

ПРИМЕНЕНИЕ ПРИНЦИПА ДОЛЖНОЙ ОСМОТРИТЕЛЬНОСТИ В ОТНОШЕНИИ АКТОВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, В ПЕРИОД МЕЖДУНАРОДНОГО ВООРУЖЕННОГО КОНФЛИКТА

Н.О. Мороз

*Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь*

В ходе современных вооруженных конфликтов активно используются различного рода информационно-коммуникационные технологии. Настоящая статья посвящена выявлению применимости принципа должной осмотрительности к актам, совершаемым с использованием информационно-коммуникационных технологий, в ходе вооруженного конфликта в отношениях между воюющими сторонами, а также в их отношениях с третьими государствами.

Ключевые слова: информационная безопасность, международное гуманитарное право, принцип должной осмотрительности, правила ответственного поведения государств в киберпространстве.

APPLICATION OF THE PRINCIPLE OF DUE DILIGENCE WITH RESPECT TO ACTS PERFORMED WITH THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES DURING INTERNATIONAL ARMED CONFLICT

N.A. Maroz

*Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus*

In the course of modern armed conflicts, various kinds of information and communication technologies are actively used. This article is devoted to identifying the applicability of the principle of due diligence to acts committed with the use of information and communication technologies during international armed conflict in relations between belligerents, as well as in their relations with third states.

Keywords: information security, international humanitarian law, due diligence principle, rules for the responsible behavior of states in cyberspace.

Принцип должной осмотрительности широко признан в современном международном праве. При этом возможность применения данного принципа к деятельности, связанной с использованием информационно-

коммуникационных технологий (далее – ИКТ), само по себе не оспаривается ни в доктрине, ни в практике. В то же время степень обязательности, а также содержание принципа должной осмотрительности в таком контексте остается предметом научных дискуссий.

В ходе современных вооруженных конфликтов активно используются различного рода ИКТ: начиная с автономных видов вооружения и заканчивая программными средствами для получения доступа, модификации, перехвата компьютерных данных, саботажа работы компьютерных систем и сетей противника. В такой ситуации закономерно возникает вопрос сохраняет ли свое действие обязательство государства заведомо не позволять использование своей территории для совершения частными лицами и третьими государства актов с использованием ИКТ, противоречащих правам других государств, в ходе вооруженного конфликта в отношениях между воюющими сторонами, а также в их отношениях с третьими государствами.

Несмотря на то, что применение принципа должной осмотрительности к деятельности, связанной с использованием ИКТ, исследовалось в научных публикациях, возможности сохранения его действия в период вооруженного конфликта практически не анализировались. Существующие научные публикации рассматривают содержание такого обязательства узко, исключительно исходя из обязательств должной осмотрительности, вытекающих из Женевских конвенций 1949 г. и Дополнительных протоколов к ним [1]. Указанное обстоятельство обуславливает новизну настоящего исследования.

В настоящей статье предпринята попытка выявить условия применимости должной осмотрительности к деятельности, связанной с использованием ИКТ, в период вооруженного конфликта.

Принцип должной осмотрительности является одним из принципов общего международного права. Международный Суд ООН в деле о проливе Корфу заявил, что «каждое государство обязано заведомо не позволять использовать свою территорию для совершения действий, противоречащих правам других государств» [2]. Формулировка «каждое государство» подчеркивает тот факт, что данное обязательство: во-первых, затрагивает любое государство (например, вне зависимости от факта его признания), во-вторых, неотъемлемо ему принадлежит (государство не может от него отказаться или быть лишено его).

Принцип распространяется на действия негосударственных субъектов и поведение третьих государств [3, с. 32].

Принцип должной осмотрительности применительно к правоотношениям, возникающим по поводу использования ИКТ, был сформулирован в отчете ГПЭ за 2015 г. В документе указано, что государства не должны заведомо позволять использовать свою территорию для совершения

международно-противоправных деяний с использованием ИКТ [4]. В то же время в доктрине считается, что этот принцип в его применении к киберпространству не получил статуса *lex lata* [3, с. 31]. В практике государств также нет единства относительно юридической силы принципа, в формулировке предложенной ГПЭ [5]. В то же время в доктрине и практике признается, что норма 13с) отчета ГПЭ за 2015 г. закрепляет хотя и, как минимум добровольный, но ожидаемый для исполнения стандарт ответственного поведения государств в связи с использованием ИКТ (пп. а п. 30 Доклада).

Комментарий к принципу должной осмотрительности, содержащийся в отчете ГПЭ 2015 г., предложенный ГПЭ в ее новом отчете, представленном в 2021 г., значительно конкретизирует содержание обязательства. Так, во-первых, возникновение обязательства не позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ связывается, прежде всего, с осведомленностью государства или его добросовестным уведомлением об инциденте [6]. Во-вторых, инцидент сам по себе должен представлять международно-противоправное деяние, совершенное с использованием ИКТ на территории уведомляемого государства или проходящим через его территорию. В-третьих, обязательство «не допускать использования своей территории» означает «использовать все соответствующие, доступные и возможные – в разумных пределах – шаги для обнаружения, расследования и урегулирования такой ситуации». В-четвертых, субъектами таких инцидентов могут быть как третьи государства, так и негосударственные субъекты.

Формулировка обязательства, содержащаяся в норме 13с) не вполне удачна, поскольку деяния негосударственных акторов, которые не могут быть атрибуированы государству, не могут квалифицироваться в качестве международно-противоправных деяний. В то же время согласно п. 29 Доклада 2021 г., указывается, что в рассматриваемой норме «заложено понимание того, что государство не должно позволять другому государству или негосударственному субъекту использовать ИКТ на своей территории для совершения международно-противоправных деяний».

Таким образом, норма 13с) нуждается в корректировке. Для устранения данной неточности в доктрине предлагалось использование формулировки, содержащейся в решении Международного Суда ООН по делу о проливе Корфу [6]. Полагаем, что использование фразы «противоречащих правам других государств» для уточнения содержания нормы 13с) поскольку сужает международно-правовое обязательство до: а) только одной формы имплементации международно-правового обязательства («соблюдения»); б) соблюдения исключительно прав, вытекающих из международно-правовых обязательств; в) соблюдения прав только государств. В этой связи

предлагается изложить формулировку обязательства должной осмотрительности, содержащуюся в норме 13с) в следующей редакции:

«Государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ и деяний, которые могли бы рассматриваться в качестве международно-противоправных, если бы были совершены государством».

Таллиннское руководство 2.0 содержит толкование принципа должной осмотрительности, которое отличается от предложенного в отчетах ГПЭ 2015 г., 2021 г., и фактически сужает сферу его действия, охватывая лишь необходимость предупреждения актов, которые затрагивают «права других государств и приводят к серьезным негативным последствиям для них». В Таллинском руководстве 2.0 содержится более подробное толкование территориальной сферы действия принципа. В частности, в нем указывается, что «государство должно проявлять должную осмотрительность, не позволяя использовать свою территорию, территорию или кибернетическую инфраструктуру, находящуюся под его контролем, для киберопераций <...> [3, с. 30].

Следует отметить, что в доктрине не единства относительно необходимости включения элемента «серьезных негативных последствий» как условия возникновения обязательства проявлять должную осмотрительность в киберконтексте. Так, Ф. Делеруа отмечает, что указанный элемент был разработан применительно к международному экологическому праву, в то же время в киберконтексте он не является обязательным компонентом принципа должной осмотрительности [7, с. 364]. Так, обязательство должной осмотрительности одинаково применимо к любым деяниям, которые могли бы рассматриваться в качестве международно-противоправных. В то же время наличие такого ущерба будет влиять на фактическую заинтересованность государства призвать к ответственности другое государство, которое не пресекает кибероперации, которые порождают такой ущерб [4, с. 365].

В настоящем исследовании будет использована трактовка принципа должной осмотрительности, предложенная ГПЭ, поскольку она в определенном смысле отражает позиции государств.

Принцип должной осмотрительности не влечет за собой каких-либо обязательств территориального государства по уголовному преследованию лиц, совершивших какие-либо кибератаки в нарушение прав других государств [3, с. 32, 48]. Фактически, наличие таких обязательств зависит от наличия применимых международных договоров к конкретной ситуации, криминализация конкретного деяния согласно уголовному законодательству территориального государства, осуществляется ли в отношении данного противоправного деяния уголовное преследование и обвинение в суде в публичном порядке и др.

Как было указано выше, принцип должной осмотрительности применительно к правоотношениям, возникающим по поводу использования ИКТ, не получил закрепления в международном договоре универсального характера. Указанное обстоятельство является одной из важнейших причин наличия доктринальных споров и различий в позициях государств о его юридической обязательности.

В то же время на региональном уровне можно проследить урегулирование его отдельных аспектов. Так, принцип должной осмотрительности отчасти нашел отражение в абз. 6-7 ст. 6 Соглашения о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности 2017 г., где указывается, что государства-участники осуществляют самостоятельно или при соответствующем обращении меры для предотвращения использования третьей стороной территории и (или) информационной инфраструктуры, находящейся под юрисдикцией государства – члена ОДКБ, для оказания деструктивного информационного воздействия, в том числе компьютерных атак, на другое государство – член ОДКБ; взаимодействуют в интересах определения источника компьютерных атак, проведенных с использованием их территории, противодействия этим атакам и ликвидации последствий.

Учитывая тот факт, что само по себе обязательство должной осмотрительности вытекает из суверенитета государства, принципа суверенного равенства государств, а «суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ» [4], полагаем, что на исполнимость данного обязательства сам факт вооруженного конфликта не оказывает влияния. В то же время более широкий контекст ситуации безусловно может оказывать влияние на практическую возможность реализации данного принципа.

Комиссией международного права ООН в Проекте статей о последствиях вооруженных конфликтов для международных договоров, было отмечено, что при определении влияния конфликта на международный договор должны приниматься во внимание: а) характер договора, в частности его предмет, его объект и цель, его содержание и количество участников договора; и (b) характеристики вооруженного конфликта, такие как его территориальная протяженность, его масштабы и интенсивность, его продолжительность и, в случае немеждународных вооруженных конфликтов, а также степень участия извне.

Как было указано выше, в доктрине возможность применения принципа должной осмотрительности к деяниям, совершаемым с использованием ИКТ, выводится из обязательства должной осмотрительности в контексте обязательств, напрямую вытекающих из норм международного

гуманитарного права (далее – МГП) (ст. 1, общая для всех Женевских конвенций о защите жертв войны 1949 г., п.1 ст. 1 I Дополнительного протокола к Женевским конвенциям 1949 г.) [1]

Не оспаривая наличие обязательства государств предпринимать позитивные меры для обеспечения соблюдения МГП другими образованиями (в частности, частными лицами), тем самым предотвращая совершение нарушений, а также его применимости к кибероперациям, следует отметить, что сужение сферы действия принципа должной осмотрительности в данном контексте не вполне корректно, что обусловлено следующим.

Во-первых, должная осмотрительность в контексте международного гуманитарного права и принцип должной осмотрительности как общий принцип международного права соотносятся как частное и общее. Так, последнее, как уже отмечалось выше, охватывает общее обязательство не позволять использовать свою территорию для совершения действий, противоречащих *любым* международно-правовым обязательствам, а не только тех, которые вытекают из международного гуманитарного права.

Во-вторых, международно-правовые обязательства государств не прекращают (приостанавливают) своего действия автоматически в связи с вооруженным конфликтом. Как указывал Э. Давид «если развязывание войны влечет за собой применение определенных норм, это не означает приостановления действия любой другой правовой нормы» [7, с. 76]. Комиссией международного права ООН также отмечалось, что вооруженный конфликт не прекращает действия международного договора *ipso facto*. Полагаем, что данный вывод вполне справедлив и по отношению к обычным нормам международного права. Таким образом, ни действие самого принципа должной осмотрительности, ни права государств, фактически нарушаемые в ходе неправомерной деятельности негосударственных акторов или третьих государств с использованием ИКТ, не прекращаются *ipso facto* в период вооруженного конфликта.

В то же время в соответствии с Венской конвенцией о праве международных договоров 1969 г. предусмотрены ситуации, когда государство может приостановить или прекратить международный договор, многие из которых могут быть связаны или стать следствием вооруженного конфликта. К данным ситуациям относятся: существенное нарушение двустороннего договора одним из его участников (ст. 60); невозможность выполнения договора вследствие безвозвратного исчезновения или уничтожения объекта, необходимого для выполнения договора (ст. 61); коренное изменение обстоятельств (ст. 62).

На все указанные ситуации недопустимо ссылаться государству, которое является нарушителем международного договора, применение которого приостанавливается или прекращается. Так, например, если уничтожение

объекта, необходимого для выполнения договора возникло по причине вооруженного конфликта, развязанного определенным государством, последнее не вправе ссылаться на последующую невозможность выполнения договора (п.2 ст. 61 Венской конвенции о праве международных договоров 1969 г.). В то же время в соответствии с п. 5 ст. 60 существенное нарушение международного договора одной стороной тем не менее не является основанием для приостановления или прекращения положений, касающихся «защиты человеческой личности, которые содержатся в договорах, носящих гуманитарный характер, и особенно к положениям, исключаящим любую форму репрессалий по отношению к лицам, пользующимся защитой по таким договорам». Таким образом, пострадавшее государство в любом случае остается связанным международно-правовыми обязательствами, которые носят гуманитарный характер и не вправе апеллировать к приостановлению или прекращению их действия даже по причине вооруженного конфликта.

Комиссией международного права ООН также обращалось внимание: а) на недопустимость извлечения выгоды государством-агрессором, связанной с прекращением или приостановлением международного договора по причине вооруженного конфликта (ст. 15 Проекта статей о последствиях вооруженных конфликтов для международных договоров 2011 г.); б) сохраняющуюся обязанность государства, совершившего международно-противоправное деяние, по исполнению нарушенного обязательства (ст. 29 Статей об ответственности государств за международно-противоправные деяния 2001 г.); в) на обязанность всех государств не признавать правомерным положение, сложившееся в результате серьезного нарушения императивной нормы общего международного права, к которому в частности относится и нарушение запрета применения силы по международному праву (п. 2 ст. 41 Статей об ответственности государств за международно-противоправные деяния 2001 г.).

Таким образом, государство, нарушившее запрет применения силы, не только не может приобретать преимущества в связи с прекращением или приостановлением международно-правовых обязательств по причине этого вооруженного конфликта, а также сохраняет обязанность выполнять свои международно-правовые обязательства первичного характера.

В свою очередь пострадавшее государство обязано соблюдать положения норм международного права, сохраняющих свое действие в ходе вооруженного конфликта.

Так, кроме обязательств, вытекающих из норм международного гуманитарного права, государства – стороны вооруженного конфликта обязаны соблюдать и применять Венскую конвенцию о дипломатических сношениях 1961 г., Венскую конвенцию о консульских сношениях 1963 г. (п. 3 резолюции Совета Безопасности ООН 667 от 16 сентября 1990 г.), основные нормы

права прав человека и права окружающей среды (п. 29-31 Консультативного заключения Международного Суда ООН о законности угрозы ядерным оружием или его применения).

В Проекте статей о последствиях вооруженных конфликтов для международных договоров 2011 г. Комиссия международного права ООН представила примерный перечень международных договоров, которые не прекращают свое действие в период вооруженного конфликта. Соответственно, если частные лица будут нарушать положения таких международных договоров в период вооруженного конфликта, воюющие стороны, тем не менее, должны оставаться связаны обязательством прекратить такую деятельность, даже если она направлена против воюющей стороны.

Так, государства кроме использования своего неотъемлемого права на самооборону также могут принимать контрмеры в ответ на нарушение международно-правовых обязательств. При этом как право на самооборону, так и на принятие контрмер не являются неограниченными. Так, в частности, контрмеры должны соответствовать требованиям, установленным в Статьях об ответственности государств за международно-противоправные деяния.

С учетом положений о принятии контрмер, закрепленных в Статьях об ответственности государств за международно-противоправные деяния, пострадавшее государство может отступить от выполнения некоторых своих обязательств. Принятие контрмер предполагает принятие активных мер, то есть действий, а не бездействия (п. 1 ст. 42 Статей об ответственности государств за международно-противоправные деяния). В настоящее время возможность принятия контрмер путем бездействия не нашла четкой поддержки в доктрине [9], в то же время указанные аспекты были предметом научных дискуссий [10, с. 20].

Таким образом, отсутствие реагирования на деяния частных лиц или третьих государств, осуществляемых с использованием ИКТ, против прав других государств не может выступать в качестве контрмер, поскольку представляет собой бездействие. Деяния частных лиц или третьих государств, совершаемые с использованием ИКТ, против прав государства – нарушителя, могут рассматриваться как деяния самого пострадавшего государства, если оно признает и принимает данное поведение в качестве собственного (ст. 11 Статей об ответственности государств за международно-противоправные деяния).

Кибератаки на гражданские объекты, объекты, содержащие опасные силы, объекты, необходимые для выживания населения; медицинские формирования и санитарно-транспортные средства; культурные ценности и места отправления культа будут охватываться принципом должной осмотрительности. При этом роль государства в вооруженном конфликте не будет иметь значения для целей применимости такого обязательства.

В то же время и ряд других атак, которые могут быть квалифицированы как нарушение международно-правовых обязательств, будут по-прежнему запрещены в период вооруженного конфликта, такие, как например, акты, посягающие на свободу морского судоходства, направленные против безопасности гражданской авиации, нарушающие тайну дипломатической переписки и др.

Как уже было указано выше, более широкий контекст ситуации вооруженного конфликта может оказывать влияние на практическую выполнимость принципа должной осмотрительности. Так, в результате вооруженного конфликта государство может не контролировать часть своей территории. В такой ситуации оккупирующее государство будет нести ответственность за осуществление принципа должной осмотрительности с этой территории (ст. 9 Статей об ответственности государств за международно-противоправные деяния, ст. 42-43 Конвенции о законах и обычаях сухопутной войны 1907 г., ст. 64 Конвенции о защите гражданского населения во время войны 1949 г.).

Таким образом, фактически, обязательство должной осмотрительности будет всегда сохранять свое действие, если совершаемое деяние может рассматриваться как нарушение:

а) международного договора, содержащегося в приложении к Проекту статей о влиянии вооруженных конфликтов на действие международного договора;

б) императивных норм общего международного права.

Содержание обязательства осуществления должной осмотрительности требует от государства принятия всех адекватных и разумно доступных мер, а также осуществимых шагов для обнаружения, расследования и урегулирования ситуации. Стандарт требуемого от государства поведения при этом не установился в практике государств [5]. При этом возможности по принятию мер у развитых и развивающихся государств в части недопущения использования их территории для совершения актов, противоречащих правам других государств, будут различными. Более того, возможности государств в этой сфере могут еще более серьезно ограничены в связи с вооруженным конфликтом (так, может быть повреждена соответствующая техническая инфраструктура, могут отсутствовать специалисты, способные пресечь совершение противоправного деяния, может отсутствовать телефонная связь, электричество и Интернет и др.). В то же время принцип должной осмотрительности порождает обязательство действия, не результата [7, с. 361]. Таким образом, недостижение цели предупреждения кибератаки в таких условиях не может рассматриваться в качестве нарушения обязательства должной осмотрительности.

При этом государства могут, но не обязаны обращаться к помощи третьих государств или частных лиц для оказания технической поддержки с целью выполнения обязательства должной осмотрительности (пп. b п. 30 Доклада ГПЭ по продвижению ответственного поведения государств в киберпространстве в контексте международной безопасности 2021 г.). Полагаем, что указанное правило будет применимо и в контексте вооруженного конфликта. При этом любые принудительные действия в отношении частных лиц, осуществляющих злонамеренную деятельность с использованием ИКТ против прав других государств, будут правомерными только с согласия государства, на территории которого они находятся, или с санкции Совета Безопасности ООН. Так, неспособность Сомали пресекать акты морского пиратства, совершаемые ее гражданами, привело к принятию целого ряда резолюций Советом Безопасности ООН, которые, в частности, предусматривали возможность для государств, которые сотрудничают с переходным федеральным правительством Сомали в борьбе с пиратством и вооруженным разбоем на море у побережья Сомали и в отношении которых переходное федеральное правительство Сомали заблаговременно направило уведомление Генеральному секретарю, входить в территориальные воды Сомали в целях пресечения актов пиратства и вооруженного разбоя на море сообразно тому, как это разрешается делать в открытом море в отношении (п. 7 резолюции Совета Безопасности ООН 1816 от 2 июня 2008 г.).

Как уже было указано выше, государство, нарушившее запрет применения силы, не может ссылаться на целый ряд обстоятельств, ставших результатом применения силы, в качестве оправдания для неисполнения международно-правового обязательства (пп. с п. 2 ст. 60, п. 2 ст. 61, пп. b п. 2 ст. 62 Венской конвенции о праве международных договоров 1969 г.; ст. 15 Проекта статей о последствиях вооруженных конфликтов для международных договоров 2011 г.).

В ходе вооруженного конфликта деятельность, совершаемая частными лицами, в ряде случаев может рассматриваться как деяние государства. Так, если частные лица, осуществляющие кибератаки на военную инфраструктуру государства – противника соответствуют признакам комбатанта, установленным в Женевской конвенции и I Дополнительным протоколом, то их деятельность в ряде случаев может рассматриваться как деяние государства. В то же время, например, население неоккупированной территории, которое при приближении неприятеля стихийно берется за оружие для борьбы со вторгающимися войсками, не успев сформироваться в регулярные войска, если оно носит открыто оружие и соблюдает законы и обычаи войны хотя и охватывается понятием «комбатанты» (п. 6 ст. 13 Конвенции об улучшении участи раненых и больных в действующих армиях от 12 августа 1949 г.), фактически не находится под контролем пострадавшего государства.

Такие лица не действуют по указаниям либо под руководством или контролем этого государства, и потому их поведение не может быть атрибутировано государству (ст. 8 Статей об ответственности государств за международно-противоправные деяния), безусловно, если последнее не признает его в качестве собственного поведения (ст. 11 Статей об ответственности государств за международно-противоправные деяния).

Деятельность третьих государств, которая наносит ущерб правам иностранных государств, также может по-разному квалифицироваться в период вооруженного конфликта. Так, если такое третье государство фактически контролирует территорию иностранного государства, с которой осуществляются кибератаки против критически важных объектов инфраструктуры других государств, именно такое третье государство будет обязано придерживаться принципа должной осмотрительности (ст. 9 Статей об ответственности государств за международно-противоправные деяния). В том случае, если государство запросила соответствующую техническую помощь третьего государства и фактически если предоставленные в его распоряжения хакеры действуют для реализации военных целей первого государства, тогда их кибератаки будут считаться актами первого государства (ст. 6 Статей об ответственности государств за международно-противоправные деяния).

Таким образом, на основе проведенного исследования представляется возможным сформулировать следующие выводы:

1. Принцип должной осмотрительности в контексте использования ИКТ имеет обычно-правовую природу и вытекает из общего обязательства каждого государства заведомо не позволять использовать свою территорию для совершения действий, противоречащих правам других государств. Ни сам принцип, ни его действие в отношении определенных международно-правовых обязательств не прекращается в связи с возникновением вооруженного конфликта между государствами *ipso facto*.

2. Формулировка обязательства, содержащаяся в норме 13с) не вполне удачна. В этой связи предлагается изложить формулировку обязательства должной осмотрительности, содержащуюся в норме 13с) в следующей редакции: «государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ и деяний, которые могли бы рассматриваться в качестве международно-противоправных, если бы были совершены государством».

3. Обязательство должной осмотрительности будет всегда сохранять свое действие в отношениях между воюющими сторонами, если деяние частных лиц или третьих государств может рассматриваться как нарушение: а) международного договора, содержащегося в приложении к Проекту

статей о влиянии вооруженных конфликтов на действие международного договора; б) императивных норм общего международного права.

Библиографический список

1. Dias, T. Cyber due diligence in international law [Electronic resource] / T. Dias, A. Coco // The Oxford Institute for Ethics Law and Armed Conflict. – Mode of access: <https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.pdf>. – Date of access: 04.06.2022.
2. Corfu Channel case, Judgment of April 9, 1949 : I.C. J. Reports 1949, P. 4. P. 22
3. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 2nd Edition / ed. by Michael N. Schmitt. – Oxford: Oxford University Press, 2017. – 598 p.
4. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015 [Electronic resource] / United Nations. – Mode of access: <https://undocs.org/A/70/174>. – Date of access: 12.10.2021.
5. Kastelic, A. Due diligence in cyberspace Normative expectations of reciprocal protection of international legal rights / A. Kastelic [Electronic resource] / UNIDIR. – Mode of access: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjxypSd2Z_7AhULiYsKHSbKBT0QFnoECAoQAQ&url=https%3A%2F%2Fwww.unidir.org%2Fpublication%2Fdue-diligence-cyberspace-normative-expectations-reciprocal-protection-international&usg=AOvVaw0hPN1vWTgMMq46z3wJnyAG. – Date of access: 25.05.2022.
6. Report of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (Advance copy), 2021, May [Electronic resource] / United Nations. – Mode of access: <https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf>. – Date of access: 12.10.2021.
7. Delerue, F. Cyber Operations and International Law / F. Delerue. – Cambridge: Cambridge University Press, 2020. – 513 p.
8. Давид, Э. Принципы права вооруженных конфликтов / Э. Давид. – Москва: МККК, 2011. – 1141 с.
9. Summary record of the 2590th meeting of the International Law Commission, A/CN.4/SR.2590. Extract from the Yearbook of the International Law Commission, – 1999. – Vol. I, § 42-43 [Electronic resource] / United Nations. – Mode of access: https://legal.un.org/ilc/documentation/english/summary_records/a_cn4_sr2590.pdf. – Date of access: 12.10.2021.
10. Murphy, S.D. International Law. Cases and materials / S.D. Murphy, L.F. Damrosch. – Sixth ed., West Academic Publishing, Saint Paul. – 1532 p.