

Дата поступления рукописи в редакцию: 09.03.2026 г.

DOI: 10.24412/2782-3830-2026-3-371-378

Дата принятия рукописи в печать: 14.04.2026 г.

МАЛЮГИНА Анна Владимировна,

кандидат филологических наук, доцент,
доцент кафедры русского и иностранных языков,
Воронежский институт МВД России,
ORCID ID: 0009-0001-6320-3265,
e-mail: malyugina-anna@yandex.ru

ВАСИЛЬЕВА Ирина Вячеславовна,

кандидат педагогических наук,
доцент кафедры русского и иностранных языков,
Академия ФСИН России,
ORCID ID: 0000-0002-5709-7718,
e-mail: irina-vas2009@yandex.ru

КИБЕРПРЕСТУПНОСТЬ: ПРОТИВОДЕЙСТВИЕ И НАКАЗАНИЕ. ОПЫТ СТРАН ЕВРОПЕЙСКОГО СОЮЗА

Аннотация. В статье представлен обзор политики и нормативно-правового регулирования кибербезопасности в странах Европейского союза (ЕС) с целью выявления перспективных направлений повышения кибербезопасности в Российской Федерации. В работе определено значение киберпреступности в современном мире в глобальном масштабе и в странах ЕС в частности. Являясь одной из глобальных проблем человечества, киберпреступность подрывает не только экономическую стабильность государства, темпы технологического прогресса, но и национальную безопасность. В статье описана эволюция киберугроз, подчеркивается их беспрецедентный уровень в настоящее время. Наиболее частотными являются киберугрозы, связанные с контентом, спам и попытки взлома. Исследование раскрывает существующие проблемы, с которыми сталкиваются страны ЕС при реализации стратегии кибербезопасности. Особое внимание уделяется изучению нормативно-правовой базы, служащей основой для борьбы с киберпреступностью в ЕС на сегодняшний день. Описана система органов, занимающихся вопросами обеспечения кибербезопасности в странах ЕС. Проанализирован опыт правоохранительных органов в области профилактики и противодействия киберпреступности. Авторы рассматривают факторы, препятствующие усилиям этих организаций по предотвращению киберпреступлений. В статье также рассматривается существующая уголовная ответственность за совершение киберпреступлений. Установлено, что подходы к уголовной ответственности за преступления в киберпространстве в законодательстве стран-членов ЕС имеют как общие, так и отличительные черты, обусловленные национальной спецификой в области противодействия киберпреступности. Сделан вывод о том, что при адаптации зарубежного опыта борьбы с киберпреступностью к российским условиям внедрение различных мер противодействия киберпреступности должно осуществляться с учетом правовых, организационных и образовательных ракурсов.

Ключевые слова: Европейский союз, зарубежный опыт, информационная безопасность, киберпреступность, киберугрозы, национальное законодательство, правовые нормы, правовое регулирование, уголовная ответственность.

MALYUGINA Anna V.,

PhD (Philology),
Associate Professor at the Russian and Foreign Languages Chair,
Voronezh Institute of the Ministry of Internal Affairs
of the Russian Federation

VASSILYEVA Irina V.,

PhD (Pedagogical Sciences),
Associate Professor at the Russian and Foreign Languages Chair,
Academy of the Federal Penal Service of Russia

CYBERCRIME: COUNTERMEASURES AND LIABILITY. EXPERIENCE OF THE EUROPEAN UNION

Annotation. The paper provides an overview of the European Union (EU) policies and legislative measures developed to regulate cybersecurity liability in order to identify promising areas for enhancing cybersecurity in the Russian Federation. The paper describes the significance of cybercrime globally and in EU countries in particular. As one of the global problems of humanity, cybercrime not only undermines the economic stability of a state, the pace of technological progress, but also its national security. The paper describes the evolution of cyber threats highlighting their unprecedented levels at present. The most common cyber threats are the ones that are content-related, spam and hacking attempts. The study reveals the problems of countering cybercrime in the EU countries. The article analyzes the most significant legal standards serving as a foundation for combating cybercrime in the EU today. The paper considers principal bodies engaged in cybersecurity in the EU countries. The authors analyse the experience of law enforcement agencies in the EU countries in the field of cybercrime prevention and counteraction. The research delves into the factors impeding the efforts to prevent cybercrimes. Finally, the article reviews the current liability framework for committing cybercrimes in the EU member countries. The authors state that the approaches to criminal liability for crimes in cyberspace in the legislation of EU member states have both common and distinctive features, depending on the national specifics of combating cybercrime policy. This study emphasizes the importance of implementing diverse cybercrime countermeasures while adapting foreign experience of combating cybercrime to Russian conditions, taking into account legal, organizational and educational perspectives.

Key words: European Union, foreign experience, information security, cybercrime, cyber threats, national legislation, legal norms, legal regulation, criminal liability.

Введение

Неотъемлемой частью современного мира являются цифровые технологии. Проникнув практически во все сферы жизнедеятельности человека, цифровизация определяется в качестве одной из основных тенденций развития экономики и общества в целом. По мере того, как мир становится все более взаимосвязанным и зависимым от цифровых технологий, растет потребность в обеспечении информационной безопасности [1, с. 194]. Сегодня угрозы кибербезопасности достигли беспрецедентного уровня, что вызывает острую озабоченность у отдельных лиц, организаций и правоохранительных органов.

Актуальность представленного исследования обусловлена необходимостью изучения зарубежного опыта в исследовании феномена киберпреступности, выявления наиболее эффективных практик противодействия и наказания, которые можно адаптировать к российским условиям. В современных реалиях особую важность приобретает также разработка оптимальной модели подготовки сотрудников полиции к вызовам в сфере киберпреступности, включающей обучение в области законодательства, использования технологий, организационных мер, иностранного языка, международного сотрудничества и др.

Цель исследования состоит в анализе опыта правоохранительных органов стран Европейского союза (далее ЕС) в области профилактики, противодействия киберпреступности, а также изучении уголовной ответственности за соверше-

ние киберпреступлений в обозначенных странах для определения перспективных направлений совершенствования деятельности органов внутренних дел по повышению уровня кибербезопасности в Российской Федерации.

Перечислим задачи нашего исследования:

- определить понятие «кибербезопасность» и охарактеризовать значение киберпреступности в современном мире в целом и в странах ЕС в частности;
- описать существующие киберугрозы и проблемы противодействия киберпреступности в странах ЕС;
- изучить специфику правового регулирования кибербезопасности в странах ЕС;
- описать уголовную ответственность за преступления в киберпространстве в странах ЕС.

Для проведения исследования были применены следующие методы: контент-анализ нормативных правовых документов Евросоюза, общенаучные и специальные методы научного познания правовых явлений, лингвистический перевод.

Материалом исследования послужили официальные сайты европейских организаций: сайт Еврокомиссии [16], сайт Европола [17], официальная онлайн-база данных законодательства Европейского союза и других публичных документов EUR-Lex [18], Конвенция Совета Европы о преступности в сфере компьютерной информации ETS №185 [19], Директива Европейского парламента и Совета Европейского союза 2013 об

атаках на информационные системы [20], заключительный отчет Совета ЕС о практической реализации и функционировании европейской политики по предотвращению и противодействию киберпреступности 2017 [21], Стратегия кибербезопасности ЕС на «цифровое десятилетие» 2020 [22] и др.

Теоретическую основу исследования составили работы, посвященные политике и законодательным мерам по проблеме регулирования кибербезопасности в Европейском союзе J. Matijašević (2014); В. И. Пантина, Н. В. Кардавы (2018), G. G. Fuster, L. Jasmontaite (2020); Э. Верхелст, Я. Ваутерс (2020); О. Г. Ковалева, А. А. Скипидарова (2021), В. А. Гирис (2024) и др. Значительное внимание также уделено работам в области профилактики и противодействия киберпреступности Н. В. Кардавы (2019); Г. Иашвили, М. Явич, С. Гнатюк, А. Фесенко (2019); Н. К. Степановой (2025) и др. Нами также рассматривались зарубежные и отечественные исследования по изучению новых угроз и существующих трудностей в борьбе с киберпреступлениями D. Dave, G. Sawhney, P. Aggarwal (2023), А. И. Бедаева (2024) и др. Кроме того, принимались во внимание исследования В. А. Шестак и А. И. Адигамова (2020), Ю. А. Воронина и Т. В. Кухтиной (2022), в которых рассматривается ответственность за преступления в киберпространстве в странах ЕС.

Представленное исследование имеет существенную прикладную ценность, заключающуюся в возможности использования европейского опыта в противодействии киберпреступности в отечественной практике.

Обсуждение и результаты

«Понятие «кибербезопасность». Значение киберпреступности в современном мире

Понимание кибербезопасности в современном праве ЕС включает два главных аспекта – состояние защищенности от киберугроз и действия, направленные на достижение подобного состояния [2, с. 21].

Как правило, степень общественного информирования о совершенных киберпреступлениях сводится к минимуму, отчасти из-за возможных отрицательных последствий, которые могут возникнуть, если проблемы с безопасностью станут достоянием общественности.

Киберпреступность сегодня является одной из глобальных проблем человечества, подрывая не только экономическую стабильность государства, темпы технологического прогресса, но и национальную безопасность. По данным Global Cybercrime Report 2025, глобальный ущерб от киберпреступности вырастет до 11,9 трлн долларов в 2026 году, а в 2030 году достигнет 19,7 трлн

долларов, что превысит текущий ВВП Китая [23]. Киберпреступность сегодня достигла колоссальных масштабов и в Европе. Девять из наиболее опасных преступных группировок в Евросоюзе занимаются киберпреступлениями [24]. Таким образом, можно констатировать, что киберпреступность в современном мире представляет собой масштабную угрозу, затрагивающую безопасность, экономику и технологическое развитие как отдельных стран, так и мирового сообщества.

Оценка киберугроз и проблемы противодействия

Угрозы кибербезопасности вызывали озабоченность с первых дней существования компьютерных сетей. В 2000–2010 гг. стремительное развитие интернета и широкое внедрение веб-технологий сопровождалось фишинговыми атаками, когда злоумышленники обманом заставляли пользователей раскрывать конфиденциальную информацию с помощью ложных электронных писем. Серьезной угрозой также были кибератаки «отказ в обслуживании», создававшие такие условия, при которых авторизованные пользователи устройства или сети не могли получить доступ к сайту, серверу или сети. С 2010 года по настоящее время важную роль в киберпространстве играют расширенные постоянные угрозы. Представляя собой сложные и целенаправленные атаки, часто спонсируемые национальными государствами, расширенные постоянные угрозы направлены на компрометацию конкретных лиц, организаций или отраслей промышленности. Эти атаки включают комбинацию методов социальной инженерии, вредоносного ПО и эксплуатации сети. Значительный рост киберугроз в последнее время наблюдается в области атак на устройства интернета вещей. Эти атаки могут варьироваться от получения несанкционированного доступа к персональным данным до управления устройствами. Еще одной значимой угрозой на современном этапе являются облачные атаки, связанные с компрометацией учетных записей в облачных хранилищах, использованием уязвимостей в облачной инфраструктуре или кражей конфиденциальных данных из облачных приложений [3, р. 2]. По количеству случаев кибервымогательства второе место в мировом рейтинге занимают компании, размещенные в странах ЕС [4].

Специалисты отмечают разное понимание серьезности информационных угроз в странах Евросоюза, обусловленное разными экономическими возможностями и уровнем кибербезопасности. С 2008 года киберугрозы в ЕС стали восприниматься как возможные угрозы военного характера [5, с. 12, 14]. Активно развивается кибершпионаж. В области разработки и примене-

ния кибербезопасности самыми передовыми национальными стратегиями в странах ЕС обладают Австрия, Венгрия, Нидерланды, Норвегия и ФРГ [6, с. 74].

Согласно данным зарубежных исследователей, изучивших динамику киберпреступлений в мире с 2015 по 2022 год, их число ежегодно увеличивалось. Рост инцидентов, связанных с контентом, составил 578 %, спама – 511 %, попыток взлома – 438% [3, р. 3]. Среди наиболее частотных векторов кибератак в странах Европы вредоносное ПО, похищение профиля и атаки неизвестного типа, которые еще не изучены [7, с. 51].

Сочетание двух факторов – постоянно меняющейся преступной деятельности и недостаток достоверной информации – затрудняют получение точной картины о состоянии киберпреступности в ЕС на современном этапе. Защита физических лиц от киберпреступлений часто осложняется проблемами, связанными с определением надлежащих мер юридического воздействия к правонарушителям, трансграничным правоприменением или признанием и использованием электронных доказательств. Так, например, правоприменительные меры в отношении сайтов с незаконным контентом (содержащих материалы о сексуальном насилии над детьми, подстрекательстве к террористическим актам, незаконной пропаганде насилия, расизма и т.д.) чрезвычайно сложны, поскольку владельцы и администраторы таких сайтов часто находятся в других странах. Сайты могут быть очень быстро перемещены, кроме того, юридическое определение «противозаконности действий» значительно варьируется в разных государствах. Многочисленные киберугрозы и проблемы противодействия обуславливают необходимость их эффективного правового регулирования.

Правовое регулирование кибербезопасности в странах Европейского союза

Публикация первой Стратегии Европейского союза (ЕС) в области кибербезопасности в 2013 году ознаменовала официальное провозглашение «кибербезопасности» в качестве новой области политики в ЕС. Сегодня европейская политика в области кибербезопасности характеризуется высокой степенью фрагментации правовой базы и можно говорить о ее гарантированном развитии в дальнейшем, учитывая растущее значение цифровых технологий в ЕС [8, р. 97–98].

В настоящее время на официальном сайте Еврокомиссии указано, что действия стран-участников ЕС в области кибербезопасности основаны на положениях Конвенции Совета Европы о киберпреступности [25]. Среди последних документов, представленных на сайте, Доку-

мент о временном регулировании обработки персональных и иных данных в целях борьбы с сексуальным насилием над детьми, (здесь и далее перевод авторов), Инструкция по борьбе с мошенничеством с безналичными платежами и Предложения по организации и регулированию действий, облегчающих трансграничный доступ к электронным доказательствам в расследовании уголовных дел. В Конвенции Совета Европы о киберпреступности прописано положение, касающееся создания в каждой стране сети, целью которой является поддержка полиции и других органов власти, занимающихся киберпреступлениями. Такая национальная сеть действует в режиме 24/7 и является связующим звеном для получения информации всеми заинтересованными органами. Обозначенная сеть выступает отправной точкой для всех запросов, касающихся обработки и расследования преступных действий, связанных с компьютерными преступлениями [9, р. 286].

Еще одним действующим правовым документом, определяющим стратегию развития кибербезопасности в странах ЕС, является Директива о безопасности сетевых и информационных систем, принятая Европейским парламентом в 2016 году. В 2020 году в Директиву были внесены изменения с учетом текущих потребностей и перспектив [10]. Директива направлена на защиту от кибератак критической инфраструктуры, связанной с обеспечением жизненно важных цифровых услуг [11, с. 144].

С целью эффективного контроля данных и уменьшения утечек данных пользователей из стран Европы в 2018 года был установлен общий регламент по защите данных GDPR – General Data Protection Regulation [7, с. 52].

Значимой законодательной инициативой в странах ЕС также стал Закон о кибербезопасности ЕС 2019 г., который впервые представил систему сертифицирования технологий цифровой безопасности на всем пространстве ЕС. Согласно этому закону? Европейское агентство по сетевой и информационной безопасности (ENISA) содействует государствам-членам ЕС в решении проблем кибербезопасности и создании национальных групп экстренного реагирования [11, с. 153; 12, с. 11].

Вопросами обеспечения кибербезопасности в странах ЕС занимается разветвленная система органов. Центральная роль отводится именно Европейскому агентству по сетевой и информационной безопасности [2, с. 23]. В августе 2025 года это агентство выпустило Индекс кибербезопасности ЕС, оценивающий состояние кибербезопасности его государств-членов. Одним из важных заключений документа стало

то, что большинство организаций ЕС не используют искусственный интеллект при обеспечении кибербезопасности [26].

В то время как Европейское агентство по сетевой и информационной безопасности занимается широким спектром вопросов кибербезопасности, Европейский центр по борьбе с киберпреступностью фокусируется на правоохранительной деятельности. Созданный Европейской комиссией в 2012 году Европейский центр по борьбе с киберпреступностью при Европоле выступает в качестве координационного центра в борьбе с киберпреступностью в ЕС, объединяя европейский опыт в области киберпреступности и оказывая поддержку в расследовании киберпреступлений в государствах-членах ЕС.

Значимым инструментом в борьбе с киберпреступностью в ЕС является также Европейская междисциплинарная платформа по борьбе с криминальными угрозами EMPACT, осуществляющая свою деятельность четырехлетними циклами. Кибератаки, схемы онлайн-мошенничества и сексуальная эксплуатация детей являются приоритетами в рамках цикла 2026-2029 годов [27].

Обобщая направления деятельности различных органов по противодействию киберпреступности в странах ЕС, можно выделить пять стратегических приоритетов ЕС в области кибербезопасности:

- достижение «кибергибкости» путем установления минимальных требований к функционированию, сотрудничеству и координации национальных компетентных органов в отношении сетевых информационных систем;
- снижение уровня киберпреступности путем обеспечения быстрого внедрения Директив ЕС, связанных с киберпреступностью, и программ финансирования для внедрения оперативных инструментов;
- разработка политики кибербезопасности путем оценки оперативных требований ЕС в области киберзащиты, содействия диалогу и координации между гражданскими и военными субъектами в ЕС, а также с международными партнерами;
- развитие промышленных и технологических ресурсов для обеспечения кибербезопасности путем создания государственно-частной платформы по сетевой и информационной безопасности;
- разработка согласованной международной политики ЕС в области киберпространства и продвижение основных ценностей ЕС путем включения вопросов киберпространства в общую внешнюю политику и политику безопасности [8, pp. 98–99].

Первостепенное значение государствами ЕС уделяется защите персональных данных и информационной деятельности организаций в киберпространстве [10].

Важно учитывать, что ЕС не только старается обеспечить максимально высокий уровень кибербезопасности собственных органов и государств-членов, но и сам может выступать источником киберугроз для российского государства и гражданского общества, поэтому анализ сильных и слабых сторон правового регулирования ЕС в области обеспечения кибербезопасности имеет неоспоримое теоретическое и практическое значение для России [2, с. 5–6].

Уголовная ответственность за преступления в киберпространстве в странах ЕС

Важным аспектом борьбы с киберпреступностью в странах ЕС является проводимая политика в области уголовной ответственности за преступления в киберпространстве. В европейских странах наказание за киберпреступления регулируется национальными законодательствами, которые учитывают как внутренние правовые нормы, так и международные соглашения, например, Конвенцию Совета Европы о киберпреступности и директивы ЕС. Санкции варьируются в зависимости от тяжести преступления, его последствий, а также от того, было ли деяние совершено организованной группой или затронуло критическую инфраструктуру

4 июля 2013 года Европейский парламент проголосовал за законопроект, предусматривающий более жесткие меры против лиц, совершающих киберпреступления. Так, минимальный срок наказания за серьезные киберпреступления (незаконный доступ, вмешательство в системы и данные) сегодня не менее 2 лет лишения свободы [28].

В нормах уголовного законодательства об ответственности за общественно опасные деяния в информационно-цифровой среде в странах ЕС отмечают наличие существенных различий в подходах к формулированию составов преступлений данной категории [13, с. 13]. Например, использование кибернетических устройств при квалификации хищений выделено в уголовном законодательстве Швейцарии и Швеции в отдельные составы преступлений, во Франции и Великобритании, однако, используются общие нормы, регулирующие имущественные преступления [14, с. 279].

Проведя сравнительный анализ уголовной ответственности за несанкционированный доступ к компьютерной информации в странах ЕС, Н.А. Швед выделяет три группы концепций в странах ЕС в отношении несанкционированного доступа к компьютерной информации:

- закрепленный в УК самостоятельный состав несанкционированного доступа (Австрия, Бельгия, Дания и др.);
- несанкционированный доступ рассматривается как способ совершения других преступлений (Испания, Швеция);
- закрепленный в УК несанкционированный доступ не только в качестве самостоятельного состава, но и его понимание как способа совершения других преступлений [15, с. 223].

Анализируя существующие санкции за несанкционированный доступ к компьютерной информации в странах ЕС, стоит отметить, что в большинстве УК за данное преступление предусматривается два вида наказания: штраф и лишение свободы (тюремное заключение) [Там же, с. 224].

В целом, можно констатировать, что подходы к уголовной ответственности за преступления в киберпространстве в законодательстве стран-членов ЕС имеют как общие, так и отличительные черты, обусловленные национальной спецификой в области противодействия киберпреступности.

Заключение

Исследование показало, что в противодействии киберпреступности в странах ЕС задействованы многочисленные организации, выступающие с разнообразными инициативами, направленными на повышение уровня информационной безопасности. Эти инициативы варьируются от принятия нового законодательства в области регулирования реализации стратегии кибербезопасности до создания специальных органов, курирующих отдельные направления. Основное внимание в ЕС уделяется улучшению оперативного сотрудничества правоохранительных органов между государствами-членами; повышению профессионального уровня сотрудников, вовлеченных в борьбу с киберпреступниками; проведению исследований, позволяющих не только оценить существующие опасности и риски от киберпреступлений, но и предсказать появление новых киберугроз.

Изучение европейского опыта борьбы с киберпреступностью является ценным источником идей и концепций для повышения уровня кибербезопасности в Российской Федерации. В первую очередь это касается анализа наиболее эффективных уголовно-правовых средств, которые бы способствовали предупреждению киберпреступности, учитывали специфику национальной правовой системы и не нарушали фундаментальных прав человека.

Важным элементом зарубежного опыта является организация надлежащей профессио-

нальной подготовки российских правоохранителей, которая позволяет овладевать инновационными технологическими решениями для работы в киберпространстве: выявлять противоправные действия в электронной информационной среде на раннем этапе; получать электронные доказательства, необходимые для расследования; участвовать в интернациональных проектах и др.

Таким образом, адаптация зарубежного опыта противодействия киберпреступности к российским условиям включает несколько уровней: законодательный (принятие соответствующих законодательных актов), организационный (создание аналогичных структур по борьбе с киберпреступлениями), образовательный (разработка профессиональных образовательных программ с учетом лучших европейских и мировых практик).

Список литературы:

- [1] Навроцкая И. Н. Цифровые технологии: преимущества и недостатки // Образование. Наука. Научные кадры. 2025. № 1. С. 193–196. DOI: 10.24412/2073-3305-2025-1-193-196
- [2] Гирис В. А. Правовое регулирование деятельности Европейского союза в области обеспечения кибербезопасности: автореф. дис. ... канд. юр. наук. Москва, 2024. – 29 с.
- [3] Dave D., Sawhney G., Aggarwal P., Silswal N., Khut D. The New Frontier of Cybersecurity: Emerging Threats and Innovations. In 2023 29th International Conference on Telecommunications (ICT), IEEE, 2023, pp. 1–6. DOI: 10.1109/ICT60153.2023.10374044
- [4] Ковалев О. Г., Скипидаров А. А. Организационные проблемы обеспечения кибербезопасности в странах Европейского союза // Столыпинский вестник. 2021. Т. 3. № 1. С. 24.
- [5] Бедаев А. И. Международная информационная безопасность в рабочей повестке Евросоюза: угрозы, направления работы и проблемы // Caspium Securitatis: журнал каспийской безопасности. 2024. Т. 4. № 1. С. 11–22.
- [6] Кардава Н. В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни // Каспийский регион: политика, экономика, культура. 2019. № 3 (60). С. 73–78. DOI: 10.21672/1818-510X-2019-60-3-073-078
- [7] Иашвили Г., Явич М., Гнатюк С., Фесенко А. Методы защиты от современных векторов кибер атак в странах Европы // Scientific and Practical Cyber Security Journal (SPCSJ), 2019. 3(2), pp. 49–53.
- [8] Fuster G. G., Jasmontaite L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In: Christen M., Gordijn B., Loi M. (eds) The Ethics of

Cybersecurity. The International Library of Ethics, Law and Technology, vol 21. Springer, Cham. pp.97–115. https://doi.org/10.1007/978-3-030-29053-5_5

[9] Matijašević J. European standards in the field of combating cyber crime // *Megatrend revija*. 2014, Vol. 11, No 4, pp. 279–300. DOI:10.5937/MegRev1404279M

[10] Ковалев О. Г., Скипидаров А. А. Нормативно-правовое регулирование реализации стратегии кибербезопасности в государствах Европейского союза // *Столыпинский вестник*. 2021. Т 3. № 2. Порядковый номер: 5.

[11] Верхелст Э., Ваутерс Я. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // *Вестник международных организаций*. 2020. Т. 15. № 2. С. 141–172 (на русском и английском языках). DOI: 10.17323/1996-7845-2020-02-07

[12] Пантин В. И., Кардава Н. В. Кибербезопасность: проблемы формирования единой политики в Европейском союзе // *Вестник Пермского университета. Политология*. 2018. № 3. С. 5–18.

[13] Воронин Ю. А., Кухтина Т. В. Уголовное законодательство зарубежных стран об ответственности за преступления в информационно-цифровой среде // *Вестник ЮУрГУ. Серия «Право»*. 2022. Т. 22, № 1, С. 13–18. DOI: 10.14529/law220102

[14] Шестак В. А., Адигамов А. И. Современные подходы в законодательстве стран-членов ЕС к уголовной ответственности за преступления в киберпространстве // *Образование и право*. 2020. № 8. С. 277–282. DOI 10.24411/2076-1503-2020-10848

[15] Швед Н. А. Сравнительный анализ уголовной ответственности за несанкционированный доступ к компьютерной информации в странах ЕС // *Вестник Нижегородского университета им. Н. И. Лобачевского*, 2016. № 5. С. 222–226.

[16] European Commission https://commission.europa.eu/index_en

[17] Europol <https://www.europol.europa.eu/how-we-work/sirius-project>

[18] EUR-Lex <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52007DC0267>

[19] Convention on Cybercrime (ETS No.185) Budapest, 23.XI.2001 <https://pircenter.org/wp-content/uploads/2022/10/Convention-of-Cybercrime.pdf?ysclid=mlhqv6j8dh300365350>

[20] Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems <https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng>

[21] Final report of the seventh round of mutual evaluations on “The practical implementation and operation of the European policies on prevention and combating cybercrime”, Council of the European

Union, 2017. <https://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf>

[22] The EU's Cybersecurity Strategy for the Digital Decade, European Commission, Brussels, 2020 <https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52020JC0018>

[23] Global Cybercrime Report 2025. Available at <https://www.proxyrack.com/blog/global-cyber-crime-report-2025/>

[24] РБК (ГК «РосБизнесКонсалтинг») <https://www.rbc.ru/society/06/04/2024/661184a19a79473655e427c7>

[25] Convention on Cybercrime (ETS No.185) Budapest, 23.XI.2001 <https://pircenter.org/wp-content/uploads/2022/10/Convention-of-Cybercrime.pdf?ysclid=mlhqv6j8dh300365350>

[26] Новый индекс кибербезопасности Евросоюза. Infowatch. <https://www.infowatch.ru/analytics/daydzhesty-i-obzory/noviy-indeks-kiber-bezopasnosti-evrosoyuza>

[27] Cybercrime. European Commission. https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

[28] Solmecke Ch. Tougher penalties for cybercrime in EU. WBS.LEGAL сайт <https://www.wbs.legal/allgemein/tougher-penalties-for-cybercrime-in-eu-15419/>

References:

[1] Navrotskaya I.N. Digital technologies: advantages and disadvantages//*Education. Science. Scientific cadres*. 2025. № 1. S. 193-196. DOI: 10.24412/2073-3305-2025-1-193-196

[2] Giris V. A. Legal regulation of the activities of the European Union in the field of cybersecurity: ref. dis.... cand. jur. sciences. Moscow, 2024. - 29 s.

[3] Dave D., Sawhney G., Aggarwal P., Silswal N., Khut D. The New Frontier of Cybersecurity: Emerging Threats and Innovations. In 2023 29th International Conference on Telecommunications (ICT), IEEE, 2023, pp. 1–6. DOI: 10.1109/ICT60153.2023.10374044

[4] Kovalev O. G., Skipidarov A. A. Organizational problems of ensuring cybersecurity in the countries of the European Union//*Stolypinsky Bulletin*. 2021. Т 3. № 1. P. 24.

[5] Bedaev A.I. International information security on the EU working agenda: threats, directions of work and problems//*Caspium Securitatis: Journal of Caspian Security*. 2024. VOL. 4. № 1. S. 11-22.

[6] Kardava N.V. Cybersecurity policy in the European Union: national and supranational levels//*Caspian region: politics, economy, culture*. 2019. № 3 (60). S. 73-78. DOI: 10.21672/1818-510X-2019-60-3-073-078

[7] Iashvili G, Yavich M, Gnatyuk S, Fesenko A. Methods of protection against modern vectors of

cyber attacks in European countries//Scientific and Practical Cyber Security Journal (SPCSJ), 2019. 3(2), pp. 49–53.

[8] Fuster G. G., Jasmontaite L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In: Christen M., Gordijn B., Loi M. (eds) The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21. Springer, Cham. pp.97–115. https://doi.org/10.1007/978-3-030-29053-5_5

[9] Matijašević J. European standards in the field of combating cyber crime // Megatrend revija. 2014, Vol. 11, No 4, pp. 279–300. DOI:10.5937/MegRev1404279M

[10] Kovalev O. G., Skipidarov A. A. Regulatory regulation of the implementation of the cybersecurity strategy in the states of the European Union//Stolypinsky Bulletin. 2021. T 3. № 2. Sequence number: 5.

[11] Verhelst E, Wouters J. Global Governance for Cybersecurity: A Perspective on International and EU Law//Bulletin of International Organizations. 2020. VOL. 15. № 2. S. 141-172 (in Russian and English). DOI: 10.17323/1996-7845-2020-02-07

[12] Pantin V.I., Kardava N.V. Cybersecurity: problems of forming a unified policy in the European Union//Bulletin of Perm University. Political science. 2018. № 3. S. 5-18.

[13] Voronin Yu. A., Kukhtina T. V. Criminal legislation of foreign countries on responsibility for crimes in the information and digital environment//Bulletin of SUSU. "Right" series. 2022. T. 22, NO. 1, S. 13-18. DOI: 10.14529/law220102

[14] Shestak V.A., Adigamov A.I. Modern approaches in the legislation of EU member states to criminal liability for crimes in cyberspace//Education and law. 2020. № 8. S. 277-282. DOI 10.24411/2076-1503-2020-10848

[15] Swede N. A. Comparative analysis of criminal liability for unauthorized access to computer information in EU countries//Bulletin of Nizhny Novgorod University named after N. I. Lobachevsky, 2016. NO. 5C. 222–226.

[16] European Commission https://commission.europa.eu/index_en

[17] Europol <https://www.europol.europa.eu/how-we-work/sirius-project>

[18] EUR-Lex <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52007DC0267>

[19] Convention on Cybercrime (ETS No.185) Budapest, 23.XI.2001 <https://pircenter.org/wp-content/uploads/2022/10/Convention-of-Cybercrime.pdf?ysclid=mlhqv6j8dh300365350>

[20] Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems <https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng>

[21] Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime", Council of the European Union, 2017. <https://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf>

[22] The EU's Cybersecurity Strategy for the Digital Decade, European Commission, Brussels, 2020 <https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52020JC0018>

[23] Global Cybercrime Report 2025. Available at <https://www.proxyrack.com/blog/global-cyber-crime-report-2025/>

[24] RBC (GC RosBusinessConsulting) <https://www.rbc.ru/society/06/04/2024/661184a19a79473655e427c7>

[25] Convention on Cybercrime (ETS No.185) Budapest, 23.XI.2001 <https://pircenter.org/wp-content/uploads/2022/10/Convention-of-Cybercrime.pdf?ysclid=mlhqv6j8dh300365350>

[26] New EU cybersecurity index. Infowatch. <https://www.infowatch.ru/analytics/day-dzhesty-i-obzory/noviy-indeks-kiberbezopasnosti-evrosoyuza>

[27] Cybercrime. European Commission. https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

[28] Solmecke Ch. Tougher penalties for cybercrime in EU. WBS.LEGAL сайт <https://www.wbs.legal/allgemein/tougher-penalties-for-cyber-crime-in-eu-15419/>

