На правах рукописи

Гирис Валерия Алексеевна

Правовое регулирование деятельности Европейского Союза в области обеспечения кибербезопасности

5.1.5. Международно-правовые науки

Автореферат диссертации на соискание
ученой степени кандидата
юридических наук

Москва - 2024

Работа выполнена на кафедре интеграционного и европейского права ФГАОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)».

Научный руководитель: **Четвериков Артем Олегович**
доктор юридических наук, профессор

Официальные оппоненты: **Понаморенко Владислав Евгеньевич**
доктор юридических наук, доцент, ФГБОУ ВО «Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации», профессор кафедры публичного права

Гуляева Елена Евгеньевна
кандидат юридических наук, доцент, ФГБОУ ВО «Дипломатическая академия Министерства иностранных дел Российской Федерации», доцент кафедры международного права

Ведущая организация **Федеральное государственное бюджетное учреждение науки «Институт государства и права Российской академии наук»**

Защита состоится «5» февраля 2025 года в 13:00 на заседании диссертационного совета 24.2.336.04, созданного на базе ФГАОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)», г. Москва, 123242, ул. Садовая-Кудринская, д. 7, строение 22, зал диссертационного совета.
С диссертацией можно ознакомиться в библиотеке и на официальном сайте ФГАОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)» http://msal.ru.

Автореферат разослан «___» _____ 20__ г.

Ученый секретарь
диссертационного совета,
доктор юридических наук,
профессор **А.В. Корнев**

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В XXI в. развитие общества, государства, права на всей планете протекает под влиянием процессов цифровизации (цифровой трансформации, дигитализации), в основе которых лежат информационно-коммуникационные технологии (далее – ИКТ) и создаваемые благодаря им информационные сети, системы, базы данных и т.д. «Мы вступаем в так называемую цифровую эпоху, которая может изменить и уже серьезно меняет наш мир»[1].

Изменения в мире, порождаемые цифровизацией, не всегда носят благоприятный характер. Новые возможности и преимущества, получаемые от широкомасштабного внедрения ИКТ в публично-правовые и частно-правовые отношения, сопровождаются появлением новых видов опасностей и преступных посягательств («кибератаки», «киберугрозы»), которые фактически превратились в новую глобальную проблему для всего человечества.

Как отмечал министр иностранных дел Российской Федерации С.В. Лавров, еще более 20 лет назад, в 1998 г., Россия с трибуны Организации Объединенных Наций (далее – ООН) «первой предупредила мир о рисках, которые таила в себе тогда еще зарождающаяся киберсфера, и предложила конкретные пути противодействия им»[2]. Позднее, в 2011 г., Россия вместе с рядом других государств разработала «Концепцию Конвенции ООН об обеспечении международной информационной безопасности»[3], а в 2023 г. представила обновленную концепцию того же документа[4].

---

[1]Корнев А.В. Дигитализация права: проблемы и перспективы // Актуальные проблемы российского права. 2019. № 6 (103). С. 11.

[2]Лавров С.В. Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью// Журнал «Внешнеэкономические связи», 28 сентября 2020.

[3]Совет Безопасности Российской Федерации: Концепция Конвенции ООН об обеспечении международной информационной безопасности. URL: http://www.scrf.gov.ru/security/information/document112/ (дата обращения 01.02.2024).

[4]Обновленная концепция Конвенции Организации Объединенных Наций об обеспечении международной информационной безопасности. Предложение Российской Федерации Соавторы: Республика Беларусь, Корейская Народно-Демократическая Республика, Республика Никарагуа, Сирийская Арабская Республика. URL:https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-

Сегодня можно с уверенностью утверждать, что обеспечение кибербезопасности (и, в более широком контексте, информационной безопасности) является одним из наиболее острых вызовов, на которые государствам предстоит ответить, действуя как индивидуально[5], так и совместно – в рамках международных организаций и международных интеграционных объединений.

В связи со сложностью и длительностью согласования позиций государств на глобальном уровне (в частности, в рамках ООН) их международное сотрудничество и интеграция в деле совместного обеспечения кибербезопасности пока более успешно развивается на региональном уровне. В свою очередь, среди региональных международных организаций и интеграционных объединений наиболее весомых результатов в разработке единообразных правовых стандартов обеспечения кибербезопасности достиг Европейский Союз (далее кратко – ЕС, Союз).

В отличие от своих аналогов в других регионах Земного шара, где юридически обязательные нормы по обеспечению кибербезопасности закрепляются международными договорами, вступление в силу и пересмотр которых обычно требует ратификационных процедур в парламентах государств-участников (например, Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г. или Конвенция Африканского союза о кибербезопасности и защите персональных данных от 27 июня 2014 г., подписанная пока менее чем половиной – 18 из 55, и ратифицированная еще

_(2021)/RUS_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation_0.pdf (дата обращения: 01.02.2024).

[5] В России обеспечение информационной безопасности определено Указом Президента Российской Федерации от 07.05.2024 N 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» в качестве одной из задач, выполнение которой характеризует достижение национальной цели «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы».

меньшим числом государств-членов Африканского союза – 14 из 55)[6], органами ЕС с той же самой целью издаются законодательные и подзаконные акты общеобязательного характера, действующие во всех его государствах-членах без ратификации. Для сравнения: подготовленный в рамках Содружества Независимых Государств Модельный закон «О противодействии киберпреступности»[7], который содержит определения понятий «кибербезопасность»[8], «киберпространство»[9], является не более чем рекомендацией, исходя из которой государства-участники, при желании, могут принимать новые и пересматривать действующие национальные нормативные правовые акты.

В современном законодательстве ЕС, направленном на обеспечение кибербезопасности, регулируемые им общественные отношения официально квалифицируются как «область кибербезопасности»[10], что свидетельствует о приобретении интеграционным правотворчеством ЕС в данной области качества самостоятельного направления правового регулирования.

Одновременно нужно учитывать, что ЕС не только старается обеспечить высокий уровень кибербезопасности собственных органов, государств-членов, граждан и юридических лиц, но и сам может выступать источником киберугроз для российского государства и гражданского общества. Подавляющее большинство государств-членов ЕС являются членами Организации

---

[6] См.: List of Countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection. 11.04.2023. URL: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (дата обращения: 01.02.2024).

[7] Модельный закон О противодействии киберпреступности // Постановление МПА СНГ от 14.04.2023 № 55-20.

[8] Кибербезопасность — сохранение конфиденциальности, целостности и доступности информации в киберпространстве, а также защищенности информационной инфраструктуры.

[9] Киберпространство — цифровая среда, возникающая в результате взаимодействия людей, программного обеспечения и сервисов в информационно-телекоммуникационных сетях, включая сеть «Интернет», посредством связанных с ними технологических устройств и сетей, не существующая в физической форме.

[10] Area of cybersecurity (англ.); domaine de la cybersécurité (франц.); Bereich der Cybersicherheit (нем.); областта на киберсигурността (болг.) и т.д.

Североатлантического договора (НАТО, Североатлантический альянс), а ЕС в целом еще с 2003 г. связан с НАТО пакетом секретных соглашений о сотрудничестве и безопасности «Берлин плюс»[11]. В этой связи, как отмечалось в одном из недавних документов Парламентской ассамблеи НАТО: «Сотрудничество с Европейским Союзом в отношении киберпространства также рассматривается в качестве приоритета для Альянса. НАТО и Европейский Союз – естественные партнеры для киберсотрудничества»[12].

Итак, анализ, осмысление, оценка сильных и слабых сторон правового регулирования ЕС в области обеспечения кибербезопасности представляют существенный теоретический и практический интерес для российского государства и правоведения. В свою очередь, исследование данной области в рамках международно-правовых наук (специальность 5.1.5. Номенклатуры научных специальностей, по которым присуждаются ученые степени) способно расширить научные представления о современных проблемах, тенденциях, направлениях, перспективах развития правовой интеграции в разных регионах Земного шара, в том числе на предмет использования выявленного положительного и отрицательного опыта в правовом регулировании евразийской интеграции.

Степень научной разработанности темы. Правовым проблемам, возникающим в связи с необходимостью обеспечения информационной безопасности (в том числе кибербезопасности), и путям их решения посвящены работы ведущих российских ученых-правоведов (И.Л. Бачило, А.В. Корнев, Е.К. Матевосова, А.В. Минбалеев, Н.А. Молчанов, О.В. Танимов, Л.В. Терентьева и др.). В рамках международно-правовых наук данные вопросы исследовались в

---

[11]Право Европейского Союза. Т. 2. Особенная часть. Основные отрасли и сферы регулирования права Европейского Союза. Правовые аспекты участия России в европейских интеграционных процессах. Учебник / под ред. С.Ю. Кашкина. М.: Юрайт, 2013. С. 934 – 935.

[12]NATO Parlamentary Assembly. The Offence-Defence Balance: NATO's Growing Cyber Challenge. Report № 015 DSCFC 22 E rev. 1 fin. 19 November 2022. P. 14. URL: https://www.nato-pa.int/download-file?filename=/sites/default/files/2023-01/015%20DSCFC%2022%20E%20rev.%201%20fin%20-%20OFFENSE%20DEFENCE%20BALANCE%20CYBER%20CHALLENGE%20-%20REPORT%20LOVERDOS.pdf (дата обращения: 01.02.2024).

трудах Л. Аримацу (L. Arimatsu), В.А. Батыря, Р. Баллесте (R. Balleste), Р.А. Вессела (R.A.Wessel), Э. Верхелст, А.А. Данельяна, П. Дугалл (P. Duggal), А.Я. Капустина, М.Б. Касеновой, К. Киттичайсари (K. Kittichaisaree), Д. Косефа (J.Koseff), Д. Кулеши (J. Kulesza), Д.В. Красикова, Д. Одерматт (J. Odermatt), А. Осулы (A.Osula), Т.А. Поляковой, М. Роскини (M.Roscini), В.П. Талимончик, Э. Тик (E. Tikk), Д.П. Фидлера (D. Fidler), Э. Фейх (E. Fahey), Г.Г. Фустера (G.G. Fuster), Н. Цагуариса (N. Tsagourias), М.Г. Порседды (M.G. Porcedda), Г.Г. Шинкарецкой и др. В России также опубликовано несколько научных статей, в которых рассмотрены отдельные аспекты правового регулирования обеспечения кибербезопасности в ЕС[13].

В то же время, необходимо отметить, что в рамках российских международно-правовых наук пока отсутствует обстоятельное монографическое, в том числе диссертационное, исследование, посвященное осмыслению всего комплекса правовых норм ЕС в области обеспечения кибербезопасности, а многие ранее опубликованные работы не учитывают последних новаций права ЕС в этой области, связанных с подготовкой новых законопроектов взамен или в дополнение ранее изданных законодательных актов о кибербезопасности.

Отмеченный пробел призвана восполнить настоящая диссертация, где впервые, опираясь на положения и научный аппарат международно-правовых наук в целом и проводимых в их рамках интеграционно-правовых исследований, в частности, предпринята попытка сформировать комплексное научное

[13]Елин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом: монография/ под общ. Ред. А.П. Баранова. М. : Московский институт государственного управления и права, 2016. 168 с.; Галицкая Н.В. Право на кибербезопасность: опыт Европейского Союза // Права человека и политика права в XXI в.: перспективы и вызовы Сборник научных трудов по итогам Всероссийской научно-практической конференции с международным участием. Саратов, 2022. С.440-449; Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности//Вопросы кибербезопасности. 2022. №1(53). С. 58-74; Пантин В.И. Кардава Н.В. Кибербезопасность: проблемы формирования единой политики в европейском Союзе// Вестник Пермского университета. Политология.2018.№3. С. 8-21.

представление о состоянии и перспективах развития правового регулирования ЕС в области кибербезопасности.

Цель и задачи исследования. Целью исследования является формирование целостного научного представления об истории и современном состоянии, перспективах дальнейшего развития правового регулирования ЕС в области обеспечения кибербезопасности с формулированием практических рекомендаций по использованию данного опыта в контексте евразийской интеграции – для Евразийского экономического союза, Союзного государства России и Беларуси.

Достижение обозначенной цели предполагает решение следующих задач:

- выявление юридического смысла понятия «кибербезопасность» в праве ЕС в сопоставлении с правовыми подходами к определению кибербезопасности и информационной безопасности в других международно-правовых и национальных (внутригосударственных) актах, а также в доктрине;

- исследование международно-правовых основ сотрудничества и интеграции государств в области обеспечения кибербезопасности в целом и правовых основ осуществления деятельности в этой области, осуществляемой органами общей и специальной компетенции ЕС, в частности;

- анализ и оценка содержания и результатов правового регулирования ЕС по обеспечению кибербезопасности субъектов публичной власти и гражданского общества во всех сферах общественной жизни;

- анализ и оценка содержания и результатов правового регулирования ЕС в ключевых сферах общественной жизни, для которых органами ЕС установлены специальные правила обеспечения кибербезопасности;

- поиск правовых достижений ЕС, которые могли бы быть использованы в практическом плане в целях совершенствования правового регулирования евразийской интеграции между Россией и другими республиками бывшего Союза ССР.

Объектом исследования выступают общественные отношения, складывающиеся в ходе принятия и претворения в жизнь источников и норм

права ЕС в области обеспечения кибербезопасности органов ЕС, его государств-членов, граждан и юридических лиц, а также функционирующих в ЕС сетей, информационных систем, продуктов информационно-коммуникационных технологий.

Предмет исследования образуют нормы первичного и вторичного права ЕС, положения законопроектов ЕС, иных международно-правовых актов и проектов, а также нормы национального законодательства государств-членов ЕС и третьих государств (прежде всего, законодательства, направленного на имплементацию права ЕС в национальные правовые системы).

Методологическую основу исследования составили философские, общенаучные и специальные методы научного познания правовых явлений, в частности, диалектический, системный, исторический (историко-правовой), сравнительный (сравнительно-правовой), формально-юридический, методы логической дедукции и индукции, а также междисциплинарный подход.

Сравнительный (сравнительно-правовой) метод широко использовался для сопоставления понятийного аппарата и содержания источников права ЕС с аналогичными по предмету источниками международного права и национальных правовых систем.

Исторический (историко-правовой) метод был положен в основу анализа процессов становления и развития правового регулирования ЕС в области кибербезопасности.

Другие вышеуказанные методы применялись в тех же целях, а также для достижения корректного толкования исследуемых юридических норм.

На базе междисциплинарного подхода автор для всесторонней оценки исследуемых правовых явлений обращался к положениям и выводам, содержащимся в трудах иных, чем международно-правовые, наук (юридических и неюридических), в которых затрагивается проблема обеспечения кибербезопасности.

Теоретическую основу исследования составляют, прежде всего, труды отечественных и зарубежных представителей международно-правовых наук, в которых представлена современная отечественная доктрина по вопросам международного публичного права и правового регулирования международной интеграции: А.Х. Абашидзе, Л.П. Ануфриева, К.А. Бекяшев, М.М. Бирюков, П.Н. Бирюков, Г.Де Бурка (G. Burca), Я. Ваутерс (J. Wouters), Г.М. Вельяминов, П.А. Калиниченко, Э. Канниццаро (E.Cannizzaro), А.Я. Капустин, С.Ю. Кашкин, П.Крейг (P. Craig), М. Куртин (D. Curtin), А. Лазовски (A. Lazowski), И.И. Лукашук, И.М. Лифшиц, Е.Г. Моисеев, О.М. Мещерякова, В.Е. Понаморенко, В.Л. Толстых, Н.А. Соколова, А.О. Четвериков, В.М. Шумилов, К. Экес (C.Eckes), В. Эльсувеге (V. Elsuwege), Л.М. Энтин, М.Л. Энтин, Ю.М. Юмашев и др.

Существенную помощь в понимании исследуемых явлений оказало изучение трудов представителей других юридических наук, особенно, применительно к вопросам трансформации права в условиях цифровизации современного общества: И.Л. Бачило, А.А. Карцхия, А.В. Корнев, В.Н. Синюков, Э.В. Талапина, Т.Я. Хабриева, С.М. Шахрай и др.

Применительно к регулированию кибербезопасности в праве ЕС и других правовых системах автором использовались специально посвященные ей труды упомянутых выше российских и зарубежных ученых правоведов: Л. Аримацу, В.А. Батыря, Р. Баллесте, Я. Ваутерса, Р. Вессела, Э. Верхелста, А.А. Данельяна, П. Дугалла (P. Duggal), А.Я. Капустина, М.Б. Касеновой, К. Киттичайсари (K. Kittichaisaree), Д. Косефа (J.Koseff), Д. Кулеши (J.Kulesza), Д.В. Красикова, А.М. Осулы (A.Osula), Т.А. Поляковой, М. Роскини (M.Roscini), В.П. Талимончик, Д.П. Фидлера (D. Fidler), Э. Фейх (E. Fahey), Г.Г. Фустер (G.G. Fuster), Н. Цагуариса (N.Tsagourias), М.Г. Порседды (M.G. Porcedda), Г.Г. Шинкарецкой и др.

Наконец, лучшему осознанию серьезности и характера проблем в области обеспечения кибербезопасности и путей их решения способствовало

ознакомление автора с трудами представителей других наук, в том числе специалистов по кибербезопасности и информационной безопасности: Р.С. Дьюар (R.S. Dewar), Е.С. Зиновьевой, М. Д. Кавелти (M.D. Cavelty), А.В. Крутских, Г. Кристоу (G. Christou), А.Х. Лашкари (A.H. Lashkari), Т. Маурера (T. Maurer), А.В. Манойло, Н.П. Ромашкиной, К. Рула (C. Ruhl), К. Хендерсона (C. Henderson), Д.Б. Холлиса (D.B. Hollis), У. Хоффмана (W. Hoffman) и др.

Нормативную основу исследования образуют действующие, ранее действовавшие и проектируемые источники права ЕС, подготовительные, консультативные и иные документы, принятые органами ЕС в рамках правотворческих процедур; международные договоры, акты, проекты и иные документы других международных организаций и интеграционных объединений; нормативные правовые акты государств-членов ЕС, направленные на трансформацию (имплементацию) права ЕС в национальные правовые системы, другие источники национального права, содержащие нормы по вопросам кибербезопасности, которые имеют отношение к цели, задачам, объекту и предмету настоящего исследования.

Научная новизна исследования. Новизна настоящей диссертации определяется, в первую очередь, ее целью и задачами, объектом и предметом, а также методологией, которые предполагают исследование всего комплекса вопросов, имеющих существенное значение для осмысления вклада права ЕС в развитие правового регулирования в области обеспечения кибербезопасности в сопоставлении с достижениями в этой области других правовых систем.

В частности, в 1 главе впервые в отечественных международно-правовых науках автором проведен анализ понятия «кибербезопасность» как новой юридической категории, все чаще используемой совместно с ранее возникшей категорией «информационная безопасность» или вместо нее.

Также впервые в диссертации исследовано историческое развитие правового регулирования ЕС в области обеспечения кибербезопасности, статус

Агентства по кибербезопасности и других органов ЕС, наделенных специальными полномочиями в этой области.

В главах 2 – 3 автором осуществлен не имеющий аналогов в ранее опубликованных научных трудах обстоятельный анализ по состоянию на первую половину 2024 г. содержания и результатов правотворческой деятельности ЕС в области обеспечения кибербезопасности субъектов публичной власти, гражданского общества в целом, а также участников общественных отношений в отдельных сферах жизни, исходя из которого выдвинуты оригинальные практические предложения по использованию опыта права ЕС для развития правового регулирования евразийской интеграции.

Автором введен в научный оборот обширный новый нормативный материал, который представляет интерес не только для международно-правовых наук, но и для юридических и междисциплинарных исследований в рамках других отраслей знаний.

Основные положения, выносимые на защиту. В соответствии с результатами проведенного исследования и сделанными из него выводами на защиту выносятся следующие основные положения, содержащие существенные признаки научной новизны.

1. Среди международных организаций и международных интеграционных объединений деятельность по обеспечению кибербезопасности наибольших масштабов достигла в Европейском Союзе (ЕС) с точки зрения 1) количества изданных и готовящихся к принятию источников юридически обязательных норм в этой области, 2) их предмета и содержания, охватывающих меры по обеспечению кибербезопасности субъектов публичной власти на разных уровнях и гражданского общества в разных сферах общественной жизни, 3) темпов модернизации действующего законодательства о кибербезопасности и его адаптации к новым вызовам и угрозам в киберпространстве.

2. Как и другие международные организации, интеграционные объединения, а также государства на национальном уровне, ЕС осуществляет рассматриваемую

деятельность ради обеспечения не только «кибербезопасности», но и «информационной безопасности». Следует согласиться с позицией Международной организации по стандартизации в том, что последняя является более широким (родовым) понятием по отношению к первой: если «информационная безопасность» подразумевает сохранение конфиденциальности, целостности и доступности любой информации, то «кибербезопасность» означает то же самое, но применительно к информации в киберпространстве, т.е. создаваемой, хранящейся и обрабатываемой с использованием информационно-коммуникационных (компьютерных) технологий.

В то же время, необходимо отметить, что сегодня в государствах и на международной арене пока не выработано единого подхода к разграничению информационной безопасности и кибербезопасности вплоть до полного отождествления двух понятий в национальных стратегиях по кибербезопасности некоторых государств-членов ЕС. Первым шагом мирового сообщества в преодолении сложившегося терминологического дуализма, по мнению диссертанта, могла бы стать подготовка в рамках системы ООН универсального классификатора в этой сфере, содержащего дефиниции ключевых понятий (подобно «Международной стандартной классификации образования» ЮНЕСКО и др.).

3. Термин «кибербезопасность» официально появился в ЕС сначала в качестве политической категории: впервые был использован Европейской комиссией в «Стратегии кибербезопасности Европейского Союза – Открытое, безопасное и надежное киберпространство» 2013 г. вместо выражения «сетевая и информационная безопасность», фигурировавшего в аналогичной по предмету проекте Стратегии 2001 г..

В настоящее время кибербезопасность выступает в качестве полноценной категории права ЕС, которая используется в нормативных правовых актах и получила там легальное определение. Понимание кибербезопасности в

современном праве ЕС имеет двойственный характер: состояние защищенности от киберугроз и действия, направленные на достижение подобного состояния.

Данный вывод вытекает из системного толкования нормы-дефиниции рассматриваемой категории в Акте о кибербезопасности 2019 г. (Регламент (ЕС) 2019/881 от 17 апреля 2019 г.) – «деятельность, необходимая для защиты сетевых и информационных систем, пользователей таких систем и других лиц, пострадавших от киберугроз», во взаимосвязи с положениями других нормативных правовых актов ЕС, которые предусматривают достижение повсеместно в ЕС высокого уровня кибербезопасности (например, Директива 2022/2555 от 14 декабря 2022 г. «О мерах по обеспечению общего высокого уровня кибербезопасности в рамках Союза»).

4. В системе источников права ЕС нормы, направленные на обеспечение кибербезопасности, закрепляются в юридически обязательных актах вторичного права прямого (регламенты, реже решения) и непрямого (директивы) действия, издаваемых законодательными органами ЕС (Европейский парламент и Совет) в рамках компетенции, предоставленной учредительными договорами (источниками первичного права) ЕС, которые далее уточняются и дополняются подзаконными актами Европейской комиссии.

Наибольшее значение для издания законодательства о кибербезопасности ЕС имеет ст. 114 Договора о функционировании ЕС о сближении (гармонизации) правовых норм государств-членов ЕС, затрагивающих создание и функционирование единого внутреннего рынка ЕС. В правотворческой и судебной практике ЕС данная статья получила широкое толкование, не ограничивающее ее предмет только вопросами экономической интеграции и фактически превращающее ее в источник дополнительной компетенции ЕС. Это, в частности, позволило издать на ее основе Акт о кибербезопасности 2019 г., устанавливающий правовую основу деятельности главного специализированного органа ЕС по координации мероприятий в рассматриваемой области – Агентства по кибербезопасности.

Помимо Агентства по кибербезопасности в организационном механизме ЕС функционирует множество других органов, подразделений органов, групп или сетей национальных органов, занимающихся вопросами обеспечения кибербезопасности, в том числе во взаимосвязи с противодействием киберпреступности.

5. В современной правотворческой деятельности ЕС – общественные отношения, вопросы, проблемы, возникающие в связи с обеспечением кибербезопасности, признаны в качестве особой сферы правового регулирования (используется выражение «область кибербезопасности» – в частности, в вышеупомянутых Акте о кибербезопасности и Директиве 2022/2555).

Отсюда вытекает целостный (комплексный) подход ЕС к обеспечению кибербезопасности всех субъектов публичной власти и гражданского общества, в рамках которого каждый из них должен принимать меры по защите себя от киберугроз, а субъекты публичной власти (ЕС в лице его органов и все государства-члены в отдельности) также обязаны обеспечивать кибербезопасность граждан, других физических и юридических лиц, проживающих, находящихся, осуществляющих деятельность в пределах их юрисдикции.

Кроме того, законодательство ЕС об обеспечении кибербезопасности (законодательство в «области кибербезопасности») характеризуется превентивным подходом, сущность которого состоит в заблаговременном выявлении, предотвращении и своевременной нейтрализации нынешних и возможных будущих киберугроз.

6. Наряду с общими вопросами обеспечения кибербезопасности правовое регулирование ЕС предусматривает меры, относящиеся к кибербезопасности в отдельных сферах жизни и более узких секторах (транспорт, энергетика и т.д.). Соответствующие нормы права нередко включаются в законодательство, посвященное регулированию общественных отношений в этих сферах или секторах (например, в Европейский кодекс электронных коммуникаций 2018 г.).

Таким образом, правовое регулирование ЕС в области обеспечения кибербезопасности развивается путем издания органами ЕС двух видов источников:

1) акты, целиком посвященные вопросам кибербезопасности;

2) акты, посвященные, в основном, иным вопросам, но включающие также отдельные нормы по вопросам кибербезопасности.

7. В качестве главных достижений европейской интеграции в области обеспечения кибербезопасности и ее правового регулирования в законодательстве ЕС следует признать:

- разработку единообразных подходов к определению «высокого уровня» кибербезопасности и мер, подлежащих принятию для его достижения всеми государствами-членами ЕС;

- создание на уровне ЕС специализированного Агентства по кибербезопасности как общего экспертно-аналитического центра, аккумулирующего информацию и вырабатывающего стандарты надлежащей практики в этой области;

- учреждение в ЕС Европейского центра компетенции в области промышленности, технологий и исследований по кибербезопасности и Сети национальных координационных центров с целью развития технологического, академического, общественного, исследовательского потенциала кибербезопасности;

- установление правовых основ для добровольной системы сертификации кибербезопасности во всех государствах-членах ЕС («Европейская схема сертификации кибербезопасности»).

8. В качестве основных недостатков современного уровня развития европейской интеграции в области обеспечения кибербезопасности, которые планируется в ближайшее время устранить путем принятия новых законодательных актов ЕС, следует признать:

- промедление с установлением единообразных требований к «продуктам с цифровыми элементами» (проект посвященного им Акта о кибер устойчивости представлен Европейской комиссией в сентябре 2022 г.);

- большие финансовые расходы на функционирование разветвленной системы органов, деятельность которых посвящена кибербезопасности, и наличие элементов дублирования в их функциях и полномочиях.

В качестве недостатка также следует признать сохранение в законодательстве и новых законопроектах ЕС терминологического дуализма «кибербезопасность» – «информационная безопасность» без указания на соотношение двух понятий по содержанию и объему.

9. Исследованные в настоящей диссертации правовые достижения и недостатки европейской интеграции свидетельствуют о принципиальной возможности включения вопросов обеспечения кибербезопасности в деятельность других региональных интеграционных объединений, в том числе с участием России.

В частности, посредством «международного договора в рамках Союза» государств-членов Евразийского экономического союза (ЕАЭС) могли бы быть установлены общие стандарты обеспечения кибербезопасности в таможенном союзе и на едином экономическом пространстве ЕАЭС. Аналогичный международный договор или акт Высшего государственного совета, касающийся обеспечения кибербезопасности во всех сферах общественной жизни, включая оборону и государственную безопасность, мог бы быть принят в рамках Союзного государства России и Беларуси.

Кроме того, целесообразно рассмотреть вопрос о создании в рамках ЕАЭС и (или) Союзного государства органа специальной компетенции, аналогичного по задачам и функциям Агентству по кибербезопасности ЕС.

Теоретическая и практическая значимость исследования. Материалы диссертационного исследования могут быть использованы в научных исследованиях в рамках международно-правовых наук, а также других

юридических наук, при осуществлении образовательной деятельности в образовательных организациях высшего образования по таким учебным дисциплинам, как «Международное право», «Интеграционное право», «Право интеграционных объединений», «Информационное право», «Правовое регулирование информационной безопасности» и др.

В практическом плане результаты исследования способны послужить целям совершенствования российского законодательства, развития правового регулирования интеграционных процессов в рамках, прежде всего, таких интеграционных объединений, как Союзное государство России и Беларуси, Евразийский экономический союз, Организация Договора о коллективной безопасности, Содружество Независимых Государств, при подготовке новых международных договоров Российской Федерации по вопросам кибербезопасности и (или) информационной безопасности.

Степень достоверности и апробация результатов.

Диссертационная работа выполнена, обсуждалась и была рекомендована к защите на заседании кафедры интеграционного и европейского права Федерального государственного автономного образовательного учреждения высшего образования «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)».

Основные выводы нашли отражение в статьях автора, опубликованных в научных изданиях, в том числе в журналах, включенных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации в Перечень ведущих рецензируемых научных журналов и изданий.

Основные результаты диссертационного исследования были представлены автором в публичных докладах на общероссийских и международных научно-практических конференциях: XXIII Международная научная конференция «Цивилизация знаний: российские реалии» (г. Москва, 8-29 апреля 2022 г.), Совместная XXII Международная научно-практическая конференция «Кутафинские чтения» Университета имени О.Е. Кутафина (МГЮА) и XXIII

Международная научно-практическая конференция Юридического факультета Московского государственного университета имени М.В. Ломоносова (г. Москва, 23-25 ноября 2022 г.); Всероссийская ежегодная декабрьская научно-практическая студенческая конференция (г. Москва, 02-14 декабря 2022 г.); X Московский международный юридический форум «Устойчивое развитие России: правовое измерение» (г. Москва, 6-8 апреля 2023 г.).

Соответствие диссертационного исследования паспорту научной специальности. В соответствии с направлениями исследования паспорта научной специальности 5.1.5. Международно-правовые науки Номенклатуры научных специальностей тема диссертации, ее содержание и результаты соответствуют следующим направлениям: 5. Право международных организаций. Правовая природа, статус, компетенция международных межправительственных организаций, международных неправительственных организаций, квазиорганизаций. Нормотворческая деятельность международных организаций. Внутреннее право международных организаций. Международные конференции; 26. Интеграция и международное право. Правовые формы интеграции. Понятие, правовая природа, виды, признаки, компетенция и деятельность международных интеграционных объединений. Право межгосударственных региональных интеграционных объединений. Правовые проблемы евразийской интеграции. Правовой статус Евразийского экономического союза (ЕАЭС) и его органов. Право ЕАЭС. Право Европейского союза (ЕС). Международная правосубъектность и компетенция ЕС; 29. Международно-правовое сотрудничество в научно-технической сфере. Международное право и новые технологии (цифровая экономика, искусственный интеллект, биотехнологии и т.д.). Международное информационное право.

Структура исследования обусловлена его целью и задачами. Работа состоит из введения, трех глав, включающих одиннадцать параграфов, заключения, списка сокращений и условных обозначений, списка используемых источников и литературы.

II. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновываются актуальность темы исследования и степень ее научной разработанности, определены объект, предмет, цель и задачи исследования, методы, а также теоретическая и нормативная основа проведенного исследования, формулируется научная новизна, выдвигаются основные положения, выносимые на защиту, раскрывается теоретическая и практическая значимость выполненной работы, указываются данные об апробации результатов исследования, сведения о соответствии диссертационного исследования паспорту научной специальности, раскрывается структура диссертации.

В **первой главе** «Международно-правовое регулирование в области обеспечения кибербезопасности и Европейский Союз», состоящей из пяти параграфов, закладывается научно-теоретический базис (в том числе понятийный аппарат) исследования.

В **первом параграфе «**Понятие «кибербезопасность» в международном праве и праве Европейского Союза» автором проведен сравнительно-правовой анализ подходов международных организаций и интеграционных объединений, включая ЕС, а также ведущих государств к определению понятия «кибербезопасность», разграничению его с понятием «информационная безопасность».

В ходе исследования автором установлено, что, как и другие международные организации, интеграционные объединения, а также государства на национальном уровне, ЕС осуществляет рассматриваемую деятельность ради обеспечения не только «кибербезопасности», но и «информационной безопасности» в более широком смысле.

Соглашаясь с позицией Международной организации по стандартизации (ИСО) в том, что «информационная безопасность» является родовым понятием по отношению к «кибербезопасности», автор, тем не менее, установил, что сегодня в государствах и на международной арене пока не выработано единого подхода к

разграничению «информационной безопасности» и «кибербезопасности» вплоть до полного отождествления двух понятий в национальных стратегиях по кибербезопасности некоторых государств-членов ЕС.

Сделан вывод, что в настоящее время «кибербезопасность» выступает в качестве полноценной категории права ЕС. Понимание кибербезопасности в современном праве ЕС имеет двойственный характер: состояние защищенности от киберугроз и действия, направленные на достижение подобного состояния. Данный вывод вытекает из системного толкования нормы-дефиниции рассматриваемой категории в Акте о кибербезопасности 2019 г. – «деятельность, необходимая для защиты сетевых и информационных систем, пользователей таких систем и других лиц, пострадавших от киберугроз», во взаимосвязи с положениями других нормативных правовых актов ЕС, которые предусматривают достижение повсеместно в ЕС высокого уровня кибербезопасности (например, Директива (ЕС) 2022/2555 о мерах по обеспечению кибербезопасности).

Во **втором параграфе** «Международно-правовые основы сотрудничества и интеграции государств в области обеспечения кибербезопасности» автор, обращая внимание на проблему сложности и длительности разработки и принятия юридически обязательных международно-правовых норм по вопросу кибербезопасности на универсальном уровне (в частности, в рамках ООН), отмечает, что международное сотрудничество и международная интеграция по вопросу обеспечения кибербезопасности пока более успешно развивается на региональном и двустороннем уровне.

В исследовании выявлено, что среди региональных международных организаций и интеграционных объединений наиболее весомых результатов в разработке единообразных правовых стандартов обеспечения кибербезопасности достиг ЕС с точки зрения 1) количества изданных и готовящихся к принятию источников юридически обязательных норм в этой области, 2) их предмета и содержания, охватывающих меры по обеспечению кибербезопасности субъектов публичной власти на разных уровнях и гражданского общества в разных сферах

общественной жизни, 3) темпов модернизации действующего законодательства о кибербезопасности и его адаптации к новым вызовам и угрозам в киберпространстве.

В **третьем параграфе** «Становление и развитие правового регулирования деятельности Европейского Союза в области обеспечения кибербезопасности» установлено, что в ЕС правовое регулирование обеспечения кибербезопасности происходило поэтапно, и охарактеризовано основное содержание каждого этапа.

Основные направления правового регулирования обеспечения кибербезопасности устанавливаются стратегическими документами ЕС, которые в дальнейшем обретают юридическую силу в нормативных правовых актах вторичного права ЕС – главным образом, посредством, юридически обязательных нормативных правовых актов прямого (регламенты) и непрямого (директивы) действия.

В **четвертом параграфе** «Компетенция Европейского Союза в области обеспечения кибербезопасности после реформы Лиссабонского договора 2007 г.» обосновано, что в первичном праве ЕС специально не закрепляется компетенция по принятию мер, направленных на обеспечение кибербезопасности.

Поскольку сфера кибербезопасности не выделяется в первичном праве ЕС, проблема кибербезопасности в ЕС рассматривается и решается в рамках единого внутреннего рынка, пространства свободы безопасности и правосудия и общей политики безопасности и обороны ЕС. Наибольшее значение для издания законодательства о кибербезопасности ЕС имеет ст. 114 Договора о функционировании ЕС о сближении (гармонизации) правовых норм государств-членов ЕС, затрагивающих создание и функционирование единого внутреннего рынка ЕС. В правотворческой и судебной практике ЕС данная статья получила широкое толкование, не ограничивающее ее предмет только вопросами экономической интеграции.

В **пятом параграфе** «Правовой статус специализированных органов Европейского Союза в области обеспечения кибербезопасности» диссертант,

проведя анализ правового статуса специализированных органов ЕС в области обеспечения кибербезопасности (к числу которых относятся Агентство ЕС по кибербезопасности, Европейский центр компетенций по промышленной, технологической и исследовательской кибербезопасности и Сеть национальных координационных центров), делает вывод, что в ЕС вопросом обеспечения кибербезопасности занимается разветвленная система органов. Центральная роль отводится Агентству ЕС по кибербезопасности.

Среди недостатков организационного механизма ЕС в области обеспечения кибербезопасности автор выделяет недостаточное четкое разграничение ответственности между различными органами, а также большие финансовые расходы на поддержку их функционирования.

На основе проведенного в пятом параграфе анализа и выводов из него автор предлагает учредить в рамках ЕАЭС орган специальной компетенции – «Центр информационной безопасности Евразийского экономического союза», наделив его статусом постоянно действующего органа со следующими функциями и вытекающими из них полномочиями:

- обеспечение сотрудничества между государствами – членами ЕАЭС и органами ЕАЭС по вопросу обеспечения информационной безопасности (в том числе кибербезопасности) для более быстрого совместного реагирования на киберугрозы и кибератаки и надлежащей координации усилий по противодействию им;

- предоставление помощи и экспертных заключений по вопросам информационной безопасности (включая кибербезопасность) для государств-членов ЕАЭС;

- консультирование компетентных органов государств-членов ЕАЭС по вопросу повышения уровня информационной безопасности (включая кибербезопасности) при функционировании таможенного союза и единого экономического пространства ЕАЭС;

- постоянный мониторинг общего состояния информационной безопасности (включая кибербезопасность) в ЕАЭС.

Вторая глава «Правовое регулирование деятельности Европейского Союза по обеспечению кибербезопасности субъектов публичной власти и гражданского общества» включает три параграфа.

В **первом параграфе** «Правовое регулирование обеспечения кибербезопасности органов Европейского Союза» автор, подчеркивая важность вопроса кибербезопасности для обеспечения непрерывности функционирования органов публичной власти, анализирует практический опыт ЕС по обеспечению кибербезопасности органов ЕС.

Автором проанализированы положения Регламента (ЕС) 2023/2841 по кибербезопасности в органах ЕС, а также проекта Регламента, устанавливающего правила информационной безопасности для всех институтов, органов, учреждений и агентств ЕС. Также исследована правоприменительная практика, относящаяся к обеспечению информационной безопасности (включая кибербезопасность) отдельных органов ЕС.

Основываясь на материалах и выводах параграфа, автор предлагает заключить между государствами-членами ЕАЭС международный договор, устанавливающий единые требования информационной безопасности для органов ЕАЭС.

Во **втором параграфе** «Правовое регулирование обеспечения кибербезопасности государств-членов, граждан и юридических лиц Европейского Союза» автором были проанализированы положения Директивы (ЕС) 2016/1148 от 6 июля 2016 г. об обеспечении безопасности сетевых и информационных систем, а также Директивы (ЕС) 2022/2555 о мерах по обеспечению кибербезопасности. Также в данном параграфе исследовано законодательство государств-членов, имплементирующее положения Директивы (ЕС) 2016/1148 от 6 июля 2016 г. об обеспечении безопасности сетевых и информационных систем

На основе положений и выводов параграфа автором предлагается заключить между государствами-членами ЕАЭС международный договор, касающийся установления в государствах-членах единых мер, направленных на обеспечение информационной безопасности (включая кибербезопасность), зафиксировав в нем следующие основные обязательства:

- принять политику по информационной безопасности и периодически обновлять ее с учетом меняющегося ландшафта угроз;

- назначить в каждом государстве-члене национальный орган, ответственный за обеспечение информационной безопасности, в том числе за информирование о нарушениях информационной безопасности;

- создать евразийскую сеть, состоящую из национальных органов, ответственных за обеспечение информационной безопасности;

- определить список критически важных организаций, для которых обязательно принятие мер по обеспечению информационной безопасности, а также распространить на такие организации обязательства по информированию о нарушениях информационной безопасности, возникающих в таких организациях, путем предоставления сведений в национальный компетентный орган.

Аналогичный международный договор или акт Высшего государственного совета, касающийся обеспечения информационной безопасности (включая кибербезопасность), мог бы быть принят в рамках Союзного государства России и Беларуси.

В третьем параграфе «Правовое регулирование обеспечения кибербезопасности сетей, информационных систем и продуктов информационно-коммуникационных технологий в Европейском Союзе» автором обстоятельно исследованы положения Акта о кибербезопасности 2019 г., который заложил правовые основы для разработки и принятия в ЕС схем сертификации информационных систем и продуктов информационно-коммуникационных технологий.

Кроме этого, автором проведен анализ проекта Регламента о горизонтальных требованиях кибербезопасности для продуктов с цифровыми элементами (более известный как Акт о кибер устойчивости), положения которого установят обязанность производителей продуктов с цифровыми элементами учитывать кибербезопасность при их проектировании, разработке и производстве, а также обязанность поддерживать кибербезопасность таких продуктов на протяжении всего жизненного цикла.

Основываясь на проведенном анализе, автором рекомендовано заключить между государствами-членами ЕАЭС международный договор, устанавливающий единую систему сертификации информационной безопасности для продуктов и услуг информационно-коммуникационных технологий (ИКТ), размещаемых на внутреннем рынке ЕАЭС, а также накладывающий обязательства для поставщиков товаров, которые имеют в своем составе ИКТ, соблюдать требования по обеспечению информационной безопасности своих продуктов на протяжении всего их жизненного цикла.

Третья глава «Правовое регулирование деятельности Европейского Союза по обеспечению кибербезопасности в отдельных сферах общественной жизни» включает три параграфа.

В **первом параграфе** «Правовое регулирование обеспечения кибербезопасности в экономической сфере» рассматривается правовое регулирование обеспечения кибербезопасности в экономической сфере. Автор подчеркивает, что отдельные секторы экономики (услуги электросвязи, транспорт, финансы и другие) сталкиваются со специфическими проблемами кибербезопасности и, следовательно, нуждаются в разработке собственных правовых подходов к вопросу обеспечения кибербезопасности. Это обстоятельство приводит к развитию правового регулирования ЕС, посредством которого устанавливаются меры кибербезопасности для отдельных секторов экономики.

Установлено, что деятельность финансовых учреждений на территории ЕС подчиняется отраслевым нормативным правовым актам, которые содержат обязательства по кибербезопасности. Данную систему должен изменить Регламент (ЕС) 2022/2554 от 14 декабря 2022 г. о цифровой операционной устойчивости для финансового сектора, положения которого вступили в силу с 2024 г. Данный Регламент устанавливает единые требования в отношении безопасности сетевых и информационных систем, поддерживающих бизнес-процессы финансовых учреждений. Для услуг электросвязи также запланирована гармонизация обязательств, налагаемых на их поставщиков. Однако в энергетическом секторе тенденции по установлению единообразных требований кибербезопасности автором не выявлено. В аспекте правового регулирования обеспечения кибербезопасности на транспорте (морской, воздушный, водный и наземный транспорт, включая железнодорожный) сделан вывод о том, что единообразные меры кибербезопасности юридически закрепляются путем издания делегированных актов Европейской комиссией.

Во **втором параграфе** «Правовое регулирование обеспечения кибербезопасности в социальной сфере» диссертантом рассмотрены правовые нормы, применяемые в Европейском Союзе для обеспечения кибербезопасности в сфере здравоохранения. Сделан вывод, что в нормативных правовых актах содержатся требования безопасности, которые тесно связанны с вопросом обеспечения кибербезопасности (но специально ему не посвящаются). В частности, устанавливаются требования, направленные на безопасность медицинских устройств, которые обязывают производителей разрабатывать и производить свою продукцию в соответствии с современным уровнем развития техники с учетом принципов управления рисками, включая риски для кибербезопасности, а также устанавливают минимальные требования к мерам кибербезопасности, включая защиту от несанкционированного доступа.

В **третьем параграфе** «Правовое регулирование обеспечения кибербезопасности в духовно-культурной сфере» автором проанализирован

подход ЕС в отношении решения проблемы недостатка квалифицированных кадров в области кибербезопасности, а также распространения среди населения цифровой грамотности, в том числе базовых знаний о кибербезопасности. Установлено, что для решения проблемы дефицита кадров в области обеспечения кибербезопасности в Европейском Союзе предпринимаются различные меры, к которым, в частности, относится инициатива создания нового европейского образовательного учреждения «Академии навыков кибербезопасности».

В **заключении** подводятся итоги исследования, обобщаются основные выводы и сделанные в работе практические предложения, представляющие интерес для интеграционных объединений, в которых принимает участие Российская Федерация, прежде всего для Евразийского экономического союза и Союзного государства России и Беларуси.

СПИСОК РАБОТ,
ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации:

1. Гирис В.А. Понятие «кибербезопасность» в праве Европейского Союза// Юридическая наука. №4. 2022. с. 115-120 (0.75 п.л.)
2. Гирис В.А. Становление и развитие правового регулирования деятельности Европейского Союза в области обеспечения кибербезопасности // Евразийский юридический журнал. №6. 2022. с.64-68. (0,83 п.л.)
3. Гирис В.А. — Правовой статус органов и учреждений Европейского Союза в области обеспечения кибербезопасности // Международное право и международные организации / International Law and International Organizations. – 2023. – № 1. DOI: 10.7256/2454-0633.2023.1.39986 EDN:CNSRATURL: https://nbpublish.com/library_read_article.php?id=39986 (1 п.л.)

Публикации в иных научных изданиях:

4. Гирис В.А. Международно-правовые основы сотрудничества и интеграции государств в области обеспечения кибербезопасности // Всероссийская ежегодная декабрьская научно-практическая студенческая конференция: (г. Москва, 02-14 декабря 2022 г.) - М.: АНО ВО «Российский новый университет», 2023. С. 312-318. (0.40 п.л.)