9. УГОЛОВНО-ПРАВОВЫЕ НАУКИ

УГОЛОВНОЕ ПРАВО И КРИМИНОЛОГИЯ, УГОЛОВНО-ИСПОЛНИТЕЛЬНОЕ ПРАВО (СПЕЦИАЛЬНОСТЬ 12.00.08)

9.1. Правовые основы кибербезопасности в Российской Федерации

DOI: 10.33693/2072-3164-2021-14-4-260-265

©Серебренникова А.В.
Московский Государственный Университет им. М.В. Ломоносова, г. Москва, Россия
serebranna@hotmail.com

Аннотация

Статья посвящена исследованию отечественных источников права в области кибербезопасности. На основе обобщения источников в области международного права, уголовного законодательства зарубежных государств и положений, выработанных в российской правовой доктрине, автор приводит к выводу о невозможности эффективной борьбы с киберпреступностью исключительно при использовании инструментария отдельно взятого государства. Необходимость международного сотрудничества в обозначенной сфере проходит красной строкой во всех программных и нормативных документах отрасли.

Цель статьи: Цель статьи заключается в анализе международно-правовых норм, действующего отечественного законодательства на предмет возможности совершенствования уголовно-правового механизма противодействия проявлениям «харассмента» в российском обществе.

Методология и методы: в настоящем исследованиии автор широко использует методы анализа, синтеза, индукции, а также метод толкования правовых норм.

Выводы: в результате исследования, автор приходит к выводу о необходимости обеспечения глобальной безопасности киберпространства не только путем совершенствования законодательства РФ, но и эффективного международного сотрудничества. В настоящей статье автором представлен генезис нормативного закрепления механизма противодействия киберугрозам, проведен анализ взаимного влияния источников международного и государственного права, рассмотрены основные положения программных и концептуальных документов, обозначающих сущность законодательных инициатив России в соответствующей сфере.

Автор делает вывод, что учет международного опыта в данном вопросе будет способствовать эффективности проводимых реформ.

Область применения результатов: материал статьи адресован студентам высший высших учебных заведений, а также аспирантам, проводящим научные исследования в рамках НИР. Помимо этого выводы по настоящей статье могут быть использованы преподавателями юридических вузов в качестве научно-методического материала.

Ключевые слова: *кибербезопасность; киберпреступность; информационная безопасность; киберугрозы; правовые основы; критическая инфраструктура; информационные технологии.*

Для цитирования*: Серебренникова А.В. Правовые основы кибербезопасности в Российской Федерации // Пробелы в российском законодательстве. 2021. Т. 14. №4. С. 260-265. DOI: 10.33693/2072-3164-2021-14-4-260-265*

The Legal Framework for Cybersecurity in the Russian Federation

DOI: 10.33693/2072-3164-2021-14-4-260-265

©Anna V. Serebrennikova
Moscow state University named after M. V. Lomonosov, Moscow, Russia
serebranna@hotmail.com

Abstract

The article is devoted to the study of domestic sources of law in the field of cybersecurity. Based on a generalization of sources in the field of international law, criminal legislation of foreign states and provisions developed in the Russian legal doctrine, the author concludes that it is impossible to effectively combat cybercrime when using the tools of a single state. The need for international cooperation in the designated area is a red line in all program and regulatory documents of the industry.

Purpose of the article: The purpose of the article is to analyze international legal norms, current domestic legislation for the possibility of improving the criminal law mechanism for countering manifestations of "harassment" in Russian society.

Methodology and methods: in this study, the author makes extensive use of methods of analysis, synthesis, induction, as well as the method of interpreting legal norms.

Conclusions: as a result of the study, the author comes to the conclusion that it is necessary to ensure the global security of cyberspace by improving the legislation of the Russian Federation and effective international cooperation. In this article, the author presents the genesis of the normative consolidation of the mechanism for countering cyber threats, analyzes the mutual influence of sources of international and state law, considers the main provisions of program and conceptual documents that indicate the essence of Russia's legislative initiatives in the relevant area.

The author concludes that taking into account international experience in this issue will contribute to the effectiveness of the reforms.

Scope of the results: the material of the article is addressed to students of higher educational institutions, as well as graduate students conducting scientific research in the framework of research. In addition, the conclusions of this article can be used by teachers of law schools as a scientific and methodological material.

***Keywords**: cybersecurity; cybercrime; Information Security; cyber threats; legal framework; critical infrastructure; Information Technology.*

***For citation**: Serebrennikova A.V. The Legal Framework for Cybersecurity in the Russian Federation // Gaps in Russian legislation. 2021. Vol. 14. №4. Pp. 260-265. (in Russ.). DOI: 10.33693/2072-3164-2021-14-4-260-265*

Введение

В настоящее время в научных кругах и в политическом дискурсе мирового сообщества все чаще встречается термин «кибербезопасность». Опасность проблемы преступности в сфере информационных технологий возрастает с каждым годом и находится в прямой зависимости от глобализации и цифровизации. Наряду с мировыми настроениями, каждое государство стремится обеспечить безопасность общественных отношений, связанных с использованием информационных технологий в своей юрисдикции, предпринимая организационные и законотворческие меры, направленные на создание эффективных механизмов противодействия противоправным проявлениям в данной сфере [16, с.63]. В условиях нарастающей угрозы от воздействия продуктов вредоносного программного обеспечения, государству, стремящемуся к недопущению дестабилизации информационной обстановки крайне важно, чтобы национальный сегмент глобальной сети Интернет был как можно более безопасным для его пользователей.

Статистические данные

По некоторым оценкам, от 10 000 до 20 000 человек в России задействованы в так называемом «даркнете», например, занимаются банковским мошенничеством, продают вредоносное ПО и рассылают спам [14, с.32]. Различные аспекты киберпреступности в России являются весьма захватывающими, загадочными, противоречивыми и сложными. Во многих зарубежных источниках сообщается, что российские хакерские сети и структуры организованной преступности сотрудничают с преступными группировками из других стран.

Ряд недавних громких киберпреступлений якобы возложен на Россию. По информации Генпрокуратуры РФ за последние пять лет число киберпреступлений, совершаемых пользователями в РФ увеличилось более чем в 11 раз, а удельный вес их в структуре преступности возрос с 1,8% до 25%. Большинство киберпреступлений совершается с использованием сети Интернет или при помощи средств мобильной связи [19]. Тема кибербезопаности стала одной из ключевых во время российско-американских переговоров, прошедших в Женеве 16 июня 2021 года [12].

В этой связи, в обществе закономерно возникает запрос на разработку эффективной законодательной основы для безопасного использования информационных технологий и противодействию киберпреступности.

Международно-правовые основы

Одним из первых документов, разработанных на международном уровне и ставших основой обеспечения глобальной кибербезопасности, стала Конвенция ООН о киберпреступности 2001 года. Отдельные особенности проведения следственных действий на территории иностранного государства без проведения процедуры их обязательного согласования, закрепленные в обозначенном документе, стали причиной того, что он не был ратифицирован РФ. Тем не менее, многие из его положений были восприняты отечественным законодателем и применены при формировании национальных правовых основ [18, с.158].

В подавляющем большинстве государств первичными являются политические меры, отражаемые в качестве ключевых направлений деятельности в концептуальных документах. В качестве наиболее актуального примера можно привести Стратегию США в области киберпространства, принятую в сентябре 2018 года [13].

Национальное законодательство

В Российской Федерации доктринальная и нормативная разработка системы кибербезопасности и информационных технологий также является политически обоснованной и берет свое начало с конца XX века. Здесь следует сказать о том, что в первоначальной редакции Уголовного кодекса РФ [1] уже были предусмотрены составы преступлений, посягающих на кибербезопасность.

Дальнейшее развитие правовых основ противодействия киберпреступности складывалось поэтапно. Среди наиболее значимых программных документов в данной сфере необходимо выделить две Доктрины информационной безопасности РФ: 2000 года[2] и 2016 года [4]. Кроме того, необходимо упомянуть об Указе Президента РФ от 17 марта 2008 г. № 351 [4], и Основу государственной политики РФ в области международной информационной безопасности на период до 2020 года [5].

Говоря о действующей Доктрине информационной безопасности 2016 года следует упомянуть, что в ней находят отражение официальные позиции органов государственной власти РФ по поводу главных вопросов в сфере обеспечения кибербезопасности. Данный документ явился логическим продолжением Концепции внешней политики РФ от 30 ноября 2016 года [6]. В Доктрине законодатель разъясняет что он подразумевает под национальными интересами в информационной сфере. Также, при обеспечении суверенитета РФ в информационной сфере рекомендовано пользоваться технологиями российского производства. Поддержка отечественных разработчиков продуктов информационной инфраструктуры представляется весьма важной и проходит одной из основных идей документа. Отмечается важность перехода информационных систем органов государственной власти и частного сектора на отечественные разработки. Подчеркивается о том, что источники посягательств на кибербезопасность могут исходить как со стороны отдельных государств, так и со стороны представителей криминальных структур и лиц,

пропагандирующих экстремизм в различных его проявлениях. В документе отмечается, что особенности сети Интернет способствуют анонимности противоправных проявлений в информационной среде. В качестве основного приоритета в борьбе с киберпреступностью в документе определяется необходимость межгосударственного взаимодействия для выявления новых угроз и создание эффективной системы противодействия им. Вышеизложенное свидетельствует о том, что отечественный законодатель открыт к ведению работы по заключению международных договоров в области кибербезопасности, о чем неоднократно отмечалось на самом высоком уровне[7].

Следующий концептуальный документ, о котором необходимо упомянуть в контексте настоящего исследования, является Стратегия развития информационного общества в РФ на 2017-2030 годы [8]. Стратегия представляет собой документ, в котором обозначены приоритеты на среднесрочную перспективу, для достижения оптимального баланса интересов внутренней и внешней политики РФ в сфере кибербезопасности. Особо упоминается о необходимости перехода от импортных криптографических алгоритмов и программного обеспечения к аналогам, разработанным российскими специалистами. При этом, такой переход рекомендуется как в цифровом документообороте органов государственной власти, так и при обмене информации между коммерческими предприятиями и гражданами.

Некоторые приоритетные направления обеспечения информационной инфраструктуры РФ были закреплены в Государственной программе «Информационное общество (2011-2020 годы)»[9]. К числу таких направлений относится обеспечение независимости нашего государства в технологическом секторе экономики, в котором активно используются элементы инновационной инфраструктуры; противодействие использования злоумышленниками широкого потенциала информационных технологий для посягательств на национальные интересы РФ; обеспечение безопасности права на частную жизнь, личную и семейную тайны; совершенствование нормативной основы в данной сфере.

Еще одним важнейшим достижением, способствующим обеспечению кибербезопасности в РФ, является создания Фонда перспективных исследований. Соответствующий Федеральный закон № 174-ФЗ был подписан 16 октября 2012 года [10]. Деятельность данного Фонда, исходя из его названия, направлена на осуществление научных исследований по различным направлениям, среди которых в законе обозначено обеспечение безопасности киберпространства.

26 июня 2017 года был подписан Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также, законы, вносящие корреспондирующие изменения в УК РФ и УПК РФ.

Федеральным законом № 187-ФЗ устанавливаются основные принципы обеспечения безопасности критической информационной инфраструктуры (КИИ), обозначены основные полномочия органов власти по данному направлению деятельности, закреплены основные права и обязанности, а также обозначена сфера ответственности граждан, в собственности или распоряжении которых находятся объекты КИИ. При этом, как в вышеобозначенном документе, так и на уровне Доктрины отмечается, что безопасность КИИ РФ предполагает защиту от компьютерных атак без нарушения ее стабильного функционирования [15]. В документе обозначена ответственность за создание и (или) распространение вредоносных компьютерных программ, а также иной информации, предназначенной для неправомерного воздействия на КИИ.

Международное сотрудничество

Отмечая вопрос международного сотрудничества в сфере обеспечения глобальной кибербезопасности и противодействия киберпреступности следует отметить активную деятельность представителей органов государственной власти РФ в данном направлении. Например, после проведения регионального заседания совета министров государств – членов СНГ, по инициативе РФ были обозначены ключевые позиции по вопросам взаимодействия правоохранительных органов стран Содружества, согласованы позиции в процессе реализации региональных программ борьбы с преступностью. Кроме того, Россия стала одним из инициаторов проведения в конце июля 2017 года в Душанбе заседания совета министров внутренних дел государств - членов СНГ, участниками которого обсуждались приоритетные направления сотрудничества правоохранительных органов Содружества по вопросам обеспечения безопасности в киберпространстве. Соглашение о сотрудничестве, ставшее итогом данного совещания, подписано 28 августа 2017 года Президентом РФ[11].

Помимо регионального сотрудничества по обеспечению кибербезопасности, важным направлением для политики РФ является глобальное сотрудничество. В данной сфере стоит упомянуть обсуждение Проекта Конвенции ООН «О сотрудничестве в сфере противодействия информационной преступности» весной 2017 года. По своей характеристике, данный документ предлагается применять в качестве альтернативы Будапештской конвенции. Хотя переговоры о ключевых позициях Конвенции ведутся до сих пор, Россия является активным их участником. В документе на глобальном уровне предлагается координированная работа, направленная на содействие принятию и укреплению мер, направленных на предупреждение и эффективную борьбу с киберпреступностью, устанавливается порядок оказания правовой и информационной помощи между государствами-участницами. Кроме того, в Проекте Конвенции предлагается введение специализированного глобального контактного центра, работающего круглосуточно. Особыми направлениями, обозначенными в Проекте Конвенции, является кадровая работа, а также проведение конференций по определению и масштабированию положительного опыта.

Законодательные новеллы

Также, в 2020 году Россия представила проект Конвенции ООН о борьбе с киберпреступностью [17]. В документе обозначен транснациональный характер киберугроз и необходимость оперативного сотрудничества государств по обмену информацией. Как и в предыдущем проекте Конвенции, здесь указывается о важности подготовки высококвалифицированных кадров для правоохранительных органов, создания международных платформ для обмена опытом. В Проекте Конвенции 2020 года предусмотрены механизмы для оперативного отслеживания перемещения лиц, причастных к совер-

шению киберпреступлений из одного государства в другое, даже при отсутствии профильных двусторонних соглашений между такими государствами.

Следует отметить, что с подобными инициативами РФ выступает уже не впервые. Первый проект Конвенции «Об обеспечении международной информационной безопасности» был направлен от нашей страны уже в 2011 году. Целью данного проекта, по мнению России, являлось создание полноценного международного соглашения по вопросам безопасности цифровой среды. В документе обозначены важнейшие аспекты противодействия идей военного противодействия в киберпространстве, борьбе с международным кибертерроризмом и преступлениями против собственности. Несмотря на все усилия, документ так не получил одобрения со стороны государств НАТО, поскольку те усмотрели в нем попытки навязывания со стороны России идеи тотального контроля над национальными сегментами глобальной сети. Поэтому, перспективы принятия Проекта Конвенции 2020 года в настоящее время остаются весьма неопределенными, особенно в условиях доминирования США на мировой арене в сфере кибертехнологий. Считаем, что налаживание дипломатических отношений России с США по вопросам взаимодействия в области кибербезопасности является неизбежным для обеих сторон.

В настоящее время вызывает опасения, что информационные технологии используются в противоправных целях не только отдельными гражданами или преступными структурами, но и спецслужбами отдельных государств, что напрямую противоречит ключевым документам ООН. Об этом напрямую указывается и в действующей Доктрине информационной безопасности.

Однако во всех вышеперечисленных нормативных актах законодателем так и не были даны определения терминам «киберпространство» и «кибербезопасность». Проект «Концепции стратегии кибербезопасности» 2014 года, в котором как раз и была предусмотрена соответствующая терминология, после длительных обсуждений так и не приобрел форму нормативного акта, и перспективы его принятия до настоящего времени являются весьма маловероятными по причине позиции ФСБ РФ.

Представляется, что отсутствие терминологии в сфере безопасности киберпространства на уровне международных и национальных источников права является существенным препятствием в процессе взаимодействия между государствами. Поэтому, мы считаем крайне необходимым разработку единой универсальной терминологии в сфере кибербезопасности, которая согласовывалась бы с уже существующими терминами информационной безопасности, КИИ и т. д.

Выводы

Обобщение правовых источников в сфере кибербезопасности, разработанных на международном уровне и в РФ приводит к выводу о невозможности эффективной борьбы с киберпреступностью при использовании инструментария отдельно взятого государства. Необходимость международного сотрудничества в обозначенной сфере проходит красной строкой во всех программных и нормативных документах отрасли. Такое сотрудничество возможно лишь при стандартизации подходов и оперативности реагирования на киберугрозы. Только восприятие передового опыта, наряду с имплементаций соответствующих положений в национальное законодательство может дать правоохранительным органам необходимый инструментарий для упреждающего воздействия на источники глобальных угроз в киберпространстве. Именно поэтому, наша позиция о необходимости разработки универсального общеобязательного международного документа по обеспечению кибербезопасности является особо актуальной. Представляется, что такой документ необходимо обновлять с учетом новых вызовов и угроз, выявляемых на международной арене.

Подводя итог исследованию правовых основ и инициатив России в сфере обеспечения кибербезопасности следует сказать, что тема противодействия киберугрозам является обширной и становится все более важной, потому что мир становится все более взаимосвязанным, а информационные сети все активнее используются для выполнения важных транзакций. Киберпреступность продолжает расходиться разными путями с каждым новым годом, как и безопасность информации. Новейшие и революционные технологии, а также новые киберинструменты и угрозы, которые обнаруживаются каждый день, бросают вызов организациям не только в том, как они защищают свою инфраструктуру, но и в том, что им для этого требуются новые платформы и технологии. Не существует идеального решения для обеспечения кибербезопасности, но государствам следует предпринимать исчерпывающие усилия по их минимизации и обеспечению безопасного будущего в киберпространстве.

Заключение

Именно поэтому, представляется важным осуществление постоянного мониторинга киберугроз, существующих на мировой арене, выявление и масштабирование передового опыта противодействия противоправным проявлениям в информационном пространстве. Организации, работающие с конфиденциальной информацией и имеющие низкие знания в области кибербезопасности, имеют огромный риск возникновения киберугроз. Именно поэтому, считаем важным направлением деятельности обеспечение учебной и просветительской работы по развитию навыков в сфере кибербезопасности работников организаций государственного и коммерческого секторов.

Список литературы:

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021) [Электронный ресурс] // Доступ: СПС «КонсультантПлюс Проф» (Дата обращения: 21.06.2021).
2. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 N Пр-1895) [Электронный ресурс] // Доступ: СПС «КонсультантПлюс Проф» (Дата обращения: 21.06.2021).

References:

1. The Criminal Code of the Russian Federation of 13.06.1996 N 63-FZ (as amended on 05/04/2021, as amended on 08/04/2021) [Electronic resource] // Access: SPS "ConsultantPlus Prof" (Date of access: 21.06.2021).
2. Doctrine of information security of the Russian Federation (approved by the President of the Russian Federation 09.09.2000 N Pr-1895) [Electronic resource] // Access: SPS "ConsultantPlus Prof" (Date of access: 21.06.2021).

3. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" [Электронный ресурс] // Доступ: СПС «КонсультантПлюс Проф» (Дата обращения: 21.06.2021).

4. Указ Президента РФ от 17.03.2008 N 351(ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" [Электронный ресурс] // Доступ: СПС «КонсультантПлюс Проф» (Дата обращения: 21.06.2021).

5. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 N Пр-1753) [Электронный ресурс] // Доступ: СПС «КонсультантПлюс Проф» (Дата обращения: 21.06.2021).

6. Указ Президента РФ от 30.11.2016 N 640 "Об утверждении Концепции внешней политики Российской Федерации" [Электронный ресурс] // Доступ: СПС «КонсультантПлюс Проф» (Дата обращения: 21.06.2021).

7. Путин отнес к киберугрозам ограничение доступа к передовым технологиям и кибератаки. ТАСС. [Электронный ресурс] // Доступ: https://tass.ru/politika/11127653 (Дата обращения: 20.06.2021).

8. Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" [Электронный ресурс] // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 10.05.2017 (Дата обращения: 18.06.2021).

9. Постановление Правительства РФ от 15.04.2014 N 313 (ред. от 16.12.2020) "Об утверждении государственной программы Российской Федерации "Информационное общество" (с изм. и доп., вступ. в силу с 26.12.2020) [Электронный ресурс] // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 10.05.2017 (Дата обращения: 18.06.2021).

10. Федеральный закон от 16.10.2012 N 174-ФЗ (ред. от 19.07.2018) "О Фонде перспективных исследований" [Электронный ресурс] // Доступ: СПС «КонсультантПлюс Проф» (Дата обращения: 19.06.2021).

11. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Заключено в г. Душанбе 28.09.2018) [Электронный ресурс] // Доступ: СПС «КонсультантПлюс Проф» (Дата обращения: 19.06.2021).

12. «Отыграть ситуацию»: почему в Белом доме вновь заговорили о возможности кибератак против России [Электронный ресурс] // https://russian.rt.com/world/article/874772-baiden-putin-kiberataki (Дата обращения: 21.06.2021).

13. National cyber strategy of the United States of America [Электронный ресурс] // Доступ: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

14. Бочкарев М.А., Марценюк А.В., Корнилов А.В. Киберпреступность в условиях современного мира: тенденция развития и методы противодействия // Студенческий вестник. 2019. № 46-3 (96). С. 31-34.

15. Елекова А.С. Развитие нормативной базы в области обеспечения безопасности в критических информационных инфраструктурах // В книге: МНСК-2017: Информационные технологии. Материалы 55-й Международной научной студенческой конференции. 2017. С. 36.

3. Decree of the President of the Russian Federation of 05.12.2016 N 646 "On Approval of the Doctrine of Information Security of the Russian Federation" [Electronic resource] // Access: SPS "ConsultantPlus Prof" (Date of access: 21.06.2021).

4. Decree of the President of the Russian Federation of 17.03.2008 N 351 (ed. Of 22.05.2015) "On measures to ensure information security of the Russian Federation when using information and telecommunication networks of international information exchange" [Electronic resource] // Access: SPS "ConsultantPlus Prof "(Date of access: 21.06.2021).

5. Fundamentals of the state policy of the Russian Federation in the field of international information security for the period until 2020 (approved by the President of the Russian Federation on July 24, 2013 N Pr-1753) [Electronic resource] // Access: SPS "ConsultantPlus Prof" (Date of access: 21.06.2021).

6. Decree of the President of the Russian Federation of 30.11.2016 N 640 "On Approval of the Concept of Foreign Policy of the Russian Federation" [Electronic resource] // Access: SPS "ConsultantPlus Prof" (Date of access: 21.06.2021).

7. Putin classified restriction of access to advanced technologies and cyber attacks as cyber threats. TASS. [Electronic resource] // Access: https://tass.ru/politika/11127653 (Date of access: 20.06.2021).

8. Decree of the President of the Russian Federation of 09.05.2017 N 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017 - 2030" [Electronic resource] // Official Internet Portal of Legal Information http://www.pravo.gov.ru, 05/10/2017 (Date of access: 06/18/2021).

9. Decree of the Government of the Russian Federation of 15.04.2014 N 313 (revised from 16.12.2020) "On approval of the state program of the Russian Federation" Information Society "(as amended and supplemented, entered into force on 26.12.2020) [Electronic resource] // Official Internet portal of legal information http://www.pravo.gov.ru, 05/10/2017 (Date of access: 06/18/2021).

10. Federal Law of 16.10.2012 N 174-FZ (as amended on 19.07.2018) "On the Fund for Advanced Research" [Electronic resource] // Access: SPS "ConsultantPlus Prof" (Date of access: 19.06.2021).

11. Agreement on cooperation of the member states of the Commonwealth of Independent States in the fight against crimes in the field of information technology (Concluded in Dushanbe on September 28, 2018) [Electronic resource] // Access: SPS "ConsultantPlus Prof" (Date of access: 06/19/2021) ...

12. "Replay the situation": why the White House again started talking about the possibility of cyberattacks against Russia [Electronic resource] // https://russian.rt.com/world/article/874772-baiden-putin-kiberataki (Date of access: 21.06 .2021).

13. National cyber strategy of the United States of America [Electronic resource] // Access: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

14. Bochkarev M.A., Martsenyuk A.V., Kornilov A.V. Cybercrime in the modern world: development trend and methods of counteraction // Student Bulletin. 2019. No. 46-3 (96). S. 31-34.

15. Elekova A.S. Development of the regulatory framework in the field of security in critical information infrastructures // In the book: MNSK-2017: Information Technologies. Materials of the 55th International Scientific Student Conference. 2017.S. 36.

16. Матвеев, В.А. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации / В.А. Матвеев. В.Л. Цирлов // Вопросы кибербезопасности. - 2013. - № 1(1). -С. 61-64.

17. Россия представила проект конвенции ООН о борьбе с киберпреступностью РИА-новости [Электронный ресурс] // Доступ: https://ria.ru/20170524/1495007020.html (Дата обращения: 20.06.2021).

18. Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис.... канд. юрид. наук. М., 2015. С. 158.

19. Число киберпреступлений в России выросло в 11 раз за пять лет. ТАСС. [Электронный ресурс] // Доступ: https://tass.ru/obschestvo/10616343 (Дата обращения: 21.06.2021).

16. Matveev, V.A. State and prospects for the development of the information security industry of the Russian Federation / V.A. Matveev. V.L. Tsirlov // Cybersecurity Issues. - 2013. - No. 1 (1). -FROM. 61-64.

17. Russia presented the draft UN convention on combating cybercrime to RIA-novosti [Electronic resource] // Access: https://ria.ru/20170524/1495007020.html (Date of access: 20.06.2021).

18. Safonov OM Criminal and legal assessment of the use of computer technologies in the commission of crimes: the state of legislation and law enforcement practice, prospects for improvement: dis .... cand. jurid. sciences. M., 2015.S. 158.

19. The number of cybercrimes in Russia has grown 11 times in five years. TASS. [Electronic resource] // Access: https://tass.ru/obschestvo/10616343 (Date of access: 21.06.2021).

Статья прошла проверку системой «Антиплагиат»; оригинальность текста – 85,81%

СВЕДЕНИЯ ОБ АВТОРЕ

Серебренникова А.В., д-р юрид. наук, профессор, МГУ им. М.В. Ломоносова, г. Москва. ORCID: http://orcid.org/0000-0002-1064-4171. E-mail: serebranna@hotmail.com

ABOUT THE AUTHOR

Anna V. Serebrennikova, Dr.Sci (Law), Professor of criminal law and criminology, Moscow state University named after M. V. Lomonosov, Moscow, Russia. ORCID: http://orcid.org/0000-0002-1064-4171. E-mail: serebranna@hotmail.com