Международное право
Правильная ссылка на статью:
Горелик И.Б. — Возможные направления развития международно-правовых институтов в области обеспечения глобальной кибербезопасности // Международное право. – 2023. – № 2. DOI: 10.25136/2644-5514.2023.2.40618 EDN: UZESRS URL: https://nbpublish.com/library_read_article.php?id=40618

Возможные направления развития международно-правовых институтов в области обеспечения глобальной кибербезопасности

Горелик Илья Борисович

аспирант, кафедра международного права, Дипломатическая Академия Министерства Иностранных Дел России

119021, Россия, г. Москва, ул. Остоженка, 53/2, стр. 1

gorelik.ilya@yandex.ru

Статья из рубрики "Развитие отдельных отраслей международного публичного права"

DOI:

10.25136/2644-5514.2023.2.40618

EDN:

UZESRS

Дата направления статьи в редакцию:

25-04-2023

Дата публикации:

02-05-2023

Аннотация: В статье рассматриваются возможные направления формирования глобальной международно-правовой системы противодействия киберпреступности и ее дальнейшего развития. Коротко анализируются результаты деятельности международных организаций в области развития международно-правовых механизмов противодействия киберпреступности. Осуществляется попытка поиска иных международно-правовых проблем, опыт решения которых может выступать в качестве концептуального базиса для формирования глобальной международно-правовой системы обеспечения кибербезопасности. Исследуются основные характеристики современных цифровых информационной-коммуникационных систем - в особенности интернет-технологий. Приводится попытка создания теоретической модели международно-правового регулирования противодействия современным цифровым угрозам исходя из глобального характера современных киберугроз. Констатируется особая роль международных организаций в области развития международного права. Приводится мнение о сложившейся глобальной цифровой информационной системе, охватывающей все

международное сообщество. Проводится параллель между концептуальными основами проблемы отмывания денег и финансирования терроризма (ОД/ФТ) и киберпреступностью. Констатируется концептуальное сходство двух указанных проблем с обоснованием такого заключения. В связи с этим предлагается использовать организационную структуру международно-правового обеспечения противодействия ОД/ФТ как концептуальную основу для аналогичного противодействия киберпреступности. В частности, в статье предлагается в рамках ООН создать специализированную международную организацию, деятельность которой будет посвящена обеспечению глобальной кибербезопасности. В качестве основы деятельности предлагается применять организационные основы аналогичные тем, которые применяются в рамках Межправительственной комиссии по финансовому мониторингу. В частности, деятельность организации предлагается осуществлять на базе перечня рекомендаций по совершенствованию национальных организационно-правовых мер противодействия угрозам в сфере цифровых технологий, а также механизмов взаимной оценки государств-членов.

Ключевые слова:

международное право, кибербезопасность, киберпреступность, международные организации, ООН, ФАТФ, противодействие отмыванию денег, рекомендации, информационные технологии, конвенция

В современных условиях стремительного развития и распространения информационно-коммуникационных технологий особенно острой становится проблема организации международно-правового регулирования противодействия преступному использованию цифровых технологий. Проблема киберпреступности была осознана достаточно давно и неоднократно отражалась в международной законотворческой деятельности.

Анализ современной деятельности по развитию международного права в сфере противодействия киберпреступности позволяет прийти к выводу о том, что одной из ее основ являются инициативы множества международных организаций. Ярким примером данного явления можно назвать деятельность Совета Европы, разработавшего Конвенцию о компьютерных преступления 2001 г. (Будапештская конвенция) [3]. В течение следующих двух десятилетий Советом также были разработаны два дополнительных протокола к Конвенции – Первый Дополнительный протокол по криминализации расистских и ксенофобских актов, совершаемых с использованием компьютерных систем [11], и Второй Дополнительный протокол по усилению сотрудничества и раскрытию электронных доказательств [15].

В рамках другой региональной международной организации – Европейского Союза – также осуществлялась активная выработка международно-правовых соглашений в области защиты персональных данных [10, С. 97]. В частности, была создана система международно-правовых норм, среди которых можно выделить Общий Регламент Европейского Парламента и Совета Европы № 2016/679 по защите персональных данных физических лиц 2016 г. [13], Регламент Европейского Парламента и Совета Европы № 1725/2018 от 23 октября 2018 г. о защите физических лиц при обработке персональных данных институтами, органами, ведомствами и агентствами и о свободном обращении таких данных [14], а также Директива Европейского Парламента и Европейского Совета № 680/2016 от 27 апреля 2016 г. о защите физических лиц при обработке персональных

данных компетентными органами в целях предотвращения, расследования, обнаружения или судебного преследования уголовных правонарушений или при исполнении уголовных наказаний [12].

Работа по созданию международно-правовых актов в сфере кибербезопасности велась и в рамках СНГ. В частности, в 2001 г. было создано Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации [8], позже прекратившее свое действие в связи с принятием нового документа в аналогичной области – Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г. [9]

Аналогичная работа велась и в рамках других региональных международных организаций – таких как ШОС, АСЕАН, Африканский Союз, Лига Арабских Государств и т.д. [2, С. 33]

В рамках ООН работа по выработке правовых основ противодействия киберпреступности осуществлялась на основе деятельности специализированной организации – Международного союза электросвязи, разработавшего Глобальную программу кибербезопасности 2008 г. [1] и Руководство по пониманию киберпреступности для развивающихся стран 2009 г. [6]. Более того, по инициативе России в ООН были созданы две специализированные группы – Рабочая группа открытого состава (РГОС) и Группа правительственных экспертов (ГПЭ). Основные результаты деятельности указанных групп оформлялись в виде резолюций Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

Таким образом, деятельность международных организаций в сфере развития международно-правовых механизмов обеспечения кибербезопасности представляется основой для развития международного права в данной области. Однако, не смотря на значительный вклад указанных ранее организаций, на данный момент можно выделить одну серьезную проблему – отсутствие глобальной правовой основы для международно-правового противодействия киберпреступности.

По мнению автора, в контексте кибербезопасности особенно важно формирование именно глобальной международно-правовой системы обеспечения информационной безопасности и, в частности, борьбы с киберпреступностью. Такое мнение обосновывается специфическими характеристиками киберпреступности, связанными с механиками функционирования современных цифровых технологий. Как известно, современные информационно-коммуникационные технологии (ИКТ) обладают возможностью быстрого распространения данных на большие расстояния. При условии практически повсеместного распространения ИКТ – в частности, распространения интернет-технологий – это приводит к тому, что международное сообщество, фактически, становится одной глобальной информационной системой. По причине неравномерного технологического развития некоторых государств и регионов эта система очень разветвлена и неоднородна, однако все же она существует на глобальном уровне и охватывает все регионы мира. Такое обстоятельство приводит к тому, что обмен данными в рамках ИКТ-сетей может осуществляться повсеместно и вне зависимости от конкретной юрисдикционной принадлежности.

Указанная особенность представляет собой значительную проблему по той причине, что каждый акт преступного использования ИКТ может одновременно затрагивать сразу

несколько юрисдикций, причем даже не находящихся в рамках одного региона. Однако учитывая различия в подходах к правовому противодействию киберпреступности и организации расследований, совместная деятельность заинтересованных государств значительно затрудняется по причине отсутствия единоначалия. Более того, если рассматривать современное международное сообщество как глобальную информационную систему, необходимо также учесть один из основных принципов теории информационной безопасности, согласно которому уровень защиты некоторой информационной системы равен уровню защиты самого незащищенного элемента такой системы [4, С. 238]. При рассмотрении международного сообщества в таком ключе роль элементов глобальной информационной системы играют отдельные государства и находящиеся в их юрисдикции комплексы ИКТ. А это означает, что даже при условии существования некоторых регионов, в рамках которых эффективно реализованы правовые меры обеспечения информационной безопасности, реальный уровень их защищенности, в конечном итоге, будет оставаться низким по причине отсутствия или неэффективной реализации аналогичных правовых мер в других регионах. Таким образом, проблема обеспечения международной кибербезопасности (по крайне мере, в контексте международного права) будет оставаться нерешенной до тех пор, пока существуют государства и регионы, в которых не реализованы эффективные правовые механизмы противодействия киберпреступности. Добиться такого результата можно только при условии создания соответствующих международных соглашений, регламентирующих сотрудничество сторон и требующих осуществить криминализацию типовых преступных деяний в сфере ИКТ. Причем, учитывая мировой масштаб сформировавшейся информационной системы, такие международно-правовые механизмы должны создаваться и реализовываться не в рамках отдельно взятых регионов, но именно в глобальном масштабе.

В связи с указанным мнением встает вопрос о том, как именно следует организовать такую деятельность. С одной стороны, в рамках ООН уже ведется работа по созданию глобальной системы противодействия киберпреступности, в основу которой, в частности, входит деятельность ГПЭ и РГОС, а также инициативы России, связанные с разработкой проектов универсальных конвенций по борьбе с киберпреступностью – проект Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности 2017 г. [7] и проект Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях 2019 г. [5] С другой стороны, такую деятельность можно некоторым образом оптимизировать.

При рассмотрении возможных способов преодоления данной проблемы можно опираться на опыт решений похожих вопросов. Одним из таких может выступать проблема отмывания денег и финансирования терроризма (ОД/ФТ). Не смотря на принципиальные различия в сущностях явлений ОД/ФТ и киберпреступности, по мнению автора, концептуально проблема ОД/ФТ обладает сходствами с проблемой киберпреступности. Например, известные способы отмывания денег часто включают в себя осуществление финансовых транзакций с участием банковских систем множества различных государств – причем особенно в этом контексте для преступников привлекательны страны, в которых недостаточно эффективно реализованы меры по противодействию ОД/ФТ (ПОД/ФТ). Кроме того, часто для ОД/ФТ используются офшорные зоны, на территории которых реализованы условия, позволяющие сохранять анонимность владельцев компаний или сопровождать их деятельность минимальной отчетностью. Здесь можно провести аналогию с использованием цифровых технологий, обеспечивающих анонимность интернет-пользователей и шифрующих их трафик (например, VPN-сервисы). Или же

использование цифровой инфраструктуры государств, в которых недостаточно эффективно реализованы меры по обеспечению информационной безопасности, в целях совершения с их территории кибератак или иных противоправных деяний в сфере ИКТ.

Кроме того, финансовые транзакции, реальной целью которых является осуществление ОД/ФТ, часто проводят с использованием как можно большего количества финансовых организаций, переводя денежные средства сложными и разветвленными путями, регулярно дробя и объединяя переводимые суммы. Такие деяния осуществляются преступниками специально для того, чтобы запутать правоохранительные органы и замедлить расследование фактов ОД/ФТ. В данном случае подходящей аналогией из сферы кибербезопасности может оказаться разветвленность интернет-сетей, также значительно затрудняющих поиск первоначального источника преступного деяния и определение юрисдикции при расследовании преступления. При этом разветвленность мировой финансовой системы может быть сопоставима с разветвленностью интернет-сетей.

В связи с описанными особенностями представляется, что проблема ПОД/ФТ во многом концептуально схожа с проблемой киберпреступности. При этом важно отметить, что, как и в случае с национально-правовыми мерами по борьбе с киберпреступностью, национальные правовые механизмы в сфере экономической безопасности также могут отличаться в зависимости от юрисдикции. Несмотря на это, на международном уровне удалось реализовать систему ПОД/ФТ, предполагающую активное сотрудничество государств по данному вопросу, а также выработку унифицированных правовых мер в рамках национальных юрисдикций. А именно была создана Межправительственная комиссия по финансовому мониторингу (также известная как Группа разработки финансовых мер по борьбе с отмыванием денег или ФАТФ). Сущность деятельности данной организации предполагала сотрудничество государств-членов в целях выработки мер по совместному противодействию ОД/ФТ, а также оптимизации национальных законодательств в целях повышения эффективности такой деятельности. Основой для реализации таких задач выступили разработанные ФАТФ рекомендации по осуществлению государствами-членами соответствующих организационно-правовых мер, соблюдение которых повысит эффективность ПОД/ФТ в каждом отдельном государстве-участнике и, таким образом, снизит глобальную угрозу ОД/ФТ.

В связи с этим представляется, что на глобальном уровне решение проблемы всестороннего обеспечения кибербезопасности может быть осуществлено похожим способом. Учитывая описанные выше концептуальные сходства между ОД/ФТ и киберпреступностью, одним из возможных способов повышения уровня глобальной кибербезопасности может быть создание специализированной международной организации в сфере информационной безопасности, принцип работы которой будет дублировать организационную структуру ФАТФ.

Основу деятельности такой организации – как и в случае с ФАТФ – могли бы составить рекомендации, разработанные государствами-членами. Среди таковых могут быть, например, рекомендации по внедрению в национальные правовые системы положений, вводящих ограничения на использование технологий, маскирующих интернет-трафик. Другими такими рекомендациями могут быть положения, рекомендующие государствам-участникам создать в рамках своих юрисдикций специализированные организации, осуществляющие постоянный анализ в области национальных трендов актуальных проблем киберпреступности, на основе которого в дальнейшем будет осуществляться разработка новых правовых мер. Также важным рекомендательным положением выступает криминализация ряда типовых актуальных видов киберпреступлений. При этом

перечень рекомендаций представляется целесообразным регулярно пересматривать в целях его актуализации в соответствии с вновь возникшими цифровыми угрозами.

Кроме того, в состав такой международной организации целесообразно включить постоянно функционирующий экспертный аналитический центр, собирающий сведения от государств-участников о национальных проблемах кибербезопасности. Результатом работы такого центра могут выступать предложения по совершенствованию и актуализации действующих международно-правовых механизмов в связи с возникновение новых угрозы в сфере ИКТ. Так как цифровые технологии постоянно развиваются, а их структура становится все более сложной, работа такого подразделения представляется особенно важной в целях поддержания эффективного и адекватного международно-правового регулирования противодействия киберугрозам. При этом, по мнению автора, работу такого подразделения важно осуществлять на базе постоянного диалога не только между государствами-участниками, но также и на основе диалога между специалистами в области юриспруденции и специалистами в области информационных технологий. Как представляется, такой принцип организации позволит разрабатывать правовые меры, в наибольшей степени отвечающие современным тенденциям развития цифровых технологий. Кроме того, такой подход может помочь сблизить специалистов различных дисциплинарных направлений в контексте понимания проблемы правового регулирования информационных технологий. В перспективе это поспособствует повышению стандартов разработки безопасных цифровых технологий с одной стороны и выработке адекватных правовых норм – с другой.

Другим эффективным механизмом, который можно реализовать в рамках такой международной организации, может выступить регулярная экспертная оценка уровня обеспечения кибербезопасности в пределах национальных юрисдикций государств-членов (по аналогии с системой взаимных оценок национальных систем ПОД/ФТ в ФАТФ). Для такой деятельности в организации может быть создана отдельная рабочая группа, занимающаяся осуществлением таких оценок, регулярно проводящая ревизии в произвольно выбранных государствах-членах, а также составляющая рейтинг безопасности среди членствующих сторон.

При этом особенно важно построить всю деятельность предлагаемой к созданию организации на базе основных принципов международного права. В частности, необходимо отдельно подчеркнуть требование к государствам-участникам соблюдать суверенитет других членов. Положение о необходимости соблюдения суверенитета государств-членов и уважении к нему должно быть отдельно закреплено в статуте международной организации, регулирующем ее деятельность.

Таким образом, как представляется, создание международной организации с такой рабочей структурой может значительно простимулировать формирование и дальнейшее развитие международно-правовой системы противодействия киберпреступности. При этом, по мнению автор, особенно важно, чтобы деятельность такой организации простиралась далеко за пределы конкретных регионов и потенциально охватывала как можно большее количество государств. В связи с этим было бы целесообразно обеспечить работу организации в рамках ООН. Также важно обеспечить особые условия для членства в ней развивающихся стран и оказать им всевозможное содействие в реализации разрабатываемых организационно-правовых мер.

С одной стороны, автор осознает исключительную сложность в создании глобальной международно-правовой системы информационной безопасности. Различие в национальных подходах правового регулирования и в уровнях технологического

развития, а также политические противоречия могут замедлить процесс формирования глобальной правовой системы кибербезопасности. В связи с этим, более вероятным в ближайшее время представляется создание международно-правовых региональных центров противодействия киберпреступности, формирующихся на базе множества региональных организаций. С одной стороны, такое направление развития может стать эффективным решением проблемы международной киберпреступности, которое позволит упростить процессы межгосударственных расследований, а также сблизить национальные законодательства в пределах отдельных регионов. Однако, учитывая именно мировой, глобальный масштаб сложившейся информационной системы, все же представляется необходимость обеспечения оптимального базиса для развития общей международно-правовой системы, не ограниченной отдельными регионами.

При этом создание специализированной международной организации представляется одним из наиболее перспективных направлений в решении данного вопроса. История развития международного права наглядно демонстрирует, что создание различных специализированных международных организаций – таких как Международная морская организация, Международная организация гражданской авиации, Международный союз электросвязи и др. – значительно способствуют оптимизации развития международно-правового регулирования в конкретных областях жизнедеятельности. В рамках таких организаций государства совместно анализируют общие проблемы, вырабатывают международные договоры, учитывающие позиции заинтересованных сторон, и способствуют сближению национальных подходов регулирования. В связи с этим, учитывая мировой масштаб распространения цифровых технологий и разнонаправленность связанных с этим угроз, представляется особенно актуальным создание аналогичной организации в сфере обеспечения глобальной кибербезопасности.

Библиография

1. Глобальная программа кибербезопасности (ГПК) МСЭ [Электронный ресурс]: 2008 г. // Информация для всех [сайт]. URL: https://www.ifap.ru/pr/2008/080908aa.pdf (дата обращения: 30.04.2023).
2. Горелик И.Б. Роль международных организаций в процессе противодействия киберпреступности // Международное право. – 2022. – №3. – С. 33. (С. 28-41)
3. Конвенция о компьютерных преступлениях [Электронный ресурс]: 23 ноября 2001. ETS №185 // Совет Европы [сайт]. URL: https://rm.coe.int/1680081580 (дата обращения: 30.04.2023).
4. Максимов А.М., Тищенко Е.Н. Особенности использования носителей информации в защищённых информационных системах // Известия Южного федерального университета. Технические науки. – 2011. – С. 238-244.
5. Письмо Временного поверенного в делах Постоянного представительства Российской Федерации при Организации Объединенных Наций от 30 июля 2021 года на имя Генерального секретаря [Электронный ресурс]: Приложение к письму Временного поверенного в делах Постоянного представительства Российской Федерации при Организации Объединенных Наций от 30 июля 2021 года на имя Генерального секретаря. Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях. 10 августа 2021 г. A/75/980. // Организация Объединенных Наций [сайт]. URL: https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/75/980&Lang=R (дата обращения: 30.04.2023).
6. Понимание киберпреступности: Руководство для развивающихся стран

[Электронный ресурс]: апрель 2009 г. // Международный Союз Электросвязи [сайт]. URL: https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf (дата обращения: 30.04.2023).

7. Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности [Электронный ресурс]: Приложение к письму Постоянного представителя Российской Федерации при Организации Объединенных Наций от 11 октября 2017 года на имя Генерального секретаря. 16 октября 2017 г. A/C.3/72/12 // Организация Объединенных Наций [сайт]. URL: https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/C.3/72/12&Lang=R (дата обращения: 30.04.2023)
8. Соглашение о сотрудничестве Государства-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // СЗ РФ. – 30.03.2009. – №13. – ст. 1460.
9. Соглашение о сотрудничестве Государства-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // СЗ РФ. – 15.08.2022. – №33. – ст. 5883.
10. Ястребова А.Ю., Акчурин Т.Ф., Анисимов И.О., Горелик И.Б. Право человека на защиту персональных данных: международно-правовые основы, примеры их имплементации в законодательстве государств, особенности регламентации в праве ЕС и национальном праве США // Международный правовой курьер. – 2021. – №7. – С. 93-106.
11. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems [Electronic resource]: 28 Jan. 2003. ETS №189 // Council of Europe [website]. URL: https://rm.coe.int/168008160f (дата обращения: 30.04.2023).
12. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [Electronic resource]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680 (дата обращения: 30.04.2023).
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Electronic resource]. – URL: https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1626789259064 (дата обращения: 30.04.2023).
14. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) [Electronic resource]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN (дата обращения: 30.04.2023).
15. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence [Electronic resource]: 12 May 2022. ETS №224 // Council of Europe [website]. URL: https://rm.coe.int/1680a49dab (дата обращения: 30.04.2023).

Результаты процедуры 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 «Возможные направления развития международно-правовых институтов в области обеспечения глобальной кибербезопасности».

Предмет исследования.
Предложенная на рецензирование статья посвящена актуальным вопросам развития международно-правовых институтов в области обеспечения глобальной кибербезопасности. Автор обобщает опыта ряда международных организаций в сфере подготовки правовых актов, затрагивающих аспекты глобальной кибербезопасности. В качестве предмета исследования выступили положения международных правовых актов, мнения ученых, практика деятельности международных организаций.

Методология исследования.
Цель исследования прямо в статье не заявлена. При этом она может быть ясно понята из названия и содержания работы. Цель может быть обозначена в качестве рассмотрения и разрешения отдельных проблемных аспектов вопроса о перспективных направлениях развития международно-правовых институтов в области обеспечения глобальной кибербезопасности. Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования.
В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике, а также сделать конкретные выводы из материалов практики деятельности различных международных организаций.
Наибольшую роль сыграли специально-юридические методы. В частности, автором активно применялся формально-юридический метод, который позволил провести анализ и осуществить толкование норм действующего законодательства (прежде всего, положений международных правовых актов). Например, следующий вывод автора: «В рамках другой региональной международной организации – Европейского Союза – также осуществлялась активная выработка международно-правовых соглашений в области защиты персональных данных [10, С. 97]. В частности, была создана система международно-правовых норм, среди которых можно выделить Общий Регламент Европейского Парламента и Совета Европы № 2016/679 по защите персональных данных физических лиц 2016 г. [13], Регламент Европейского Парламента и Совета Европы № 1725/2018 от 23 октября 2018 г. о защите физических лиц при обработке персональных данных институтами, органами, ведомствами и агентствами и о свободном обращении таких данных [14], а также Директива Европейского Парламента и Европейского Совета № 680/2016 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или судебного преследования уголовных правонарушений или при исполнении уголовных наказаний [12]».
Другой пример, когда автор сопоставляет практику деятельности различных международных организаций: «В рамках ООН работа по выработке правовых основ противодействия киберпреступности осуществлялась на основе деятельности

специализированной организации – Международного союза электросвязи, разработавшего Глобальную программу кибербезопасности 2008 г. [1] и Руководство по пониманию киберпреступности для развивающихся стран 2009 г. [6]. Более того, по инициативе России в ООН были созданы две специализированные группы – Рабочая группа открытого состава (РГОС) и Группа правительственных экспертов (ГПЭ). Основные результаты деятельности указанных групп оформлялись в виде резолюций Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»».
Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.
Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории тема обеспечения глобальной кибербезопасности сложна и неоднозначна. В современном мире угрозы в цифровой среде опасны как в сфере обеспечения личных прав и свобод (к примеру, в сфере защиты персональных данных, тайны личной жизни), так и непосредственно в связи с охраной имущественных интересов (нередко мошеннические действия и иные хищения совершаются с использованием возможностей цифровой среды). Однако решение проблемы ввиду глобальности онлайн-пространства возможно только на наднациональном международном уровне, что, учитывая нынешнюю экономическую и политическую ситуацию, представляется трудно разрешимой задачей. Автор прав, что осветил этот аспект актуальности. С практической стороны следует признать, что необходимы поиски механизмов совершенствования международно-правового регулирования в рассматриваемой сфере. Приводимые автором в статье примеры из практики деятельности различных международных организаций демонстрируют этот вопрос.
Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.
Научная новизна предложенной статьи не вызывает сомнений. Во-первых, она выражается в конкретных выводах автора. Среди них, например, такой вывод:
«автор осознает исключительную сложность в создании глобальной международно-правовой системы информационной безопасности. Различие в национальных подходах правового регулирования и в уровнях технологического развития, а также политические противоречия могут замедлить процесс формирования глобальной правовой системы кибербезопасности. В связи с этим, более вероятным в ближайшее время представляется создание международно-правовых региональных центров противодействия киберпреступности, формирующихся на базе множества региональных организаций. С одной стороны, такое направление развития может стать эффективным решением проблемы международной киберпреступности, которое позволит упростить процессы межгосударственных расследований, а также сблизить национальные законодательства в пределах отдельных регионов. Однако, учитывая именно мировой, глобальный масштаб сложившейся информационной системы, все же представляется необходимость обеспечения оптимального базиса для развития общей международно-правовой системы, не ограниченной отдельными регионами».
Важен и другой вывод: «При этом создание специализированной международной организации представляется одним из наиболее перспективных направлений в решении данного вопроса. История развития международного права наглядно демонстрирует, что создание различных специализированных международных организаций – таких как

Международная морская организация, Международная организация гражданской авиации, Международный союз электросвязи и др. – значительно способствуют оптимизации развития международно-правового регулирования в конкретных областях жизнедеятельности. В рамках таких организаций государства совместно анализируют общие проблемы, вырабатывают международные договоры, учитывающие позиции заинтересованных сторон, и способствуют сближению национальных подходов регулирования. В связи с этим, учитывая мировой масштаб распространения цифровых технологий и разнонаправленность связанных с этим угроз, представляется особенно актуальным создание аналогичной организации в сфере обеспечения глобальной кибербезопасности».

Указанный и иные теоретические выводы могут быть использованы в дальнейших научных исследованиях. Приведенные выводы могут быть актуальны и полезны для правотворческой деятельности.

Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.

Стиль, структура, содержание.

Тематика статьи соответствует специализации журнала «Международное право», так как она посвящена правовым проблемам, связанным с направлениями развития международно-правовых норм и положений в определенной сфере (обеспечение глобальной кибербезопасности).

Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели исследования.

Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.

Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.

Библиография.

Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России и из-за рубежа (Горелик И.Б., Максимов А.М., Тищенко Е.Н., Ястребова А.Ю., Акчурин Т.Ф., Анисимов И.О. Горелик И.Б. и другие).

Таким образом, труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.

Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.

Выводы в полной мере являются логичными, так как они получены с использованием общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к вопросам перспективных направлениях развития международно-правовых институтов в области обеспечения глобальной кибербезопасности.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи

«Рекомендую опубликовать»