https://doi.org/10.17816/RJLS46326

Компьютерные сетевые атаки как акт агрессии в условиях развития современных международных отношений: pro et contra[1]

Лобач Дмитрий Владимирович,
кандидат юридических наук,
доцент кафедры теории и истории российского
и зарубежного права Института права
Владивостокского государственного университета
экономики и сервиса, г. Владивосток
E-mail: dimaved85@mail.ru

Смирнова Евгения Александровна,
кандидат юридических наук,
старший преподаватель кафедры трудового
и экологического права Юридической школы
Дальневосточного федерального университета, г. Владивосток
E-mail: smirnova.ea@dvfu.ru

Аннотация. *В статье анализируются противоречивые подходы к возможному признанию компьютерных сетевых атак в качестве акта агрессии в фокусе современных международных отношений и трендов научно-технического прогресса. Актуализируется вопрос: возможна ли агрессия против другого государства посредством исключительного использования кибернетического оружия? Для решения обозначенной задачи используется схоластический метод ведения дискуссии, при котором выдвигаются два ряда противоречащих аргументов относительно предмета обсуждения, а в заключении резюмируется общий вывод, исходя из частных тезисов. Аргументируется вывод о том, что исторически сложившееся определение агрессии в современных условиях развития научно-технического прогресса не отвечает интересам международного мира и безопасности, так как появляются новые виды силовых форм деструктивного воздействия, которые могут порождать последствия, сравнимые по масштабам и серьезности с последствиями от использования обычных вооружений. Однако остаются отдельные проблемные моменты, возникающие в связи с квалификацией кибератак в качестве преступления агрессии, требующие своего перспективного осмысления и разрешения сообразно с развитием науки международного права и правоприменительной практики в срезе динамики международных отношений.*

Ключевые слова: *преступление агрессии, кибератака, компьютерные сетевые атаки, международное уголовное право, международный мир, безопасность, кибероружие.*

Технологические процессы и новации, происходящие в современном мире, детерминируют качественные изменения в социально-культурной, экономической, политической и других сферах жизни общества. Интенсификация и широкое распространение различных форм электронного взаимодействия и развитие виртуального информационно-коммуникационного пространства приводит к трансформации многих деструктивных явлений социальной действительности, проявляемых в сфере международных отношений. В этом контексте особый интерес представляет такое явление, как кибервойна, так как в современных условиях информационно-коммуникационного усложнения социального взаимодействия актуализируется проблема скрытого использования одним государством своих кибернетических ресурсов против объектов охраняемой инфраструктуры в целях оказания воздействия на политическую независимость другого государства. В этом аспекте закономерна следующая постановка вопроса: возможна ли агрессия против другого государства посредством исключительного использования кибернетического оружия? Ответ

[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».

на обозначенный вопрос позволит определить правомерные границы самообороны в рамках ст. 51 Устава ООН, а также конкретизировать момент состояния войны. Для решения обозначенной задачи представляется целесообразным использовать схоластический метод ведения дискуссии, при котором выдвигаются два ряда противоречащих аргументов относительно предмета обсуждения, а в заключении резюмировать общий вывод, исходя из частных тезисов.

Позиция «pro». На сегодняшний день нормативная определенность преступления агрессии находит свое отражение в Римском статуте Международного уголовного суда от 1998 г. (далее по тексту — Римский статут МУС)[2] Так, в ч. 1 ст. 8-бис данного документа преступление агрессии означает планирование, подготовку, инициирование или осуществление лицом, которое в состоянии фактически осуществлять руководство или контроль за политическими или военными действиями государства, акта агрессии, который в силу своего характера, серьезности и масштабов является грубым нарушением Устава Организации Объединенных Наций. В ч. 2 этой статьи дается легальное определение акта агрессии и представлены его варианты. В частности, акт агрессии означает применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства или каким-либо другим образом, несовместимым с Уставом ООН. К актам агрессии относятся: a) вторжение или нападение вооруженных сил государства на территорию другого государства или любая военная оккупация, какой бы временный характер она ни носила, являющаяся результатом такого вторжения или нападения, или любая аннексия с применением силы на территории другого государства или ее части; b) бомбардировка вооруженными силами государства территории другого государства или применение любого оружия государством против территории другого государства; c) блокада портов или берегов государства вооруженными силами другого государства; d) нападение вооруженными силами государства на сухопутные, морские или воздушные силы или морские и воздушные флоты другого государства; e) применение вооруженных сил одного государства, находящихся на территории другого государства по соглашению с принимающим государством, в нарушение условий, предусмотренных в соглашении, или любое продолжение их пребывания на такой территории по прекращении действия соглашения; f) действие государства, позволяющее, чтобы его территория, которую оно предоставило в распоряжение другого государства, использовалась этим другим государством для совершения акта агрессии против третьего государства; g) засылка государством или от имени государства вооруженных банд, групп, иррегулярных сил или наемников, которые осуществляют акты применения вооруженной силы против другого государства, носящие столь серьезный характер, что это равносильно перечисленным выше актам, или его значительное участие в них.

Обращает на себя внимание, что дефиниция «акт агрессии», как она представлена в ч. 2 ст. 8-бис Римского статута МУС, в рамках широкой интерпретации может охватывать не только традиционные действия, связанные с применением вооруженной силы одним государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства, но также и другие акты, осуществляемые каким-либо другим образом, несовместимым с Уставом ООН. Кроме того, если обратиться к самой резолюции Генеральной Ассамблеи ООН 3314 от 14 декабря 1974 г., то в ст. 4 этого документа закреплено, что перечень актов агрессии, отраженный в ст. 3, не является исчерпывающим, а Совет Безопасности ООН может определить, что другие акты представляют собой агрессию согласно положениям Устава ООН[3].

Между тем отсутствие и в Римском статуте МУС, и в вышеупомянутой резолюции ссылки на компьютерные сетевые атаки в контексте интерпретации понятия вооруженной силы (акта вооруженной силы) еще не означает, что такой вариант акта применения вооруженных сил не приемлем. Прежде всего, следует отметить, что в концептуально-правовом фокусе современная парадигма межгосударственного вооруженного конфликта охватывает не только обычные вооружения, но и различного рода комбинированные, кумулятивные, информационно-коммутационные средства связи, источники информации, сложные многоуровневые системы управления и средства поражения, которые в своей совокупности способствуют повышению темпа операции, эффективности поражения сил противника и синхронизации совместных действий. Учитывая высокие темпы компьютеризации и информационно-коммуникационной интеграции систем управления между разными акторами социальной организации, киберпространство становится новой сферой

[2] Римский статут Международного уголовного суда от 1998 г. Официальный сайт Международного уголовного суда. URL: https://www.icc-cpi.int/resource-library/documents/rs-eng.pdf (дата обращения: 10.12.2020).

[3] Печегин Д.А. Становление международной уголовной юстиции: история вопроса // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2014. № 12 (140). С. 149-153.

ведения боевых действий наряду с наземной, морской и воздушно-космической сферами [1, с. 241], а объекты критической информационной инфраструктуры начинают рассматриваться как потенциальные цели для использования компьютерных сетевых атак [2, с. 264].

В национальной военной политике отдельных государств также прослеживается тенденция к признанию возможности использования компьютерных сетевых атак в качестве новой разновидности вооруженных сил страны. Показательными в этом плане примерами являются военные доктрины США[4], России[5], Китая[6], Индии[7]. Анализ этих документов позволяет прийти к выводу о признании киберпространства в качестве нового театра военно-технологического противодействия в условиях усиливающегося геополитического противостояния, а также стремления указанных мировых держав к созданию, обеспечению и развитию новых видов войсковых структур, которые могут использоваться как для обороны объектов критически важной информационной инфраструктуры, так и для проведения кибератак в отношении вероятного противника. Кроме того, на межгосударственном уровне также наблюдается тенденция к признанию использования компьютерных сетевых атак в качестве акта агрессии. В этом плане обращает на себя внимание принятое не так давно «Таллиннское руководство по применению юридических норм международного права к военным действиям в киберпространстве», где оговаривается, что действия в киберпространстве, которые непосредственно приводят к ранению или гибели людей или существенным разрушениям инфраструктуры, могут рассматриваться как использование силы[8].

В теории международного уголовного права также высказываются мнения о необходимости признания кибератак в качестве возможного акта агрессии. Так, например, Й. Динштейн, исследуя природу вооруженного нападения, приходит к выводу, что компьютерные сетевые атаки могут рассматриваться в качестве разновидности вооруженного нападения, если такие атаки отвечают сущностным характеристикам такого нападения, т.е. они должны влечь материальный ущерб или даже человеческие жертвы. В этом плане, отмечает ученый, кибератаки могут быть квалифицированы как вооруженное нападение, если, например, эти атаки приводят к отключению компьютеров, управляющих гидротехническими сооружениями и плотинами, что приводит к затоплению населенных пунктов [3, p. 212]. Другие авторы (Г. Лилиенталь и А. Нехалуддин) отмечают, что кибератаки могут подорвать информационную безопасность, парализовать военную инфраструктуру и ослабить экономическую систему не в меньшей степени, чем непосредственное применение вооруженных сил [4, p. 390-400]. Ян Браунли, сравнивая по характеру последствий биологическое оружие с информационными кибератаками, приходит к выводу, что последнее также может быть отнесено к применению вооруженных сил [5, p. 34]. Нельзя не согласиться с позицией Тимошкова С.Г., в соответствии с которой современное понятие агрессии может и должно охватывать кибератаки, что обусловлено усложнением межгосударственных отношений в условиях глобализации и развитием научно-технологического прогресса. Вмешательство во внутренние дела государства либо подрыв государственного суверенитета на современном этапе могут быть осуществлены с помощью кибератаки, которую при определенных условиях можно квалифицировать как акт агрессии, имеющий невооруженный характер. При этом ущерб от кибератаки должен быть соизмерим с вооруженным нападением, а также может выражаться в подрыве инфраструктуры целого государства, в том числе системы противоракетной обороны страны [6, с. 10-11].

Позиция «contra». Прежде всего следует отметить, что в ст. 8-бис Римского статута МУС делается отсылка к резолюции Генеральной Ассамблеи ООН 3314 от 14 декабря 1974 г. в части квалификации соответствующих актов агрессии. Однако, в отличие от самой резолюции (ст. 4), в Римском статуте МУС отсутствует положение о том, что указанный в ней перечень актов агрессии не является исчерпывающим и Совет Безопасности может определить, что другие акты представляют собой агрессию согласно положениям Устава. С позиции de jure

---

[4] Summary of the National Defense Strategy Sharpening the American Military's Competitive. 2018. URL: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (дата обращения: 10.11.2020).

[5] Военная доктрина Российской Федерации от 25.12.2014. СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_172989/ (дата обращения: 10.11.2020).

[6] China's National Defense in the New Era. The State Council Information Office of the People's Republic of China July 2019. URL: https://www.globalsecurity.org/jhtml/jframe.html#https://www.globalsecurity.org/military/library/report/2019/china-national-defense-new-era_20190724.pdf|||China%EF%BF%BDs%20National%20Defense%20in%20the%20New%20Era (дата обращения: 10.11.2020).

[7] Joint Doctrine Indian Armed Forces 2017. Headquarters Integrated Defense Staff Ministry of Defence. URL: https://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf (дата обращения: 18.11.2020).

[8] Tallinn manual on the international law applicable to cyber warfare. 2013. Центр стратегических оценок и прогнозов. URL: http://csef.ru/media/articles/3990/3990.pdf (дата обращения: 13.11.2020).

это означает, что нормативное положение ч. 2 ст. 8-бис Римского статута МУС не подлежит расширенному толкованию, а перечень актов агрессии не может быть дополнен новыми актами применения вооруженных сил.

Во-вторых, заслуживает внимания позиция, в соответствии с которой компьютерные сетевые атаки низкой интенсивности (например, шпионаж или атаки, которые приводят к сбоям функционирования системы связи, но без человеческих жертв и материального ущерба) могут рассматриваться только как недружественный акт[9]. Даже если исходить из презумпции, что кибератаки направлены против объектов критически важной инфраструктуры другого государства и могут в практическом плане квалифицироваться как преступление агрессии, это еще не означает prima facie акта агрессии, поскольку такие действия должны в силу своего характера, серьезности и масштабов являться грубым нарушением Устава Организации Объединенных Наций. Известный немецкий специалист в области международного уголовного права профессор Г. Верле отмечает, что далеко не любое применение силы может рассматриваться как акт агрессии. Акты фактической агрессии меньшей степени интенсивности по сравнению с диапазоном актов применения вооруженной силы в агрессивных целях, как это представлено в резолюции Генеральной Ассамблеи ООН 3314 от 14 декабря 1974 г., не являются преступлением, даже если они и нарушают ст. 2 (4) Устава ООН или вызывают реакцию в порядке самообороны в соответствии со ст. 51 этого Устава[10]. Представляется, что вероятность квалификации компьютерных сетевых атак в качестве акта агрессии будет ставиться в зависимость от решения, принятого Советом Безопасности в рамках реализации своих дискреционных полномочий по определению угрозы миру.

Интересной представляется позиция российского специалиста в области международного уголовного права С. Саяпина, который отмечает, что несмотря на серьезный характер военных опасностей, связанных с кибератаками, тем не менее, использование компьютеров не соответствует стандартным параметрам обычного вооружения. Кроме того, кибератаки проводятся не столько против территории другого государства, сколько в отношении электронных систем, которые не охватываются территориальным признаком потерпевшего государства [7, p. 273]. Данный вывод не лишен рационального зерна. Действительно, сущность агрессивной войны выражается в ее особой общественной опасности — происходит посягательство на международный мир посредством противоправного применения вооруженных сил одним государством против политической независимости, территориальной целостности и суверенитета другого государства. В контексте исторического анализа работы Нюрнбергского и Токийского трибуналов ведение агрессивной войны как раз и проявлялось в захвате чужой территории, уничтожении или подчинении политического режима захваченной страны, а также установлении внешнего контроля в отношении подчиненного государства при ограниченном сохранении национальных государственных структур. В этом ключе агрессивная война in natura отличается от смежных проявлений (например, приграничный вооруженный конфликт, террористический акт на территории другого государства, диверсия, враждебная разведка, посягательство на зарубежного дипломата), которые не могут рассматриваться в качестве акта агрессии по причине недостижимости необходимой степени общественной опасности, при том, что характер общественной опасности — угроза международному миру — остается перманентным. Вместе с тем позиция С. Саяпина представляется небезупречной, так как в современном международном уголовном праве криминализирована не только сама агрессивная война, но также ее планирование, подготовка и инициирование. Представляется, что инициирование агрессивной войны (ранее использовалась формулировка развязывание агрессивной войны), т.е. действия, направленные на непосредственное начало войны, могут выражаться в комбинированном виде: применение обычных вооружений может синхронизироваться с сопутствующими кибератаками на электронные системы обороны противника, что в целом согласуется с концепцией сетецентрической войны.

В-третьих, особый акцент с позиции «contra» следует сделать на рост опасности осложнения международных отношений при возможном редуцировании понятия «применение вооруженной силы» до уровня кибератаки. Дело в том, что если компьютерные сетевые атаки приравнивать в нетипичному (нетрадиционному) вооружению и изначально рассматривать как акт агрессии, то для потерпевшего государства открываются перспективные возможности реализации своего юридического права на самооборону в соответствии со ст. 51 Устава ООН[11]. В этом аспекте

[9] Dinstein Y. Computer Network Attacks and SelfDefense P. 105. URL: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1397&context=ils (дата обращения: 10.11.2020).

[10] Герхард В. Принципы международного уголовного права: учебник / Герхард Верле; пер. с англ. С.В. Саяпина. Одесса: Фенікс; М.: ТрансЛит, 2011. С. 661.

[11] Устав Организации Объединенных Наций от 24 октября 1945 г. Официальный сайт Организации Объединенных Наций. URL: https://www.un.org/ru/sections/un-charter/chapter-vii/index.html (дата обращения: 10.12.2020).

возникает ряд проблемных моментов относительно приемлемости ссылки на ст. 51 Устава ООН в условиях адекватной обороны. В частности, компьютерные сетевые атаки могут не обладать необходимым характером общественной опасности, но в силу политических конъюнктурных соображений и спекулятивных факторов может быть инициировано применение обычных вооруженных сил в отношении предполагаемого агрессора в целях уничтожения на его территории военной инфраструктуры и ослабления экономической системы. Другими словами, широкое истолкование акта агрессии посредством применения кибероружия повышает риски злонамеренного применения национальных вооруженных сил против другого государства. Кроме того, в силу отсутствия в международном праве необходимой правоприменительной практики в области самообороны от агрессивных действий в информационно-коммуникационном пространстве также актуализируется проблема юридико-технического доказывания факта агрессии, инициируемого и проводимого конкретным государством, так как подобные действия a priori носят транснациональный характер и, как правило, охватывают множество субъектов, вовлеченных в преступную деятельность из разных стран мира. Остается также открытым вопрос о критериях целесообразности и пропорциональности при реализации права на самооборону, поскольку при несоразмерных актах применения ответных вооруженных сил возникает вероятность того, что обороняющееся государство станет агрессором.

Проблема признания кибератаки в качестве возможного акта агрессии также осложняется в связи с неопределенностью понятия «применение силы». В этом контексте наблюдается определенная дискуссия среди американских и европейских экспертов в области международной безопасности. Например, американские эксперты стоят на позиции, в соответствии с которой физические последствия информационной операции являются достаточным основанием для трактовки правомерности применения силы. Действия в киберпространстве, которые непосредственно приводят к ранению или гибели людей или к существенным разрушениям инфраструктуры, могут рассматриваться как использование силы. Европейские эксперты, напротив, рассматривают и оценивают кибератаки в фокусе масштабов и последствий, сопоставимых с применением конвенционального оружия, т.е. в случае, если применение средств информационной борьбы ведет к ранению или гибели людей [8, с. 19]. Представляется, что европейская позиция в этом вопросе является более определенной, чем американский релевантный подход, в плане допущения различных толкований. Вместе с тем, несмотря на экспертно-аналитические подходы в оценке и квалификации применения компьютерных сетевых атак как проявления нетипичной формы агрессии, все еще остается без ответа вопрос: как квалифицировать агрессивные действия в информационном пространстве, направленные на дестабилизацию обстановки в другом государстве или подрыв военной инфраструктуры, при условии, что эти действия не привели к планируемым последствиям, однако существовала большая вероятность наступления таких последствий, если бы государство не обладало эффективной системой электронного противодействия подобным атакам? В подобной ситуации может возникнуть дуализм в правовой оценке таких действий: с одной стороны, эти атаки могут быть квалифицированы как акт агрессии, выраженный в применении силы без последствий (по аналогии с запуском ракеты против военных объектов другого государства, которая была сбита, не причинив какого-либо ущерба обороняющемуся государству), с другой стороны, в принципе ни что не мешает квалифицировать эти действия как угрозу миру, не переходящую в агрессию в силу того факта, что последствия не носят достаточно серьезного характера.

Подводя итог вышеизложенному, следует отметить, что в современных условиях кибератаки (компьютерные сетевые атаки), совершаемые против объектов критической информационной инфраструктуры другого государства и порождающие последствия, сравнимые с последствиями, возникающими в результате применения традиционных вооружений (например, уничтожение объектов военной или гражданской инфраструктуры, гибель людей, ослабление экономической системы), могут рассматриваться как акт агрессии при условии контекстуального элемента, выраженного в направленности совершаемых действий против суверенитета, территориальной целостности и политической независимости другого государства, что соответствует сложившемуся политико-правовому подходу восприятия преступления агрессии. Представляется, что исторически сложившееся определение агрессии, как оно изначально было представлено в резолюции Генеральной Ассамблеи ООН 3314 от 14 декабря 1974 г., а затем отражено в Римском статуте МУС, в современных условиях развития научно-технического прогресса не отвечает интересам международного мира и безопасности, так как появляются новые виды силовых форм деструктивного воздействия, которые могут порождать последствия, сравнимые по масштабам и серьезности с последствиями от использования обычных вооружений. Вместе с тем остаются отдельные проблемные

моменты, возникающие в связи с квалификацией кибератак в качестве преступления агрессии, требующие своего перспективного осмысления и разрешения сообразно с развитием науки международного права и правоприменительной практики в срезе динамики международных отношений.

Список литературы

1. Макаренко С.И., Иванов М.С. Сетецентрическая война — принципы, технологии, примеры и перспективы. Монография. СПб.: Наукоемкие технологии, 2018. 898 с.
2. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. СПб.: Наукоемкие технологии, 2017. 546 с.
3. Печегин Д.А. Становление международной уголовной юстиции: история вопроса // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2014. № 12 (140). С. 149-153.
4. Dinstein Y. War, Aggression and Self-Defence. Fifth Edition. Cambridge University Press. 2001. 292 p.
5. Lilienthal G., Nehaluddin A. Cyber-attack as Inevitable Kinetic War // Computer Law & Security Review. 2015. Vol. 31. Iss. 3. P. 390-400.
6. Brownlie L. International Law and the Use of Force by States. UK: Clarendon. 1963. 532 p.
7. Тимошков С.Г. Агрессия как международное преступление: 12.00.10: автореф. … дис. к.ю.н. Москва, 2017. 27 с.
8. Sayapin S. The Crime of Aggression in International Criminal Law. Historical Development, Comparative Analysis and Present State. Springer, 2014. 334 p.
9. Гриняев С. «Таллиннское руководство по применению юридических норм международного права к военным действиям в киберпространстве» в оценках западных экспертов // Обзор. НЦПТИ. 2013. № 3. С. 18–22.

Computer Network Attacks as an Act of Aggression in the Context of the Development of Modern International Relations: Pros and Cons[1]

Lobach Dmitry,
PhD in Law, Associate Professor of the Department of Theory and History of Russian and Foreign Law, Vladivostok State University of Economics and Service, Institute of Law
E-mail: dimaved85@mail.ru

Smirnova Evgeniya,
PhD in Law, Senior Lecturer at the Department of Labor and Environmental Law, Far Eastern Federal University, Law School
E-mail: smirnova.ea@dvfu.ru

Abstract. *The article analyzes the conflicting approaches to the possible recognition of computer network attacks as an act of aggression in the focus of modern international relations and trends in scientific and technological progress. The question raised in the article is as follows: is aggression against another state possible through the exclusive use of cyber weapons? To solve the indicated problem, the scholastic method of conducting a discussion is used, in which two series of contradictory arguments regarding the subject of discussion are put forth, and the conclusion summarizes the general conclusion based on particular theses. The conclusion is argued that the historically established definition of aggression in modern conditions of development of scientific and technological progress does not meet the interests of international peace and security, since new types of force of destructive influence constantly appear, which can generate consequences comparable in scale and severity to the consequences of using conventional weapons. However, there are still some problematic moments that arise in connection with the qualification of cyberattacks as a crime of aggression, requiring understanding and resolution in accordance with the development of the science of international law and law enforcement practice in the context of international relations.*

Keywords: *Crime of aggression, cyber-attack, computer network attack, international criminal law, international peace, security, cyber weapons.*

[1] This work was financially supported by the Russian Federation Presidential Grant 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."

References

1. Makarenko S.I., Ivanov M.S. Setetsentricheskaya voyna — printsipy, tekhnologii, primery i perspektivy. Monografiya. Saint Petersburg: Science-intensive technologies, 2018. 898 p. (In Russ.).
2. Makarenko S.I. Informatsionnoye protivoborstvo i radioelektronnaya bor'ba v setetsentricheskikh voynakh nachala XXI veka. Monografiya. Saint Petersburg: Science-intensive technologies, 2017. 546 p. (In Russ.).
3. Pechegin D.A. International Criminal Justice and its Establishment: Historical View // Tambov University Review. Series Humanities. 2014. № 12 (140). P. 149-153.
4. Dinstein Y. War, Aggression and Self-Defence. Fifth Edition. Cambridge University Press. 2001. 292 p.
5. Lilienthal G., Nehaluddin A. Cyber-attack as Inevitable Kinetic War. *Computer Law & Security Review.* 2015;31(3):390-400.
6. Brownlie L. International Law and the Use of Force by States. UK: Clarendon. 1963. 532 p.
7. Timoshkov S.G. Agressiya kak mezhdunarodnoye prestupleniye: avtoref. … diss. k.yu.n. Moscow, 2017. 27 p. (In Russ.).
8. Sayapin S. The Crime of Aggression in International Criminal Law. Historical Development, Comparative Analysis and Present State. Springer, 2014. 334 p.
9. Grinyaev S. «Tallinnskoye rukovodstvo po primeneniyu yuridicheskikh norm mezhdunarodnogo prava k voyennym deystviyam v kiberprostranstve» v otsenkakh zapadnykh ekspertov. *Zhurnal OBZOR. NCPTI.* 2013;(3):18-22. (In Russ.).