Международное право и международные организации / International Law and International Organizations
Правильная ссылка на статью:
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: CNSRAT URL: https://nbpublish.com/library_read_article.php?id=39986

Правовой статус органов и учреждений Европейского Союза в области обеспечения кибербезопасности

Гирис Валерия Алексеевна

ORCID: 0000-0000-0000-0000

аспирант, кафедра интеграционного и европейского права, Московский государственный юридический университет имени О.Е. Кутафина

123000, Россия, г. Москва, ул. Садовая-Кудринская, 9

valeri_ka@list.ru

Статья из рубрики " Интеграционное право и наднациональные объединения"

DOI:

10.7256/2454-0633.2023.1.39986

EDN:

CNSRAT

Дата направления статьи в редакцию:

14-03-2023

Дата публикации:

21-03-2023

Аннотация: Актуальность темы исследования обуславливается тем, что в решении проблем кибербезопасности в государствах задействованы различные органы, каждый из которых имеет свои цели и задачи, при этом их успешное решение всецело зависит от эффективного сотрудничества между ними. Существующие ресурсы и опыт, имеющиеся в государствах-членах ЕС и соответствующих институтах, органах и агентствах ЕС, обеспечивают прочную основу для коллективного реагирования на угрозы кибербезопасности. Благодаря чему в ЕС была создана система органов по управлению рисками в области кибербезопасности. На данный момент в России не были разработаны комплексные исследования, специально посвященные анализу деятельности органов и учреждений Европейского Союза в области обеспечения кибербезопасности. Целью настоящей статьи является исследование деятельности ключевых органов ЕС в области кибербезопасности. Для достижения указанной цели автором были использованы системный подход, формально-юридический метод, сравнительно-правовой метод, исторический метод, с их помощью была проанализирована деятельность основных

органов ЕС в области кибербезопасности. Автор приходит к выводу, что сотрудничество и обмен информацией являются важнейшими элементами в решении вопросов кибербезопасности. При этом для достижения согласованности действий между органами, занимающимися вопросами кибербезопасности, в ЕС предпринимаются меры, направленные на укрепление их совместной работы. Кроме этого, делается вывод о том, что ЕС как региональная интеграционная организация, где государства члены действуют на основе принципа взаимного доверия, представляет собой надежную платформу для решения проблем кибербезопасности.

Ключевые слова:

право ЕС, кибербезопасность, киберугрозы, киберустойчивость, киберзащита, киберпространство, кибер атака, информационная безопасность, киберпреступность, киберинцидент

Потребность в усилении безопасности современного общества от резко увеличивающегося числа киберугроз стала катализатором для развития нормативной правовой базы, направленной на повышение уровня киберустойчивости современных государств.

Сегодня требования к кибербезопасности, предъявляемые в одном государстве, могут значительно отличаться от требований, предъявляемых в другом. Это обстоятельство стало одной из причин, по которой вопрос обеспечения кибербезопасности приобрел большое международное значение.

Однако развитие международного права по данному вопросу осложнено. На международном уровне до сих пор отсутствуют универсальные соглашения по вопросу обеспечения кибербезопасности, равно как и отсутствуют совместные механизмы для реагирования на киберугрозы. Это обстоятельство делает уязвимым государства к возникающим киберугрозам, поскольку в киберпространстве государства находятся в состоянии взаимозависимости из-за децентрализованного характера угроз.

Европейский Союз (далее – ЕС, Союз) предпринял попытку создать единый подход к кибербезопасности среди государств-членов ЕС и обеспечить его реализацию с помощью деятельности системы органов ЕС.

Профессор С. Ю. Кашкин отмечает, что ЕС располагает широким организационным механизмом, субъекты которого все более необычным образом переплетаются между собой [1, с.70]. В этой связи, хотелось бы отметить, что с развитием области кибербербезопасности в ЕС наметилась тенденция к усложнению институциональной системы.

Далее мы остановимся на более детальном рассмотрении правового статуса и деятельности органов ЕС в области кибербезопасности.

Европейская комиссия ставит своей целью укрепить сотрудничество государств-членов по вопросу повышения уровня кибербезопасности. Достижение указанной цели Европейская комиссия осуществляет совместно с другими институтами, органами и агентствами ЕС.

Ключевое место среди органов ЕС в области кибербезопасности занимает Агентство ЕС

по кибербезопасности, ранее называвшееся Европейское агентство по сетевой и информационной безопасности (далее – Агентство). Следует отметить, что в соответствии с законодательством ЕС, агентства являются отдельными органами, отличными от институтов ЕС, и отдельными юридическими лицами, которые учреждаются для выполнения конкретных задач.

Согласно п. 2 ст. 1 Регламента №460/2004 о создании Европейского агентства по сетевой и информационной безопасности, роль Агентства заключается в «оказании помощи Европейской комиссии и государствам-членам ЕС, а также, поддержки сотрудничества с предпринимателями, чтобы помочь им выполнить требования, предъявляемые к сетевой и информационной безопасности, обеспечивая тем самым бесперебойное функционирование внутреннего рынка, включая требования, изложенные в настоящем и будущем законодательстве Сообщества» [2].

Исходя из этого, работа Агентства сведена как к независимому консультационному органу государств-членов ЕС и европейских предпринимателей, обеспечивающему доступ к информации и ресурсам, необходимым для функционирования в киберпространстве.

Первоначально работа Агентства в основном заключалась в сборе информации обо всех возникающих угрозах в киберпространстве, предоставлении необязательных консультаций государствам-членам ЕС и иным заинтересованным лицам, а также в создании платформы для обмена опытом.

Правовой основной, принятия Регламента №460/2004, учредившего Агентство, стала ст. 95 Договора об учреждении Европейского Сообщества, которая позволяет принимать органам ЕС меры, гармонизирующие национальное законодательство государств-членов ЕС.

Тем не менее со стороны Великобритании была проявлена озабоченность по поводу правомерности использования статьи 95 Договора об учреждении Европейского Сообщества в качестве правовой основы для создания Агентства, поскольку «функции Агентства ограничиваются развитием экспертизы и предоставлением консультаций широкому кругу потенциальных получателей, и единственная возможная связь, которая может существовать между задачами, которые оно выполняет, и гармонизацией права, - это связь, вытекающая из того факта, что Агентство помогает Европейской комиссии. Однако эта роль, которая представляется как техническая исследовательская функция, слишком далека от законодательства Сообщества, направленного на гармонизацию национального законодательства»[3].

Великобритания в поданном в Суд ЕС заявлении об отмене Регламента №460/2004 заявила, что предоставление необязательных консультаций не может быть равносильно «сближению положений, установленных законодательными актами, регламентами или административными актами в государствах-членах» по смыслу ст. 95 Договора об учреждении Европейского Сообщества. Более того распространение таких рекомендаций может на практике увеличить различия, которые существуют между национальными законами»[3].

В своем Решении Суд ЕС отклонил заявление Великобритании и обосновал правомерность принятия Европейским парламентом Регламента №460/2004 в соответствии со ст. 95 Договора об учреждении Европейского Сообщества, постановив следующее:

- задачи, возложенные на Агентство в соответствии со ст. 3 Регламента №460/2004 тесно связаны с целями, преследуемыми Директивами, регулирующими услуги электронных коммуникаций и связанных с ними средств и услуг, и конкретными Директивами в области сетевой и информационной безопасности.

-Европейский парламент был вправе считать, что мнение независимого органа, предоставляющего технические консультации по просьбе Европейской комиссии и государств-членов ЕС, может облегчить перенос Директив, регулирующих услуги электронных коммуникаций в законы государств-членов и реализацию этих Директив на национальном уровне.

-Регламент №460/2004 не представляет собой изолированную меру, но входит в соответствующий законодательный механизм, ограниченный Директивой [4] и специальными Директивами, и направлен на завершение внутреннего рынка в области электронных коммуникаций.

Таким образом, вышеуказанное решение позволило ЕС не только предпринимать меры, способствующие гармонизации, но и учреждать органы, способные облегчить сближение политик государств-членов ЕС в области кибербезопасности. Суд ЕС постановил, что Агентство является надлежащим средством предотвращения возникновения различий, которые могут создать препятствия для бесперебойного функционирования внутреннего рынка в данной области.

Спустя год функционирования Агентства Европейская комиссия провела оценку его деятельности, которое было заранее предусмотрено ст. 25 Регламента №460/2004 и было обязательно для принятия решения о дальнейшем продлении полномочий данной организации после окончания пятилетнего мандата.

Оценка деятельности Агентства была изложена в соответствующем сообщении Европейской комиссии [5], в котором последняя сделала положительное заключение о продлении мандата Агентства, а также указала на ряд проблем, связанных с деятельностью Агентства, и пути их решения.

Основные проблемы, обозначенные Европейской комиссией, можно определить как организационные, в них входят недостатки в структуре Агентства, удаленность местоположения Агентства (штаб-квартира Агентства располагалась в Ираклионе, Греция) и проблема стратегической роли Агентства, которая на тот момент была сосредоточена в основном на подготовке отчетов о ходе реализации своей деятельности. В своем сообщении Европейская комиссия предложила рекомендации относительно структуры управления Агентства, а также о пересмотре ст. 2 и ст. 3 Регламента №460/2004 для того, чтобы установить основанные на конечных результатах ключевые цели Агентства.

Учитывая положительную оценку деятельности Агентства, выданную Европейской комиссией в 2008 г. Европейский парламент и Совет приняли еще один Регламент № 1007/2008 [6], продлевающий мандат Агентства до марта 2012г..

В Резолюции Совета ЕС от 18 декабря 2009 г.[7] признается роль и потенциал Агентства и необходимость «дальнейшего развития Агентства в эффективный орган». В связи с этим Европейской комиссией был разработан проект нового Регламента об Агентстве [8], предлагающий расширение его функций и продление мандата. В качестве правовой основы данной организации предложено использовать ст. 114 Договора о

функционировании ЕС, которая почти идентична ст. 95 Договора об учреждении Европейских Сообществ.

Стратегия кибербезопасности для Европейского союза 2013 года - Открытое, безопасное и надежное [9] определила Агентство как необходимого субъекта, осуществляющего надзор за управлением кибербезопасностью, которая нуждалась только в модернизированном мандате с дополнительными полномочиями. В связи с этим был принят новый Регламент об Агентстве, который усиливал мандат данной организации. Ранее Регламент № 580/2011 [10] продлил срок действия мандата Агентства до 13 сентября 2013 г. Новый мандат был утвержден Регламентом 526/2013 16 апреля 2013 г. [11] и был установлен на семь лет.

Как уже было сказано, новый Регламент об Агентстве предусматривал усиление его роли. В первую очередь новый Регламент предоставил Агентству полномочия на поддержку создания и функционирования полномасштабной Группы реагирования на компьютерные чрезвычайные ситуации ЕС (далее – CERT-EU) для противодействия кибератакам на уровне ЕС.

Для повышения эффективности работы новый Регламент учредил новый дополнительный филиал Агентства с оперативным персоналом в Афинах. Изменения коснулись и структуры управления, в которую был введен исполнительный совет, позволяющий правлению Агентства сосредоточиться на вопросах стратегической важности и тем самым повысить эффективность Агентства. Исполнительный директор, согласно Регламенту, назначается с одобрения Европейского парламента.

Директивой № 2016/1148 [12] Агентству была отведена роль секретариата Групп реагирования на инциденты, связанные с компьютерной безопасностью (далее- CSIRTs), которая была создана для содействия быстрому и эффективному оперативному сотрудничеству между государствами-членами ЕС в отношении конкретных инцидентов в области кибербезопасности и обмену информацией о рисках.

Таким образом, с принятием Директивы №2016/1148 фактически произошло усиление роли Агентства, которое в дальнейшем было признано Европейской комиссией в ходе проведения оценки его деятельности и закреплено в последующем принятом Регламенте №2019/881 [13], который окончательно отвел Агентству центральную роль в обеспечении кибербезопасности в ЕС.

Одним из аспектов кибербезопасности выступает киберпреступность. С целью минимизации рисков от киберпреступности в рамках ЕС были приняты нормативные правовые акты, направленные на борьбу с киберпреступностью. Кроме этого, значимую роль в решении вопросов киберпреступности осуществляют специализированные органы ЕС, такие как Агентство ЕС по сотрудничеству между полицейскими органами (далее – Европол) и Агентство ЕС по сотрудничеству в области уголовной юстиции (далее – Евроюст).

Евроюст был учрежден на основании решения Совета ЕС [14] в качестве агентства ЕС с целью улучшения координации и сотрудничества между компетентными судебными органами государств-членов особенно в отношении серьезной организованной преступности. Упомянутое решение было заменено Регламентом 2018/1727 [15], который в свою очередь направлен на то, чтобы укрепить роль Евроюста в отправлении правосудия через границы для более безопасной Европы. В Евроюсте создана Группа по

борьбе с финансовыми и экономическими преступлениями (далее – Группа) в полномочия которой входит борьба с киберпреступностью.

Дополнительно к работе Группы в 2016 г. на основании Заключения Совета ЕС от 9 июня 2016г. [16] была создана Европейская судебная сеть по борьбе с киберпреступностью при Евроюсте для поддержки судебных органов, занимающихся киберпреступностью. Пленарные заседания Европейской судебной сети по борьбе с киберпреступностью проводятся два раза в год при поддержке Евроюста и при совместном участии представителей из Европола, Европейской комиссии, что, в свою очередь, способствует обмену мнениями между заинтересованными сторонами об общих проблемах киберпреступности.

Европол это правоохранительное учреждение, которое было учреждено Решением Совета от 6 апреля 2009 г. о создании Европейского полицейского ведомства. Согласно которому, оно предназначено для оказания практического содействия и информационной поддержки на европейском уровне мероприятиям полицейских органов государств в области борьбы: с транснациональной организованной преступностью, с международным терроризмом, а также с другими тяжкими формами преступности международного характера: торговлей наркотиками, отмыванием денег и т.д. [17]. Современной правовой основой деятельности Европола является Регламент (ЕС) 2016/794 Европейского парламента и Совета от 11 мая 2016 г. об Агентстве ЕС по сотрудничеству между правоохранительными органами (Европол) и заменяющий и отменяющий Решения Совета 2009/371/ПВД, 2009/934/ПВД, 2009 г. /935/ПВД, 2009/936/ПВД и 2009/968/ПВД.

Изначально решение вопросов, связанных с киберпреступностью, не входило в область задач Европола. Действительно, в одном из исследований Э. Ильбиз и К. Каунерт подчеркивают, что деятельность Европола, направленная на борьбу с киберпреступностью, до второй половины 2010х. г. не являлась его приоритетной задачей [18, с.3].

Тем не менее в принятой Европейской комиссией 22 ноября 2010 г. Стратегии внутренней безопасности ЕС [19] отмечается, что Центр по борьбе с высокотехнологичными преступлениями Европола играет важную координирующую роль для правоохранительных органов в борьбе с киберпреступностью.

В качестве одного из дальнейших приоритетных действий Стратегии внутренней безопасности ЕС определил учреждение к 2013 г. в рамках Европола Европейского центра по борьбе с киберпреступностью.

Более подробное предложение с описанием основных функций Европейского центра по борьбе с киберпреступностью было изложено в Сообщении [20] Европейской комиссии. Официальный запуск Европейского центра по борьбе с киберпреступностью был осуществлен Европолом в январе 2013г. в качестве его подразделения.

Важно отметить, что правовой основой для создания данного подразделения послужил Европол. На наш взгляд, создание данного подразделения в рамках организационной структуры Европола послужило прочной правовой основой для дальнейшего его развития как значимого субъекта в борьбе с киберпреступностью, поскольку позволило ему использовать уже имеющийся и накопленный арсенал возможностей Европола для проведения расследований и сотрудничества в расследовании киберпреступлений.

Таким образом, в ЕС была создана простая и экономичная организационная структура для того, чтобы обеспечить эффективное выполнение задач, поставленных перед ней [21].

Учитывая количество органов, задействованных в предотвращении киберпреступности, важно обратить внимание на то, что в ЕС особое внимание придается сотрудничеству между ними, обеспечению синергии и взаимодополняемости их мандатов и компетенций.

В этой связи для обсуждения и определения приоритетов ключевых проблем и дальнейших действий в борьбе с киберпреступностью в ЕС создаются площадки для взаимодействия. К числу таких относится Целевая группа ЕС по борьбе с киберпреступностью. Она является форумом для руководителей органов ЕС по борьбе с киберпреступностью и государств-членов, который собирается два раза в год в Европоле. Кроме этого, Европейским центром по борьбе с киберпреступностью Европола совместно с Целевой группой ЕС по борьбе с киберпреступностью была создана Совместная целевая группа по борьбе с киберпреступностью, которая состоит из сотрудников по кибербезопасности из государств-членов, партнеров по правоохранительным органам, не входящих в ЕС, и сотрудников Европейского центра по борьбе с киберпреступностью Европола.

Европейские исследователи, проведя анализ деятельности различных структур, занимающихся киберпреступностью как в ЕС, так и в государствах-членах приходят к мнению, что существует приемлемость создания совершенно новых организационных структур, особенно в текущем экономическом климате [22, с.4].

В итоге хотелось бы подчеркнуть, что в результате проведенного анализа можно сделать вывод, что расширение организационного механизма ЕС, основным видом деятельности которого является борьба с преступностью, свидетельствует о растущем характере угроз, связанных с киберпреступностью. В условиях, когда деятельность специализированного органа не может справиться с решением вновь возникших видов преступлений, требуется создание эффективных подраздеделений, деятельность которых будет сосредоточена только на борьбе с отдельным видами преступлений (киберпреступлений).

Продолжая мысль о растущем характер угроз, которые влекут за собой информационно-коммуникационные технологии, Р. Вессел и Ю. Мядзвецкая отмечают, что растущее число кибератак и их разрушительный характер стали причиной для создания в ЕС ответных мер, ориентированных на внешнюю политику[23, с.414].

Согласно Оперативному руководству по международному сотрудничеству ЕС в области наращивания киберпотенциала [24], опубликованному Европейской комиссией, необходимыми мерами в области кибербезопасности являются меры по обеспечению дипломатических обязательств, направленных на поддержание открытого, свободного и безопасного киберпространства, и разработка стратегий киберзащиты для защиты военных сетей и активов.

В реализации вышеуказанных мер активную деятельность осуществляют Европейская служба внешнеполитической деятельности, Европейское оборонное агентство, Постоянное структурированное сотрудничество.

Европейская служба внешнеполитической деятельности была учреждена Решением Совета ЕС 2010/427/ЕС от 26 июля 2010 г.[25] в качестве автономного органа ЕС, который находится под руководством Высокого представителя и оказывает ему

поддержку в выполнении его мандата. Европейская служба внешнеполитической деятельности оказывает поддержку государствам-членам в использовании дипломатических мер, в частности, что касается общественной коммуникации, поддержки общей ситуационной осведомленности и взаимодействия с третьими странами в случае кризиса.

В рамках Европейской службы внешнеполитической деятельности в вопросе обеспечения кибербезопасности задействованы Центр анализа разведданных ЕС , Группа экспертов высокого уровня и Военный штаб ЕС.

Анализируя роль Европейской службы внешнеполитической деятельности в сфере кибербезопасности, Д. Дуйч приходит к выводу, что основная роль данной службы является вспомогательной и заключается в обеспечении большей согласованности и координации в сфере кибербезопасности, особенно в области киберзащиты[26, с.101].

Европейское оборонное агентство учреждено Решение Совета 2004/551/CFSP от 12 июля 2004 г. о создании Европейского оборонного агентства [27] и является агентством ЕС, целью которого является развитие оборонного потенциала в области управления кризисными ситуациями, а также содействие и укрепление европейского сотрудничества в области вооружений. Европейское оборонное агентство было создано на основании п. 3 ст. 42 Договора о ЕС. Его задачи подробно изложены в ст. 45 Договора о ЕС.

В области кибербезопасности Европейское оборонное агентство является ответственным за координацию киберзащитных возможностей. Под эгидой Европейского оборонного агентства функционирует несколько программ, которые также фокусируются на развитии сотрудничества между государствами-членами по вопросам кибербезопасности. Из их числа можно выделить программу Развертываемый потенциал сбора и оценки кибердоказательств, которая направлена на разработку технической демонстрации возможностей цифровой криминалистики для военных.

Также в рамках проектной группы Европейского оборонного агентства по киберзащите был запущен проект Федерация киберполигонов, целью которого является объединение и совместное использование существующих возможностей киберполигонов между государствами-членами.

В качестве одной из последних программ Европейского оборонного агентства следует отметить оперативную сеть Военной компьютерной группы реагирования на чрезвычайные ситуации – MICNET. Запуск этой программы был инициирован Политикой ЕС в области киберзащиты[28]. MICNET должна служить основой и инфраструктурой для обмена информацией между различными уровнями сообщества киберзащиты и внешними заинтересованными сторонами.

Кроме этого, вопросы, связанные с областью кибербезопасности, включены в Постоянное структурированное сотрудничество, запущенное в 2017 г. Решением Совета Е С [28]. Его правовой основой является ст. 42 (6) Договора о ЕС, которая предусматривает, что те государства-члены, военный потенциал которых соответствует более высоким критериям и которые взяли на себя более обязательные обязательства друг перед другом в этой области с целью выполнения наиболее сложных задач, должны установить постоянное структурированное сотрудничество в рамках Союза.

Для области кибербезопасности Постоянное структурированное сотрудничество осуществляет немаловажную роль. В качестве одного из первых проектов, которое было

инициировано в рамках Постоянного структурированного сотрудничества, стал проект по организации Групп быстрого кибернетического реагирования. Специалисты в области кибербезопасности, объединенные в рамках такой группы, могут оказывать помощь государствам-членам, институтам ЕС, миссиям и операциям ЕС, а также странам-партнерам, внося свой вклад в общий потенциал ЕС по предотвращению, сдерживанию и реагированию на киберугрозы.

К.К. Ренда справедливо указывает, что отсутствие у ЕС централизованного киберкомандования подрывает его возможности киберзащиты и ограничивает его амбиции стать более влиятельным в этой новой области политики[29, с.482].

Тот факт, что для военных операций и миссий ЕС в киберпространстве или через него также требуется создание соответствующей организационной структуры, которая могла бы адекватно отражать требования киберзащиты, было подтверждено в Стратегии ЕС в отношении киберпространства как области операций [30]. В дальнейшем опубликованная Политика ЕС в области киберзащиты[28] заложила основу для создания Конференции киберкомандующих ЕС. Планируется, что она будет собираться при секретариате Европейского оборонного агентства и при участии Военного штаба ЕС не реже двух раз в год для обсуждения оперативных вопросов и других актуальных тем.

Таким образом, подход ЕС к обеспечению кибербезопасности основывается не только на обеспечении внутренней безопасности посредством правоохранительных органов, таких как Европол и Евроюст. В ЕС особое внимание уделяется внешним аспектам безопасности, международному участию ЕС в решении данных вопросов, включая реагирование на вредоносные действия. В этой связи в рамках общей политики безопасности и обороны с помощью деятельности Европейского оборонного агентства, Европейской службы внешнеполитической деятельности, Постоянного структурированного сотрудничества ведется работа по укреплению общего уровня кибербезопасности государств-членов и ЕС.

Безусловно, достижение высокого уровня кибербезопасности невозможно без развития и формирования интеллектуального потенциала. В связи с этим в организационную структуру ЕС Регламентом №2021/887 Европейского парламента и Совета от 20 мая 2021 [31] были включены еще два структурных элемента : Европейский центр компетенции по промышленной, технологической и исследовательской кибербезопасности (далее - Центр компетенции) и Сеть национальных координационных центров (далее - Сеть).

Согласно ст. 3 Регламента, роль Центра компетенции и Сети состоит в том, чтобы помочь ЕС в развитии технологического, академического общественного, исследовательского и промышленного потенциала кибербезопасности.

Из представленного следует, что в ЕС обеспечением кибербезопасности занимается разветвленная система органов. В качестве основных органов в области кибербезопасности можно выделить Агентство ЕС по кибербезопасности, Европейское оборонное агентство, Европол и Евроюст.

Учитывая, что сотрудничество и обмен информацией в решении проблем кибербезопасности являются важнейшими элементами для достижения высокого уровня защиты от киберугроз, необходимо создание согласованного механизма взаимодействия и сотрудничества между органами, задействованными в области кибербезопасности.

Характеризуя организационный механизм ЕС, профессор А.Я. Капустин также указывает,

что поддержание постоянного диалога и сотрудничества между институтами ЕС является существенной характеристикой взаимоотношений между институтами[32, с.232].

Так, с целью установления сотрудничества между Европолом и Агентством ЕС по кибербезопасности и оказания поддержки государствам-членам ЕС и его учреждениям в предотвращении и борьбе с киберпреступностью в 2014 г. было подписано Соглашение о стратегическом партнерстве между Агентством ЕС по кибербезопасности и Европолом [31], которое также закладывает основу для взаимодействия и взаимопомощи между данными организациями.

Тем не менее в правовом плане отправной точкой для установления сотрудничества между органами, занимающимися кибербезопасностью, послужила статья ст. 7 Регламента №2019/881 [13]. В указанном Регламенте в качестве обязательства определено, что Агентство должно сотрудничать на оперативном уровне и налаживать взаимодействие с институтами, органами, учреждениями и агентствами Союза, включая CERT-EU, органами, занимающимися киберпреступностью, и органами, занимающимися защитой конфиденциальности и персональных данных.

Официально соглашение о сотрудничестве между Агентством и CERT-EU было установлено после подписания в 2021г. Меморандума о взаимопонимании [33], в котором определены области сотрудничества (наращивание потенциала, оперативное сотрудничество, а также знания и информация) и устанавливает примерное распределение ролей между ними: CERT-EU будет играть ведущую роль в оказании помощи институтам, органам и учреждениям ЕС, а Агентство будет вносить свой вклад в объеме и пределах, определенных его мандатом, и наоборот.

Кроме того, для улучшения сотрудничества между Европейским оборонным агентством, Агентством ЕС по кибербезопасности, Европейским центром по борьбе с киберпреступностью и CERT-EU был также подписан Меморандум о взаимопонимании [34]. В Докладе [35] Европейской комиссии определено, что данный Меморандум укрепил сотрудничество и синергию между этими организациями в соответствии с их мандатами и способствовал дальнейшему развитию предоставления экспертных знаний, оперативной и технической поддержки ЕС и государствам-членам в области кибербезопасности.

В июне 2021 г. Европейская комиссия в своей Рекомендации [36] объявила о создании Совместного кибер-подразделения. Ранее предложение о его создании было изложено в политических руководящих принципах [37] председателя Европейской комиссии Урсулы фон дер Ляйен. Данная инициатива является важным шагом на пути к завершению европейской системы управления рисками в области кибербезопасности. Она направлена на обеспечение координации усилий в ЕС по предотвращению, обнаружению, сдерживанию, смягчению последствий и реагированию на крупномасштабные киберинциденты и кризисы.

Объединенное киберподразделение будет выступать в качестве платформы для обеспечения скоординированного реагирования ЕС на крупномасштабные киберинциденты и кризисы, а также для оказания помощи в восстановлении после этих атак.

Объединенное киберподразделение обеспечивает виртуальную и физическую платформу и не требует создания дополнительного автономного органа. Его создание не должно влиять на компетенцию и полномочия национальных органов по кибербезопасности и

соответствующих структур Союза. Оно объединяет все сообщества по кибербезопасности, то есть гражданское население, правоохранительные органы, дипломатию и оборону.

Участники платформы должны играть либо оперативную, либо вспомогательную роль. Оперативные участники должны включать Агентство по кибербезопасности, Европол, Группу реагирования на компьютерные чрезвычайные ситуации для институтов, органов и агентств ЕС, Европейскую комиссию, Европейскую службу внешних действий, сеть CSIRTs и Европейская сеть организации по связям с киберкризисами[1](далее - EU-CyCLONe). Вспомогательные участники должны включать Европейское оборонное агентство, председателя Горизонтальной рабочей группы Совета по киберпространству и одного представителя из проектов по кибербезопасности Постоянного структурированного сотрудничества.

Следует подчеркнуть, что в настоящий момент ЕС находится на пути к завершению европейской системы управления рисками в области кибербезопасности.

Результаты работы Агентства ЕС по кибербезопасности демонстрируют успешный опыт в объединении заинтересованных субъектов, деятельность которых направлена на обеспечение киберезопасности. Принятые нормативные правовые акты в ЕС, усиливающие мандат Агентства по кибербезопасности ЕС, а также акты, регламентирующие деятельность в области кибербербезопасности иных рассмотренных органов, подчеркивают эту необходимость.

Таким образом, подход ЕС к достижению высокого уровня кибербезопасности заключается в создании оптимальных условий для усиления дальнейшей координации и сотрудничества между соответствующими институтами, органами и агентствами ЕС. С целью оказания взаимной помощи киберсообществам, ответственным за кибербезопасность, за борьбу с киберпреступностью, за проведение кибердипломатии, за киберзащиту было инициировано создание Совместного кибер подразделения.

Завершая, следует отметить, что ЕС как региональная интеграционная организация, где государства-члены действуют на основе принципа взаимного доверия, представляет собой надежную платформу для решения проблем кибербезопасности. Это обстоятельство демонстрирует необходимость в дальнейшем укреплении сотрудничества между Российской Федерацией и ее партнерами на региональном уровне для достижения высокого общего уровня кибербезопасности.

[1]С принятием в декабре 2022г. Директивы 2022/2555 официально была создана Европейская сеть организации по связям с киберкризисами (далее - EU-CyCLONe) для поддержки скоординированного управления инцидентами кибербезопасности в масштабах всего ЕС, а также для обеспечения регулярного обмена информацией между государствами членами и институтами, органами, офисами и агенствами ЕС.

Библиография

1. Кашкин С.Ю. Лиссабонский договор-новый этап развития права Европейского Союза // Государство и право. 2008. №9. С.59-66.
2. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency // Official Journal of the European Union. 13.3.2004. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004R0460 (дата обращения 20.02.2023 г.).

3. Judgment of the Court United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union. Regulation (EC) No 460/2004-European Network and Information Security Agency-Choice of legal basis. CaseC-217/04. 2 May 2006 C.10 [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62004CJ0217&from=EN (дата обращения 20.02.2023 г.).
4. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) // Official Journal. 24.04.2002. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0021 (дата обращения 20.02.2023 г.).
5. Communication from the Commission to the European Parliament and the Council On the evaluation of the European Network and Information Security Agency (ENISA) // Brussels. 1.6.2007. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52007DC0285 (дата обращения 20.02.2023 г.).
6. Regulation (EC) no 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration // Official Journal of the European Union. 31.10.2008. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R1007&from=EN (дата обращения 20.02.2023 г.).
7. Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security 2009/C 321/01 // Official Journal of the European Union. 29.12.2009. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009G1229%2801%29 (дата обращения 20.02.2023 г.).
8. Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) // Brussels. 30.9.2010. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0521&from=EN (дата обращения 20.02.2023 г.).
9. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace // Brussels. 7.2.2013. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN (дата обращения 20.02.2023 г.).
10. Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration Text with EEA relevance // Official Journal of the European Union. 24.6.2011. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R0580&from=EN (дата обращения 20.02.2023 г.).
11. Regulation (EU) No 526/2013 of the European Parliament and the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 // Official Journal of the European Union. 18.6.2013. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013R0526(дата обращения

20.02.2023 г.).

12. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // Official Journal of the European Union. 19.07.2016. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (дата обращения 20.02.2023 г.).
13. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) // Official Journal of the European Union.07.06.2019. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG (дата обращения 20.02.2023 г.).
14. Decision 2002/187/JHA — setting up Eurojust with a view to reinforcing the fight against serious crime // Official Journal of the European Communities. 6.3.2002. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002D0187 (дата обращения 20.02.2023 г.).
15. Regulation (EU) 2018/1727 of the European parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA/ // Official Journal of the European Union. 21.11.2018. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1727&from=BG (дата обращения 20.02.2023 г.).
16. Conclusions of the Council of the European Union on the European Judicial Cybercrime Network-Council conclusions // Brussels. 9 June 2016. [Электронный ресурс] – Режим доступа: https://www.consilium.europa.eu/media/24301/network-en.pdf (дата обращения 20.02.2023 г.).
17. Четвериков А.О. Решение Совета от 6 апреля 2009 г. о создании Европейского полицейского ведомства (Европол) [Электронный ресурс] – Режим доступа: https://eulaw.ru/translation/reshenie-o-sozdanii-evropola/ (дата обращения 20.02.2023 г.).
18. Ilbiz E., Kaunert C. Europol and cybercrime: Europol's sharing decryption platform // Journal of Contemporary European Studies.2021. С.3
19. Communication from the Commission to the European Parliament and the Council the EU Internal Security Strategy in Action: Five steps towards a more secure Europe // Brussels. 22.11.2010. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52010DC0673 (дата обращения 20.02.2023 г.).
20. Communication From The Commission To The Council And The European Parliament Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre // Brussels. 28.3.2012. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0140 (дата обращения 20.02.2023 г.).
21. Robinson N., Disley E., Potoglou D., Reding A., Culley D. M., Maryse M., Botterman M., Carpenter G., Blackman C., Millard J. Feasibility Study for a European Cybercrime Centre // RAND Corporation.2012.
22. Miadzvetskaya Y., Wessel R.A. The Externalisation of the EU's Cybersecurity Regime:

The Cyber Diplomacy Toolbox // European Papers. 2022. No. 27/2022. 7(1). C. 413-438.

23. Operational guidance for the EU's international cooperation on cyber capacity building // Luxembourg: Publications Office of the European Union. 2018. [Электронный ресурс] – Режим доступа: https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building (дата обращения 20.02.2023 г.).
24. Council decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service 2010/427/EU/ // Official Journal of the European Union. 3.8.2010. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:201:0030:0040:EN:PDF (дата обращения 20.02.2023 г.).
25. Duic D. The EEAS as a Navigator of EU Defence Aspects in Cyberspace/ Duic D. // European Foreign Affairs Review. –2021.–№
26. – С. 101 – 114. 26. Council Joint Action 2004/551/CFSP of 12 July 2004 on the establishment of the European Defence Agency // Official Journal. 17.7.2004. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004E0551 (дата обращения 20.02.2023 г.).
27. EU Policy on Cyber Defence // Brussels. 10.11.2022 [Электронный ресурс] – Режим доступа:https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf (дата обращения 20.02.2023 г.).
28. Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States // Official Journal of the European Union. 14.12.2017 [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32017D2315 (дата обращения 20.02.2023 г.).
29. Renda K.K. The development of EU cybersecurity policy: from a coordinating actor to a cyber power? // Ankara AvrupaÇalışmalarıDergisi. N2.2021. C. 467-495
30. European Union Military Vision and Strategy on Cyberspace as a Domain of Operations // (EEAS(2021) 706 REV 4, 15 September 2021. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004E0551 (дата обращения 20.02.2023г.).
31. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres // Official Journal of the European Union. 8.6.2021. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0887 (дата обращения 20.02.2023 г.).
32. Капустин А.Я. Общая характеристика основных принципов институциональной системы Европейского Союза // Известия высших учебных заведений. правоведение.№1.2000. С.232.
33. Agreement on strategic co-operation between the European Union Agency for Network and information security and the European Police office (26.06.2014) [Электронный ресурс] – Режим доступа: https://www.europol.europa.eu/cms/sites/default/files/documents/Agreement_on_Strategic_Co-operation_between_the_European_Union_Agency_for_Network_and_Information_Security_and_the_European_Police_Office.pdf (дата обращения 20.02.2023)
34. Memorandum of Understanding on structured cooperation between ENISA and CERT-EU

(15.02.2021). [Электронный ресурс] – Режим доступа: https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2021-4-on-structured-cooperation-with-cert-eu-with-annex-mou (дата обращения 20.02.2023г.).

35. Memorandum of Understanding The European Union Agency for Network and Information Security (ENISA) of the first The European Defence Agency (EDA) of the second part, Europol's European Cybercrime Centre (EC3) of the third part, The Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) of the fourth part (23.05.2018) [Электронный ресурс] – Режим доступа: https://eda.europa.eu/docs/default-source/documents/mou---eda-enisa-cert-eu-ec3---23-05-18.pdf (дата обращения 20.02.2023 г.)
36. Commission Recommendation (EU) 2021/1086 of 23 June 2021 on building a Joint Cyber Unit // Official Journal of the European Union. 5.7.2021. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H1086 (дата обращения 20.02.2023 г.)
37. Ursula von der Leyen A Union that strives for more My agenda for Europe : political guidelines for the next European Commission 2019-2024. [Электронный ресурс] – Режим доступа: https://op.europa.eu/en/publication-detail/-/publication/43a17056-ebf1-11e9-9c4e-01aa75ed71a1 (дата обращения 20.02.2023 г.)

Результаты процедуры рецензирования статьи

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

Предмет исследования. Предметом рецензируемой статьи "Правовой статус органов и учреждений Европейского Союза в области обеспечения кибербезопасности" являются нормы права, закрепленные в международно-правовых актах, определяющие правовое положение органов (организаций) Европейского Союза, на которые возложены функции по обеспечению международной информационной безопасности государств-членов.
Методология исследования. Методологический аппарат этой научной работы составили современные методы познания: исторический, формально-логический, юридико-технический, формально-догматический, сравнительного правоведения и др. Также автором статьи применялись такие научные способы и приемы, как дедукция, моделирование, систематизация и обобщение. Основной метод - сравнительный анализ. В работе использовалось сочетание теоретической и эмпирической информации.
Актуальность исследования. Глобальная цифровизация и построение информационного общества (с переходом к обществу знаний) безусловно кроме "удобств" несет много вызовов, рисков и угроз, что требует принятия соответствующих юридических, организационных и технически мер, в том числе на международном уровне. Организационно-правовой опыт Европейского Союза может представлять не только научный, но и практический интерес. Заслуживает внимания вопрос об организации (структуре органов) обеспечения информационной безопасности на территории Европейского Союза.
Научная новизна исследования. Вопросы обеспечения кибербезопасности, включая организацию деятельности органов (организаций) Европейского Союза, были предметом исследования таких авторов как В.А. Гирис, В.И. Пантин, А.К. Паньковская и др. Однако выбранный автором этой статьи аспект исследования имеет элементы научной новизны: впервые аргументируется необходимость и целесообразность особого учреждения: "с целью оказания взаимной помощи киберсообществам, ответственным за

кибербезопасность, за борьбу с киберпреступностью, за проведение кибердипломатии, за киберзащиту было инициировано создание Совместного киберподразделения".

Стиль, структура, содержание. Статья написана научным стилем, с применением специальной терминологии. Материал изложен последовательно, грамотно и ясно. Позиция автора аргументирована. Статья хотя формально не разделена на части, тем не менее логически структурирована (введение, основная часть и заключение) . Заявленная автором тема раскрыта, по содержанию статья соответствует своему названию. Хотя, на взгляд рецензента, возможно некорректно использование в названии статьи термина "учреждения", т.к. необходимо его разъяснение. Можно только домыслить, что автор имел ввиду такую юридическую категорию как "организация", поскольку "учреждение" для юристов - это особая организационно-правовая форма некоммерческих организаций.

Библиография. Несмотря на достаточно большой перечень использованных источников, можно сделать замечание, что автором не изучены работы других ученых (выше о них упоминалось: В.А. Гирис, В.И. Пантин, А.К. Паньковская), которые тоже изучали проблемы международной информационной безопасности Европейского Союза. Нет в статье ссылок на работы ведущего российского специалиста в области информационного права и информационной безопасности Т.А. Поляковой.

Апелляция к оппонентам. Обращение к точкам зрения других ученых корректное, все заимствования оформлены в форме цитирования со ссылками на источник опубликования.

Выводы, интерес читательской аудитории. Рецензируемая статья "Правовой статус органов и учреждений Европейского Союза в области обеспечения кибербезопасности" отвечает требованиям, предъявляемыми к научным публикациям, является актуальной, практически значимой и содержит элементы научной новизны. Данная работа рекомендуется к опубликования в научном журнале "Международное право и международные организации / International Law and International Organizations". поскольку отвечает редакционной политике этого издания. Статья может представлять интерес для специалистов в области информационного права и информационной безопасности, международного права, а также преподавателей, докторантов, аспирантов, магистрантов и студентов юридических факультетов и вузов.