Международное право
Правильная ссылка на статью:
Шинкарецкая Г.Г. — Проблема выработки определения кибератаки // Международное право. – 2023. – № 2.
DOI: 10.25136/2644-5514.2023.2.40051 EDN: NYDJJZ URL: https://nbpublish.com/library_read_article.php?id=40051

Проблема выработки определения кибератаки

Шинкарецкая Галина Георгиевна

доктор юридических наук

главный научный сотрудник, Институт государства и права Российской академии наук

119019, Россия, г. Москва, ул. Знаменка, 10

gshinkaretskaya@yandex.ru

Статья из рубрики "Теория и философия международного права"

DOI:

10.25136/2644-5514.2023.2.40051

EDN:

NYDJJZ

Дата направления статьи в редакцию:

25-03-2023

Дата публикации:

08-04-2023

Аннотация: В статье рассматриваются проблемные аспекты в части выработки определения кибератаки. Отмечается, что такового рода противоправные действия способные вывести из строя ядерные центрифуги, системы противовоздушной обороны и электрические сети и т.д., бесспорно, представляют серьезную угрозу национальной безопасности. В сущности, по своей разрушительной силе, кибератаки приближаются к вооруженным действиям. Констатируется, что в международном праве пока нет договоров или иных нормативных документов, способных регулировать международное сотрудничество в целах предотвращения и ограничения кибератак. Для более эффективного противодействия кибератакам необходима новая всеобъемлющая правовая база как на внутреннем, так и на международном уровнях. Методологической базой исследования являются всеобщий (диалектический), логический, формально-юридический, сравнительно-правовой, герменевтический методы. Автором фиксируется важность использования теоретико-правовых наработок в сфере информационной безопасности в правотворческой деятельности. В исследовании обозначены основные предлагаемые в современной научной литературе теоретические подходы к определению понятия "кибератака", делается попытка отграничить его от понятий "кибервойна", "киберпреступление" и "киберпреступность". Подчеркивается мысль, что

международные усилия по регулированию кибератак должны начинаться с соглашения об определении кибератаки, киберпреступности и кибервойны. Это заложило бы основу для расширения международного сотрудничества в области обмена информацией, сбора доказательств и уголовного преследования лиц, причастных к кибератакам, и что более важно, для нового международно-правового акта о кибератаках.

Ключевые слова:

кибератаки, информационные системы, кибертехнологии, киберпреступность, предотвращение кибератак, национальная безопасность, компьютерные сети, Интернет, информационное право, международно-правовое регулирование

XXI век открыл новую страницу в международной преступности, а именно — почти повседневным явлением стали хакерские атаки, сначала как средство ограбления счетов и аккаунтов граждан, а затем – как средство враждебного воздействия на компьютерные сети одного государства со стороны другого с целью внести изменения, разрушить или повредить их. Есть данные о том, что примерно более тридцати стран обладают соответствующими возможностями [25, p. 1023]. Поскольку современные системы управления любого государства – в транспорте, энергетике, здравоохранении и т.д. – всегда включают в себя компьютерные сети, хакерская атака на такие сети становится чрезвычайно вредоносной [14, с. 35].

Нападения на компьютерные системы предпринимались в нашем веке неоднократно; самой заметной по масштабам и демонстративности стала атака на центрифуги Ирана в 2010 г., которую приписывают Израилю [26]. Орудием этой атаки стал так называемый компьютерный "червь" Stuxnet. Несколько месяцев спустя все население Бирмы было отключено от Интернета перед первыми национальными выборами в стране за двадцать лет [18]. В наше время ежегодно фиксируется множество атак, направленных непосредственно против государств или их органов.

К сожалению, международное сотрудничество в области противодействия кибератаким затрудняется совершенно недостаточным международно-правовым регулированием. Достижение организационно-правового режима информационной безопасности – сложная задача [11, с. 45; 17, с. 36-37; 16, с. 11]. При этом надо понимать, что угрозы информационной безопасности - это оборотная сторона использования информационных технологий [15, с. 129].

На сегодняшний день в международном праве почти нет соответствующих правовых норм, которые бы способствовали противодействию кибератак в сети Интернет. Одно из затруднений – отсутствие согласованного определения кибератаки, что затрудняет специалистам разных стран приходить к каким-то общим рекомендациям. Новые понятия и термины не имеют четкого соответствия в разных языках и переводятся пока только примерно: «cyber attacks» и «cyber war» («кибератаки — кибернетические нападения» и «киберентические» или «компьютерные войны»). Обозначаемые ими недружественные действия в отношении компьютерных систем управления часто называют «information attacks» («информационные атаки») или «information wars» («информационные войны»).

Между тем наличие ограниченного и выверенного объекта регулирования в любой отрасли права – непременное условие его эффективности.

Пока можно рассмотреть лишь некоторые доктринальные предложения. Одно из наиболее часто цитируемых определений сделано американским специалистом по международной безопасности Ричардом Кларком: «Действия одного государства по проникновению в компьютеры или сети другой страны с целью нанесения ущерба или нарушения" [19, p. 6]. Бывший директор ЦРУ Майкл Хейден говорил о кибервойне как о "преднамеренной попытке вывести из строя или уничтожить компьютерные сети другой страны" [22]. Однако в этих определениях не проводится различия между киберпреступностью, кибератакой и кибервойной, поэтому они могут применяться слишком широко.

Первое официальное определение кибератаки было дано в 2011 г. в Справочнике по кибероперациям Министерством обороны США: это такие операции, *в которых задействованы «электронные средства для получения доступа к информации или внесения изменений в информацию, содержащуюся в информационной системе, которая избрана целью воздействия, без разрушения ее физических компонентов»* [21, p. 5]. В данном определении целью атаки подразумевается воздействие только на критически важные системы.

Более широкий подход принят Шанхайской организацией сотрудничества, которая выразила «обеспокоенность по поводу угроз, связанных с возможным использованием новых информационных и коммуникационных технологий и средств в целях, несовместимых с обеспечением международной безопасности и стабильности как в гражданской, так и в военной сферах» [7]. "Информационная война" определяется в Соглашении как противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны». Более того, в нем одной из главных угроз информационной безопасности определено распространение информации, наносящей вред «социально-политическим, социальным и экономическим системам, а также духовным, нравственным и культурным сферам других государств» [7].

Таким образом, Шанхайская организация сотрудничества считает необходимым проявление широкого подхода к понятию кибератаки которое охватывает использование кибертехнологий для подрыва политической стабильности. Правда, некоторыми авторами высказывалось опасение того, что такой подход может вести к оправданию политической цензуры в Интернете [23]. Очевидно, в основе таких опасений лежит опыт усилий подавления политических организаций с использованием новых средств массовой информации в Иране, Египте и других странах.

Попытаемся проанализировать отдельные элементы, которые могут составить искомое определение.

Термин «кибератака» подразумевает требование активного поведения: либо нападение, либо активная защита. Для защиты могут использоваться как активные, так и пассивные оборонительные меры, но пассивная оборона не может составить кибер-атаку.

Атака может быть осуществлена с помощью любого действия — взлома, бомбардировка, порезов, заражениея и так далее — но чтобы быть кибератакой, она должна быть

направлена на подрыв или нарушение функционирования компьютерной сети. Действия вооруженных сил могут быть классифицированы на основе средств нападения. Например, война может быть классифицирована как кинетическая (обычная, физическая) война, биологическая война, химическая война, ядерная война, война на основе разведки, сетевая война или партизанская война.

Действия вооруженных сил определяются также их целью, например, назовем информационную войну, психологическую войну, электронную войну и экономическую войну.

Определение кибератаки по цели имеет первостепенное значение по двум причинам. Во-первых, и это самое важное, этот тип определения просто более интуитивно понятен. Использование компьютерной сети в одном из штатов США для управления беспилотным летательным аппаратом для атаки сухопутного подразделения в Пакистане - это не кибератака; скорее, это технологически продвинутая обычная война. С другой стороны, использование обычной взрывчатки для разрыва подводных сетевых кабелей, по которым передаются информационные пакеты между континентами, является кибератакой [10].

Во-вторых, практика управления вооруженными силами государств показала логичность выделения кибервойск: кроме традиционно существующих военно-морских, военно-воздушных и сухопутных войск в государствах созданы кибервойска, предназначенные действовать в киберпространстве [27].

Важной частью определения кибератаки служит также ее цель - нарушение функционирования компьютерной сети. Это может быть достигнуто различными средствами: используются так называемые черви, вирусы, «Троянские кони». В результате атаки может быть нарушена работаоперационной системы компьютера, приводя к сбоям в работе сети; или операционная система будет цела, но под угрозу поставлена точность обрабатываемой ею информации, она будет восприниматься как работающая правильно, но она будет генерировать неверные ответы.

Кибератака нацелена на компьютерную сеть, то есть систему компьютеров и других устройств, соединенных каналами связи. Часто это соединение производится через Интернет, но существует также множество закрытых сетей, таких как защищенные сети, используемые правительственными учреждениями. Важно иметь в виду, что компьютерные сети есть везде; они управляют лифтами и светофорами, регулируют давление в водопроводных сетях и повсеместно используются в таких бытовых приборах, как мобильные телефоны, телевизоры и даже стиральные машины. Такая ситуация и порождает опасность широкомасштабного ущерба от кибератаки практически во всех сферах человеческой деятельности.

Кибератака от обычного уголовного киберпреступления отличается, как правило, наличием политической цели или цели ущерба национальной безопасности. Любое агрессивное действие, предпринятое от имени государства в киберпространстве, обязательно затрагивает национальную безопасность и, следовательно, является кибератакой, независимо от того, доходит ли оно до уровня кибервойны или нет. Киберпреступление, совершенное негосударственным субъектом в целях политической или национальной безопасности, также является кибератакой. С другой стороны, киберпреступление, которое не совершается по политическим мотивам или в целях нарушения национальной безопасности, как большинство случаев интернет-мошенничества, кражи личных данных и пиратства интеллектуальной собственности, не

соответствуют этому последнему элементу "кибератаки" и, следовательно, являются простым киберпреступлением.

В силу невысокой стоимости и трудности атрибуции деяния, *prima facie* обладающего признаками кибератаки, необходимо выделить такой признак политической кибер-атаки, как ее публично-правовой характер. Поскольку негосударственные субъекты могут совершать или могут быть жертвами кибератак, именно цель, а не субъект, должны отличать кибератаку от простого киберпреступления. Киберпреступность - это широкое понятие, аналитически отличное от кибератаки. Хотя, как и в случае с понятием кибератаки, общепризнанного определения киберпреступности нет, существует признание некоторых элементов киберпреступности. В частности, киберпреступность обычно понимается как использование компьютерных средств для совершения противоправного деяния. Чаще всего киберпреступность определяется как "любое преступление, совершенное или совершаемое с использованием компьютера, сети или иного технического устройства" [20]. Это значит, что киберпреступность, в отличие от кибератаки, определяется ее средствами, то есть компьютерной системой и охватывает очень широкий спектр незаконных действий. К ним обычно относят мошенничество в Интернете, интернет-пиратство, хранение и распространение детской порнографии на компьютере и компьютерное хакерство. При этом компьютерная сеть остается неповрежденной, а цель не имеет политического характера. Наконец, как и все преступления, киберпреступления обычно понимаются как совершаемые отдельными физическими лицами и не от лица государства. Деяние является киберпреступлением только тогда, когда негосударственный субъект совершает деяние, которое квалифицируется как уголовное преступление в соответствии с внутренним или международным правом.

В момент киберсобытия часто не сразу становится очевидным, с каким именно явлением мы имеем дело, и это затрудняет незамедлительное реагирование.

В российском действующем законодательстве [8; 9] пока нет отделения киберпреступлений от кибератак, вернее, все положения относительно неправомерных деяний с использованием информационных технологий относятся к киберпреступлениям [12, с. 25].

В доктрине международного права широко распространено мнение о том, что международное гуманитарное право может применяться к кибератакам без выделения кибер-атак как специального предмета регулирования [13, с. 421-430].

Действительно, в действующих законах и обычаях войны нет специальных правил относительно компьютерных атак. Но это не отменяет действия международного гуманитарного права. Замечательный российский ученый Ф.Ф.Мартенс предложил применять в таких случаях норму, которая получила название «оговорка Мартенса»: отсутствие договорного положения, ясно запрещающего какое-либо определенное поведение во время вооруженного конфликта, не означает, что международное право разрешает его. Эта общепризнанная ныне норма включена в преамбулу Гаагской конвенции 1899 г. "О законах и обычаях сухопутной войны" и затем фигурировала в ряде документах международного гуманитарного права, включая Женевские конвенции 1949 г. [1; 3; 4; 5; 6] и развита в Дополнительном протоколе I к Женевским конвенциям: «В случаях, не предусмотренных настоящим Протоколом или другими международными соглашениями, гражданские лица и комбатантыостаются под защитой и действием принципов международного права, проистекающих из установившихся обычаев, из

принципов гуманности и из требований общественного сознания» (ст. 1.2) [2]. Кроме того, ст. 36 того же Протокола обязывает государств-участников при изучении, разработке, приобретении или принятии на вооружение новых видов оружия, средств или методов ведения войны определить, подпадает ли их применение, при некоторых или при всех обстоятельствах, под запрещения, содержащиеся в Протоколе или в каких-либо других нормах международного права, применяемых ими [2].

Таким образом, можно сделать вывод: международное гуманитарное право распространяется на компьютерные атаки, но предмет регулирования не определен четко. Такое мнение, в целом, господствует и в научной литературе [24, p. 1149].

При этом, вплоть до начала 2000-х гг. казалось достаточным применение международного гуманитарного права по аналогии. В настоящее время, учитывая рост числа и разнообразия пользователей компьютерных сетей, в том числе осуществляющих хакерские атаки; помня о потенциально растущей разрушительной силе кибератак становится все более необходимым принятие международных нормативных документов в области предотвращения и пресечения кибератак. Формулирование понятия и определения кибер-атаки может стать первым шагом к разработке согласованного регулирования.

Библиография

1. IV Гаагская конвенция о законах и обычаях сухопутной войны с приложением: «Положение о законах и обычаях сухопутной войны» от 18 октября 1907 г. [Электронный ресурс]. – URL: https://doc.mil.ru/documents/quick_search/more.htm?id=11967448%40egNPA (дата обращения 06.03.2022).
2. Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов (Протокол I). Женева, 8 июня 1977 г. (с изм. и доп.) [Электронный ресурс]. – URL: https://constitution.garant.ru/act/right/megdunar/2540377/ (дата обращения 06.03.2022).
3. Женевская Конвенция о защите гражданского населения во время войны (Женева, 12 августа 1949 г.) (ст. 158) [Электронный ресурс]. – URL: https://constitution.garant.ru/act/right/megdunar/2540383/ (дата обращения 06.03.2022).
4. Женевская Конвенция об обращении с военнопленными (Женева, 12 августа 1949 г.) (ст. 142) [Электронный ресурс]. – URL: https://constitution.garant.ru/act/right/megdunar/2540382/ (дата обращения 06.03.2022).
5. Женевская Конвенция об улучшении участи раненых и больных в действующих армиях (Женева, 12 августа 1949 г.) (ст. 63) [Электронный ресурс]. – URL: https://constitution.garant.ru/act/right/megdunar/2540380/ (дата обращения 06.03.2022).
6. Женевская Конвенция об улучшении участи раненых, больных и лиц, потерпевших кораблекрушение, из состава вооруженных сил на море (Женева, 12 августа 1949 г.) (ст. 62) [Электронный ресурс]. – URL: https://constitution.garant.ru/act/right/megdunar/2540381/ (дата обращения 06.03.2022).
7. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной

информационной безопасности [Электронный ресурс]. – URL: https://docs.cntd.ru/document/902289626 (дата обращения 06.03.2022).

8. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. № 187-ФЗ (посл. ред.) [Электронный ресурс]. – URL: https://base.garant.ru/71730198/ (дата обращения 06.03.2022).
9. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ (посл. ред.) [Электронный ресурс]. – URL: https://base.garant.ru/12148555/ (дата обращения 06.03.2022).
10. Chairman of the Joint Chiefs of Staff, U.S. Dep't of Defense, National Military Strategy for Cyberspace Operations 15 (2006).
11. Демидов О. Глобальное управление Интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества. - М.: Альпина Паблишер, 2016. - 198 с.
12. Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. – С. 25-33.
13. Конохов М.В., Бутрим И.И. Приоритетные направления сотрудничества Российской Федерации в сфере обеспечения информационной безопасности в рамках региональных объединений: военно-правовые аспекты // Материалы Международной научно-практической конференции Четвертые Бачиловские чтения (февраль 2021). – Саратов: Амирит, 2022. – С. 421-430.
14. Полякова Т.А. Развитие системы информационного права и приоритетные задачи обеспечения информационной безопасности в условиях современных вызовов и угроз // Материалы Международной научно-практической конференции «Четвертые Бачиловские чтения» (февраль 2021). – Саратов: Амирит, 2022. – С. 34-54.
15. Прончев Г.Б., Лонцов В.В., Монахов Д.Н., Монахова Г.А. Проблемы безопасности информационного общества современной России: Монография. - М.: Экон-Информ, 2014. - 215 с.
16. Рыжов В.Б. Информационная безопасность в государствах Европейского Союза: к постановке проблемы // Представительная власть: XXI век: законодательство, комментарии, проблемы. 2018. № 4 (163). – С. 8-12.
17. Стрельцов А.А. Основные проблемы правового обеспечения международной информационной безопасности // Динамика институтов информационной безопасности. Правовые проблемы. Сб. науч. трудов / Отв. ред. Т.А. Полякова, В.Б. Наумов, Э.В. Талапина. – М.: ИГП РАН – Изд-во «Канон+» РООИ «Реабилитация», 2018. - С. 28-37.
18. Burma Hit by Massive Net Attack Ahead of Election [Электронный ресурс] // BBC News (Nov. 4, 2010). URL: http://www.bbc.co.uk/news/technology-11693214 (дата обращения 06.03.2022).
19. Clarke Richard A., Knake Robert K. Cyber war: the next threat to national security and what to do about it. – OUP, 2010. – P. 6.
20. Computer Crime and Intellectual Property Section, Criminal Division, U.S. Dep't of Justice, Prosecuting Computer Crimes (2d ed. 2010).
21. Department of Defense, Office of General Counsel. An Assessment of International Legal Issues in Information Operations. May 1999. [Assessment of International Legal Issues] – P. 5.
22. Extending the Law of War to Cyberspace [Электронный ресурс]. - URL: http://www.npr.org/templates/story/story.php?storyId=130023318 (дата обращения: 06.03.2022).

23. Gjelten Tom. Seeing the Internet as an 'Information Weapon [Электронный ресурс]. Sept. 23, 2010. – URL: http://www.npr.org/templates/story/story.php?storyId=130052701 (дата обращения: 06.03.2022).
24. Jensen E.T. Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations? // 18 American University International Law Review. 2003. V. 18. – P. 1149.
25. Hollis D.B. Why States need an International Law for Information Operations // Lewis and Clark Law Review. 2007. Vol. 11. № 4. – P. 1023.
26. The Stuxnet Worm: A Cyber-Missile Aimed at Iran? [Электронный ресурс] // Economist babbage blogs (Sept. 24, 2010). – URL: http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm (дата обращения: 06.03.2022).
27. War in the Fifth Domain [Электронный ресурс] // Economist. July 1, 2010. – URL: http://www.economist.com/node/16478792 (дата: обращения 06.03.2022).

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предмет исследования в представленной на рецензирование статье составляет, как это следует из ее наименования, "Проблема выработки определения кибер-атаки". Название работы необходимо уточнить ("Проблема выработки определения понятия "кибератака", "Проблема выработки дефиниции понятия "кибератака", "Основные теоретические подходы к определению понятия "кибератака" и т.п.). Несмотря на то, что в сети Интернет часто встречается написание слова "кибератака" через дефис, согласно действующим нормам русского языка это слово пишется слитно. Заявленные границы исследования полностью соблюдены автором.
Методология исследования в тексте статьи не раскрывается, но очевидно, что ученым использовались всеобщий диалектический, логический, формально-юридический, сравнительно-правовой, герменевтический методы исследования.
Актуальность избранной автором темы исследования не подлежит сомнению и обосновывается им следующим образом: "Поскольку современные системы управления любого государства – в транспорте, энергетике, здравоохранении и т.д. – всегда включают в себя компьютерные сети, хакерская атака на такие сети становится чрезвычайно вредоносной [13, с. 35]". Кроме того, "К сожалению, международное сотрудничество в области противодействия кибер-атакам затрудняется совершенно недостаточным международно-правовым регулированием". Следует согласиться с ученым в том, что "Одно из затруднений – отсутствие согласованного определения кибер-атаки, что затрудняет специалистам разных стран приходить к каким-то общим рекомендациям".
В чем проявляется научная новизна исследования, автор прямо не говорит. Фактически она могла бы проявиться в предложенных ученым оригинальных дефинициях понятий "кибератака", "киберпреступление", "киберпреступность", но по каким-то причинам этого не было сделано. Автором выделены отдельные существенные признаки исследуемых понятий, но на этом исследователь остановился. Таким образом, в данном виде представленная на рецензирование статья не вносит особого вклада в развитие наук информационного права и международного публичного права.
Научный стиль исследования выдержан автором в полной мере.

Структура работы вполне логична. Во вводной части статьи автор обосновывает актуальность избранной темы исследования. В основной части работы ученый рассматривает предлагаемые в современной научной литературе теоретические подходы к определению понятия "кибератака", делает попытку отграничить его от понятий "киберпреступление" и "киберпреступность". В заключительной части статьи содержатся выводы по результатам проведенного исследования.

Содержание работы соответствует ее наименованию, но не лишено некоторых недостатков.

Так, автор пишет: "Одно из наиболее часто цитируемых определений сделано американским специалистом по международной безопасности Ричардом Кларком: «Действия одного государства по проникновению в компьютеры или сети другой страны с целью нанесения ущерба или нарушения" [16, p. 6]. Бывший директор ЦРУ Майкл Хейден говорил о кибервойне как о "преднамеренной попытке вывести из строя или уничтожить компьютерные сети другой страны"[8]. Однако в этих определениях не проводится различия между киберпреступностью, кибератакой и кибервойной, поэтому они могут применяться слишком широко". Ученому нужно выделить и другие недостатки приведенных им в качестве примеров определений (как минимум, это неполнота выделения существенных признаков).

Ученый отмечает: "Первое официальное определение кибер-атаки было дано в 2011 г. в Справочнике по кибероперациям Министерством обороны США: это такие операции, в которых задействованы «электронные средства для получения доступа к информации или внесения изменений в информацию, содержащуюся в информационной системе, которая избрана целью воздействия, без разрушения ее физических компонентов» [18; 19]. В данном определении целью атаки подразумевается воздействие только на критически важные системы". Следует добавить, что в данном определении отсутствует указание на негативный характер цели кибератаки.

В целом критический анализ предлагаемых в литературе теоретических подходов к определению понятия "кибератака" должен быть проведен более тщательно.

Автор пишет: "Правда, некоторыми авторами высказывалось опасение того, что такой подход может вести к оправданию политической цензуры в Интернете [20]. Очевидно, в основе таких опасений лежит опыт усилий подавления политических организаций с использованием новых средств массовой информации в Иране, Египте и других странах". Своей точки зрения по данному дискуссионному вопросу ученый не высказывает, а это было бы вполне логичным.

В завершение основной части статьи автору нужно было предложить свои оригинальные дефиниции понятий "кибератака", "киберпреступление", "киберпреступность", но этого почему-то не сделано. Между тем именно в этом могла бы проявиться научная новизна работы.

Библиография исследования представлена 24 источниками (международными документами, нормативными правовыми актами, монографиями, научными статьями, аналитическими материалами, в том числе на английском языке). Этого достаточно и с формальной, и с фактической точек зрения, но некоторые положения работы нуждаются в уточнении и усилении аргументации автора.

Апелляция к оппонентам имеется, как общая, так и частная (Р. Кларк, М. Хейден и др.) и вполне достаточна. Научная дискуссия ведется автором корректно, однако его позиции по спорным вопросам не всегда обоснованы в достаточной степени, на что было указано неоднократно.

Выводы по результатам исследования имеются, но носят общий характер и не обладают свойством научной новизны ("Таким образом, вплоть до начала 2000-х гг. казалось достаточным применение международного гуманитарного права по аналогии. В

настоящее время, учитывая рост числа и разнообразия пользователей компьютерных сетей, в том числе осуществляющих хакерские атаки; помня о потенциально растущей разрушительной силе кибер-атак становится все более необходимым принятие международных нормативных документов в области предотвращения и пресечения кибер-атак. Формулирование понятия и определения кибер-атаки может стать первым шагом к разработке согласованного регулирования"), и потому нуждаются в уточнении и конкретизации. Выводы должны отражать все научные достижения автора по исследуемым им вопросам.

Статья не вычитана ученым. В ней встречаются опечатки, орфографические, пунктуационные, синтаксические, стилистические ошибки.

Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере информационного права и международного публичного права при условии ее существенной доработки: уточнении наименования работы и ее отдельных положений, раскрытии методологии исследования, введении необходимых элементов научной новизны, дополнении и конкретизации выводов по результатам исследования, устранении нарушений в оформлении работы.

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ на статью на тему «Проблема выработки определения кибератаки».

Предмет исследования. Предложенная на рецензирование статья посвящена проблемам «…выработки определения кибератаки». Автором выбран особый предмет исследования: предложенные вопросы исследуются с точки зрения международного права, международного гуманитарного, информационного права, при этом автором отмечено, что «…повседневным явлением стали хакерские атаки, сначала как средство ограбления счетов и аккаунтов граждан, а затем – как средство враждебного воздействия на компьютерные сети одного государства со стороны другого с целью внести изменения, разрушить или повредить их». Изучаются НПА, конвенции, соглашения, имеющие отношение к цели исследования. Также изучается и обобщается большой объем российской и зарубежной (на английском языке) научной литературы по заявленной проблематике, анализ и дискуссия с данными авторами-оппонентами присутствует. При этом автор отмечает: «…международное сотрудничество в области противодействия кибератакам затрудняется совершенно недостаточным международно-правовым регулированием».

Методология исследования. Цель исследования определена названием и содержанием работы: «… наличие ограниченного и выверенного объекта регулирования в любой отрасли права – непременное условие его эффективности», «…Шанхайская организация сотрудничества считает необходимым проявление широкого подхода к понятию кибератаки которое охватывает использование кибертехнологий для подрыва политической стабильности», «Термин «кибератака» подразумевает требование активного поведения: либо нападение, либо активная защита. Для защиты могут использоваться как активные, так и пассивные оборонительные меры, но пассивная оборона не может составить кибер-атаку». Они могут быть обозначены в качестве рассмотрения и разрешения отдельных проблемных аспектов, связанных с

вышеназванными вопросами и использованием определенного опыта. Исходя из поставленных цели и задач, автором выбрана определенная методологическая основа исследования. Автором используется совокупность частнонаучных, специально-юридических методов познания. В частности, методы анализа и синтеза позволили обобщить подходы к предложенной тематике и повлияли на выводы автора. Наибольшую роль сыграли специально-юридические методы. В частности, автором применялись формально-юридический и сравнительно-правовой методы, которые позволили провести анализ и осуществить толкование норм актов российского и международного законодательства и сопоставить различные документы. В частности, делаются такие выводы: «Любое агрессивное действие, предпринятое от имени государства в киберпространстве, обязательно затрагивает национальную безопасность и, следовательно, является кибератакой, независимо от того, доходит ли оно до уровня кибервойны или нет. Киберпреступление, совершенное негосударственным субъектом в целях политической или национальной безопасности, также является кибератакой» и др. Таким образом, выбранная автором методология в полной мере адекватна цели статьи, позволяет изучить многие аспекты темы.

Актуальность заявленной проблематики не вызывает сомнений. Данная тема является важной в мире и в России, с правовой точки зрения предлагаемая автором работа может считаться актуальной, а именно он отмечает «…в международном праве почти нет соответствующих правовых норм, которые бы способствовали противодействию кибератак в сети Интернет. Одно из затруднений – отсутствие согласованного определения кибератаки, что затрудняет специалистам разных стран приходить к каким-то общим рекомендациям». И на самом деле здесь должен следовать анализ работ оппонентов, и он следует и автор показывает умение владеть материалом. Тем самым, научные изыскания в предложенной области стоит только приветствовать.

Научная новизна. Научная новизна предложенной статьи не вызывает сомнения. Она выражается в конкретных научных выводах автора. Среди них, например, такой: «… необходимо выделить такой признак политической кибер-атаки, как ее публично-правовой характер». Как видно, указанный и иные «теоретические» выводы могут быть использованы в дальнейших исследованиях. Таким образом, материалы статьи в представленном виде могут иметь интерес для научного сообщества.

Стиль, структура, содержание. Тематика статьи соответствует специализации журнала «Международное право», так как посвящена проблемам «…выработки определения кибератаки». В статье присутствует аналитика по научным работам оппонентов, поэтому автор отмечает, что уже ставился вопрос, близкий к данной теме и автор использует их материалы, дискутирует с оппонентами. Содержание статьи соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели своего исследования. Качество представления исследования и его результатов следует признать доработанным. Из текста статьи прямо следуют предмет, задачи, методология, результаты исследования, научная новизна. Оформление работы соответствует требованиям, предъявляемым к подобного рода работам. Существенные нарушения данных требований не обнаружены, кроме описок «заражениея» (заражения), «работаоперационной» (работа операционной), «комбатантыостаются» и др.

Библиография достаточно полная, содержит публикации, НПА, конвенции, соглашения, к которым автор обращается. Это позволяет автору правильно определить проблемы и поставить их на обсуждение. Следует высоко оценить качество представленной и использованной литературы. Присутствие научной литературы показало обоснованность выводов автора и повлияло на выводы автора. Труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию многих аспектов темы.

Апелляция к оппонентам. Автор провел серьезный анализ текущего состояния исследуемой проблемы. Автор описывает разные точки зрения оппонентов на проблему, аргументирует более правильную по его мнению позицию, опираясь на работы оппонентов, предлагает варианты решения проблем.

Выводы, интерес читательской аудитории. Выводы являются логичными, конкретными «… учитывая рост числа и разнообразия пользователей компьютерных сетей, в том числе осуществляющих хакерские атаки; помня о потенциально растущей разрушительной силе кибератак становится все более необходимым принятие международных нормативных документов в области предотвращения и пресечения кибератак. Формулирование понятия и определения кибер-атаки может стать первым шагом к разработке согласованного регулирования» и др. Статья в данном виде может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к заявленным в статье вопросам. На основании изложенного, суммируя все положительные и отрицательные стороны статьи «рекомендую опубликовать» с учетом исправления грамматических описок.