. Неотъемлемая часть в регламентации вопросов кибербезопасности является международное сотрудничество.

Список использованной литературы

1. “О Присоединении Республики Казахстан к Конвенции о Признании и Приведении в Исполнение Иностранных Арбитражных Решений 1958 Года – ИПС ‘Әділет.’” Дата обращения: 20.03.2021г.
2. http://adilet.zan.kz/rus/docs/U950002485_
3. “Правила поведения в области обеспечения международной информационной безопасности (МИБ)”. Дата обращения: 20.03.2021г.
4. https://digitallibrary.un.org/record/786846/files/A_69_723-RU.pdf?version=1
5. “Стратегия Коллективной Безопасности Организации Договора о Коллективной Безопасности на период до 2025 года”. Дата обращения: 20.03.2021г. https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/
6. “INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19.” Дата обращения: 20.03.2021г. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.
7. Katzan, Harry. “Contemporary Issues in Cybersecurity.” Journal of Cybersecurity Research (JCR) 1, no. 1 (2016): 1–6.
8. “Ministry of Law, Justice and Company Affairs (Legislative Department) | Ministry of Electronics and Information Technology, Government of India”. Дата обращения: 20.03.2021г.
9. https://www.meity.gov.in/content/ministry-law-justice-and-company-affairs-legislative-department-0
10. RESOLUTIONS ON INFORMATION AFFAIRS. 35th SESSION OF THE COUNCIL OF FOREIGN MINISTERS, 2008. Дата обращения: 20.03.2021г.
11. https://www.oic-oci.org/docdown/?docID=427&refID=30
12. Sheldon, John B. “Geopolitics and Cyber Power: Why Geography Still Matters.” *American Foreign Policy Interests* 36, no. 5 (2014): 286–93.
13. Van Harten, Gus. “The Public-Private Distinction in the International Arbitration of Individual Claims against the State.” International and Comparative Law Quarterly, 2007, 371–93.
14. “WTO | Legal Texts – Marrakesh Agreement”. Дата обращения: 20.03.2021г. https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXXI
15. “WTO | Dispute Settlement – the Disputes – DS512”. Дата обращения: 20.03.2021г. https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds512_e.htm