УДК 343.85
ББК 67.515
DOI 10.25724/VAMVD.CVWX

М. А. Желудков, А. М. Попов, М. М. Дубровина

ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РОССИИ И ЗАРУБЕЖНЫХ СТРАНАХ

Актуальность представленной статьи заключается в том, что при анализе зарубежного опыта по противодействию киберпреступности видны противоречивые положения национальных законодательных систем. По разным критериям оцениваются виды компьютерных преступлений и прорабатываются стратегии обеспечения кибербезопасности, отсутствует единый документ нормативного регулирования, причем накопленный опыт в этой сфере информативен, что позволяет осуществлять анализ борьбы с киберпреступностью с учетом различных наднациональных правовых систем. Обоснован вывод о том, что необходимо оценить реализацию нормативного содержания обеспечения кибербезопасности в разных странах. Без закрепления в нормативной документации определенного понятийного аппарата невозможно создать полноценную структуру защищенности. В научной статье поставлена цель изучить различные подходы к построению общих и специальных норм правового обеспечения противодействия киберпреступности и отразить те ценные моменты, которые следует задействовать в отечественном нормативном поле.

Ключевые слова: киберпреступления, кибербезопасность, стратегия борьбы с киберпреступлениями, информационные технологии, конвенция, национальное киберпространство.

M. A. Zheludkov, A. M. Popov, M. M. Dubrovina

PROBLEMS OF LEGAL SUPPORT OF COUNTERACTION OF CYBERCRIME IN RUSSIA AND FOREIGN COUNTRIES

The relevance of the presented article is that when analyzing foreign experience in countering cybercrime, there are contradictory provisions of national legislative systems. According to different criteria, types of computer crimes are assessed and strategies for ensuring cybersecurity are being developed, there is no single regulatory document, and the accumulated experience in this field is informative, which makes it possible to carry out an analysis of the fight against cybercrime, taking into account various supranational legal systems. The conclusion is substantiated that it is necessary to evaluate the implementation of the normative content of ensuring cybersecurity in different countries. Without fixing in the normative documentation of a certain conceptual apparatus, it is impossible to create a full-fledged security structure. The scientific article aims to study various approaches to the construction of general and special norms for the legal support of countering cybercrime and to reflect those valuable moments that should be used in the domestic regulatory field.

Key words: cybercrime, cybersecurity, strategy against cybercrime, information technology, convention, national cyberspace.

Современное государство нельзя представить без цифрового информационного пространства, которое направлено на процветание экономики, развитие научного потенциала, формирование определенного уровня общения в различных сферах общественных отношений. «Наиболее общим направлением государственной политики в кибербезопасности является защита стратегических интересов» [1, с. 46]. Однако для того чтобы эти технологии продолжали открывать людям новые возможности, насущной необходимостью становится наличие системной основы правового обеспечения безопасности как на уровне национального, так и международного законодательства. «Политические конфликты в киберпространстве, киберпреступность, негативные тенденции в онлайн-экономике и в онлайн-образовании — с этой реальностью приходится сталкиваться уже всем без исключения членам мирового сообщества. Российская Федерация не является исключением и в большей или меньшей степени активно участвует в этих глобальных процессах» [2]. Если говорить о преступных угрозах в указанной сфере, то по данным, представленным Генеральным прокурором Российской Федерации: «Число преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, в России с 2013 по 2016 г. увеличилось в 6 раз — с 11 тыс. до 66 тыс.» [3]. Стоит отметить, что при прокурорском надзоре подобным угрозам нужно уделить принципиальное внимание [4, с. 102].

Нельзя забывать и о том, что, кроме негативных последствий для права собственности «реализация киберугроз может привести к нарушению мира и безопасности, к подрыву доверия в международных отношениях, а также к отрицательному воздействию на целостность государственных инфраструктур и нанесению недопустимого ущерба» [5, с. 59]. В связи с этим необходимо оценить реализацию нормативного содержания обеспечения кибербезопасности в различных странах. Как указывают отдельные авторы: «Социально-юридическая природа рассматриваемых поступков едина» [6, с. 150], — поэтому для принятия национальной стратегии кибербезопасности важно не упустить ценного информационного материала, накопленного в других государствах. Так, подход Соединенных Штатов Америки (США) к принципам защищенности киберпространства основывается на убеждении, что сетевые технологии обладают огромным потенциалом для всего мира. США вошли в число стран, которые первыми начали борьбу с киберпреступлениями. Еще в 1986 г. был принят специальный закон о компьютерном мошенничестве и компьютерных злоупотреблениях, где были выделены три группы преступных деяний. Дополнением выступил Закон «О конфиденциальности электронных сообщений» (Electronic Communications Privacy Act of 1986, ECPA). В нем закреплялось понятие электронного сообщения и несанкционированного доступа к электронным сведениям, предусматривались меры наказания «не более одного года тюремного заключения; штраф в размере не более 500 долларов» [7]. Среди других нормативных документов США выделим следующие: Акт поправок к Закону «О компьютерных злоупотреблениях» (1994 г.), Акт о модернизации финансовых услуг (1999 г.), Акт о контаминации компьютеров (2000 г.), Национальная стратегия по защите киберпространства (2003 г) и др. На эти документы обратили внимание в Европе. Здесь были подготовлены различные стратегии и планы киберзащиты. «Список всех национальных стратегий кибербезопасности стран Евросоюза (ЕС) и некоторых других стран, не входящих в его состав, опубликован Европейским агентством по безопасности сетей и информационной безопасности (The European Network and Information Security Agency — ENISA)» [8].

Самыми распространенными «направлениями государственных основ борьбы с киберпреступлениями в разных странах стали:

1. Защита стратегических и правительственных информационных систем от кибератак и актов кибертерроризма (Германия, Великобритания, Канада, Литва, Люксембург, Нидерланды, США, Эстония).

2. Правовое регулирование, а также совершенствование уголовного и информационного законодательства (Германия, Канада, Люксембург, США, Эстония, Японии).

3. Защита информации и персональных данных (Словакия, Франция, Чешская Республика, Литва).

4. Государственное и международное сотрудничество (Люксембург, США, Япония).

Среди других направлений можно выделить обучение сотрудников правоохранительных органов и информирование граждан о киберугрозе (Люксембург, Эстония) и продвижение международных стандартов экономической безопасности (США, Люксембург)» [1, с. 45—46]. В частности, в 2006 г. была разработана Стратегия безопасности Интернета в Швеции. В Эстонии в 2008 г. была опубликована Государственная стратегия кибербезопасности. «Стратегия информационной безопасности Словакии от 2008 г. основной задачей ставила создание платформы, необходимой для формирования информационного общества и направленной на поддержку благоприятных условий для обеспечения интересов граждан, общества и государства» [9].

«Стратегия Финляндии также была разработана в 2008 г. В ее основе лежит понимание кибербезопасности в качестве проблемы экономического характера, напрямую связанной с формированием финского информационного общества. Здесь особое внимание уделяется необходимости обеспечения безопасности данных для обычных пользователей сети „Интернет“. Кроме того, в Стратегии Финляндии отмечается, что основа для обеспечения кибербезопасности — это подготовленность всего общества, требующая наличия высокого уровня образования населения, профессиональных компаний, работающих на международном рынке в сфере защиты данных, а также научно-исследовательских работ, проводимых передовыми университетами и институтами» [9].

«В Германии в 2011 г. была принята Стратегия безопасности в киберпространстве и создано Национальное агентство киберзащиты, необходимое для взаимодействия с полицией, разведкой и Федеральным управлением по информационной безопасности. Основой ее работы стало создание системы для оперативного обнаружения и эффективного отражения хакерских атак, а также обеспечения безопасности критически важных информационных систем» [10].

Нужно отметить, что большинство зарубежных государств при предупреждении киберпреступности придают большое значение именно разработке стратегий безопасности.

В числе общепринятых источников международного обеспечения кибербезопасности следует назвать Рекомендацию № R 89 (9) Комитета министров стран — членов Совета Европы о преступлениях, связанных с компьютерами, от 13 сентября 1989 г. В отдельных научных трудах указывается, что именно в ней закреплена система «преступлений, связанных с использованием компьютерных технологий» [11, с. 120]. В полной мере с этим мнением согласиться нельзя. «Обращаясь к первоисточнику, на сайте Совета

Европы находим, что данная рекомендация представлена только на одной странице и в ней отражены лишь вопросы, связанные с необходимостью государств-членов учитывать при рассмотрении своего законодательства доклад по компьютерной преступности, разработанный Европейским комитетом по проблемам преступности» [12, с. 193]; [13].

Указание на необходимость разработки национального законодательства не подкреплено определением общественно опасных деяний в сфере компьютерной безопасности, поэтому от рекомендации следует перейти к докладу Европейского комитета по проблемам преступности, где «в перечень правонарушений, рекомендованных к обязательному включению во внутригосударственное уголовное законодательство, внесены:

a) компьютерное мошенничество;

b) компьютерный подлог;

c) причинение ущерба компьютерным данным или компьютерным программам;

d) компьютерный саботаж;

e) несанкционированный доступ;

f) несанкционированный перехват;

g) несанкционированное воспроизведение охраняемой авторским правом компьютерной программы;

h) несанкционированное воспроизведение микросхемы.

К факультативному перечню были отнесены:

a) изменение компьютерных данных или компьютерных программ;

b) компьютерный шпионаж;

c) несанкционированное использование компьютера;

d) несанкционированное использование охраняемой законом компьютерной программы» [11, с. 121—122].

Если провести сравнение с уголовным законодательством России, то можно смело утверждать, что многие деяния, которые признаются преступлениями в зарубежных странах, не имеют норм в Уголовном кодексе Российской Федерации. Отсюда заключаем, что «киберпреступность является реальной угрозой мировой безопасности наряду с международным терроризмом и торговлей наркотиками, и поэтому возникают обстоятельные вопросы к национальному российскому законодательству, на каком уровне находится нормативное регулирование предупреждения указанных деяний?» [13, с. 194]. В России правовая база в рассматриваемой сфере развивается с 2000 г., когда была принята первая Доктрина информационной безопасности Российской Федерации, которая утратила силу в связи с принятием Указа Президента Российской Федерации от 5 декабря 2016 г. № 646, утвердившего новую Доктрину информационной безопасности Российской Федерации.

17 марта 2008 г. Президентом Российской Федерации был подписан Указ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» № 315. Данный документ закрепил ограничения для информационных ресурсов, содержащих государственную и служебную тайну, при использовании технических средств подключения к информационно-телекоммуникационным сетям международного обмена информацией и Интернету.

В ноябре 2013 г. Совет Федерации проводил слушания по поводу проекта Концепции стратегии кибербезопасности Российской Федерации, который затем (в 2014 г.) был представлен на сайте Совета Федерации для общественного обсуждения [13]. В этом документе нашли отражение многие спорные позиции, однако его содержание вызвало вопросы. Одним из них стал вопрос о том, как можно включить в наименование документа сразу два термина «концепция» и «стратегия». Концепция (от лат. conceptio — понимание, система) — это определенный способ понимания, трактовки каких-либо явлений, основная точка зрения, руководящая идея для их освещения; система взглядов на явления в мире, природе, обществе. В свою очередь, «стратегия — это общий, недетализированный план какой-либо деятельности, охватывающий длительный период; способ достижения сложной цели» [13, с. 194]. Под стратегией в различных источниках также понимается искусство руководства общественной, политической борьбой, планирования руководства, основанного на правильных и далеко идущих прогнозах [14].

Обоснованно задаемся вопросом: предложенный в Совете Федерации проект следует считать планом деятельности или системой взглядов на подобную деятельность? Отметим, что: «Концепция кибербезопасности — это идеи, которые при их реализации отражают определенное состояние объекта, где ему не может угрожать опасность. Состояние характеризуется тем, что описывает переменные свойства, положение объекта в пространстве или во времени. Создать план „состояния“ юридически невозможно. В данном случае напрашивается план обеспечительных мероприятий защищенности объекта. Необходимо разрабатывать именно стратегию действий на определенный период, так как различные концепции кибербезопасности не дают полноценной возможности для предупредительной работы правоохранительных органов в данном направлении» [13, с. 194]. Возможно, по этой причине в конце 2013 г. был принят другой нормативный источник «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» [9]. Однако и его нельзя

назвать полноценной стратегией предупреждения именно киберпреступлений.

На международном уровне «со стороны Российской Федерации в различных структурах ООН постоянно обсуждаются документы, направленные на регулирование вопросов кибербезопасности. Так, в 2011 г. на сессии Генеральной Ассамблеи ООН представители Китая, Российской Федерации, Таджикистана и Узбекистана предложили рассмотреть Правила поведения в области обеспечения международной информационной безопасности. В обосновании указывалось то, что вопросы интернет-безопасности следует рассматривать в рамках международного сотрудничества и в духе взаимного уважения. Принимаемый Кодекс был призван создать защитный механизм в Интернете от угроз и уязвимости» [8]. Однако эти и другие подобные инициативы были проигнорированы международным сообществом, представленные документы обсуждались, но решение об их одобрении и принятии отсутствует.

Таким образом, оценка сведений по нормативному обеспечению кибербезопасности приводит нас к неутешительному выводу о том, что на данном этапе уровень международного сотрудничества слабо обеспечивает предупреждение киберпреступности. Каждая страна концентрирует свои усилия на вопросах противодействия отдельным видам компьютерных преступлений. При этом современное российское общество находится в процессе саморегулирования, создавая специальные уровни общения в социальных сетях, посвященных именно безопасности в киберпространстве. Например, «по адресу social.ligainternet.ru. создана сеть „Кибердружина“, в которую может вступить любой желающий. Цели ее создания заключаются в объединении на одной тематической площадке всех граждан, заинтересованных в кибербезопасности. В настоящее время на этом ресурсе зарегистрировано более 10 тыс. человек не только из регионов России, но и из стран СНГ, ближнего зарубежья, Европы и США. Началась работа над английской версией проекта» [5].

Отметим и тот факт, что сегодня в мире защищаются конфиденциальные данные и права человека, вместе с тем отсутствуют кодификационные подходы к решению этих проблем. Сложности существуют также при создании единого международного органа, который будет уполномочен расследовать преступления и осуществлять уголовное преследование преступной киберагрессии. В связи с этим перед нашим государством возникает главный вопрос: «как сохранить весь позитивный потенциал борьбы с киберпреступностью и в то же время нейтрализовать негативные и деструктивные тенденции интернет-пространства?» [5].

Отсутствие единой международной стратегии кибербезопасности и нежелание мирового сообщества достигнуть консенсуса при ее разработке приводят к тому, что отдельные страны прорабатывают свои защитные меры. В частности, «каждый пользователь китайского сегмента информационного пространства при регистрации в социальных сетях и на других сайтах обязан вводить паспортные данные, иначе доступ к таким сайтам для этого пользователя будет закрыт. Такие меры были вызваны распространением клеветы, недобросовестной рекламы и мошенничества в киберпространстве КНР. Они сильно повлияли на внешний облик киберпространства Китая, фактически уничтожив свободу общения. Однако свой вклад в противодействие киберпреступности данные нововведения внесли — уровень киберпреступности в социальных сетях Китая резко снизился» [15, с. 55]; [1]. В этом направлении движется и система правового обеспечения киберзащиты в России.

В то же время с учетом насущных задач предупредительной деятельности в области кибербезопасности обоснованно считаем, что: «Несогласованность российского и международного нормативного регулирования указанных процессов предопределяет слабую эффективность защиты объектов собственности от киберпреступлений. Уголовно-правовое регулирование кибербезопасности невозможно без соответствующей стратегии предупредительной деятельности, без реальной оценки угроз от киберпреступности, которая проявляется на различных временных промежутках и в различных сферах общественной жизни Российского государства» [13, с. 195]. В связи с этим, по нашему мнению, сегодня наиболее возможно реализовать защищенность киберпространства не с позиции международного права, а с учетом того что каждое государство имеет правовые полномочия и должно самостоятельно управлять своим информационным пространством регулируемым нормами национального законодательства, где международные нормы обеспечения кибербезопасности, которые показали свою эффективность, найдут достойное место. Предлагаем вновь провести общественное обсуждение по имплементации международных норм в российское законодательство, что позволит осуществить идеи, закрепленные в мировой практике, но на основе юридической техники России. Кроме того, необходимо принять стратегию кибербезопасности, которая должна учитывать принципы свободы слова и не ограничивать уровень общения в интернет-пространстве без достаточных на то оснований и реальных угроз.

1. Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. … канд. юрид. наук. М., 2016. 232 с.
2. Кибербезопасность и управление интернетом: документы и материалы для российских регуляторов и экспертов / отв. ред. М. Б. Касенова; сост. О. В. Демидов и М. Б. Касенова. М.: Статут, 2013. 464 с.
3. Егоров И. Юрий Чайка рассказал о борьбе с интернет-преступностью // Рос. газ. 2017. № 7356 (190).
4. Печников Н. П. Проблемы теории и практики прокурорского надзора за процессуальной деятельностью органов предварительного следствия // Вопросы современной науки и практики. Университет им. В. И. Вернадского. 2012. № 38. С. 101—105.
5. Казарин О. В, Тарасов А. А. Современные концепции кибербезопасности ведущих зарубежных государств // Вестник РГГУ. Серия «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность». 2013. № 2. С. 58—63.
6. Медведева С. В., Ментюкова М. А. Особенности классификации и состава обстоятельств, исключающих правовую ответственность личности // Вопросы современной науки и практики. Университет им. В. И. Вернадского. 2015. № 1 (55). С. 150.
7. Electronic Communications Privacy Act of 1986, ECPA. URL: http://dorothy.as.arizona.edu/ LAW/ ref5.html (дата обращения 05.02.2018).
8. The National Strategy to Secure Cyberspace. URL: http://www.whitehouse.gov/pcipb/ (дата обращения 05.02.2018).
9. Государственные стратегии кибербезопасности. URL: https://www.securitylab.ru (дата обращения 05.02.2018).
10. Germany passes strict cyber-security law to protect «critical infrastructure». URL: https:// www.rt.com/news (дата обращения 05.02.2018).
11. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2001. 496 с.
12. Сайт Совета Европы. URL: https: // search.coe.int (дата обращения 22.01.2018).
13. Желудков М. А. Особенности реализации в России международного опыта по защите от корыстных преступлений, совершаемых в киберпространстве // Вестник экономической безопасности. 2016. № 5. С. 191—195.
14. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. М.: Азъ, 1992. URL: http://lib.ru /DIC/OZHEGOW (дата обращения 22.01.2018).
15. Информационный ресурс «China Space». URL: http://www.chinaspace.ru (дата обращения: 06.01.2013).

1. Prostorydov M. A. Economic crimes committed in cyberspace, and measures to counteract them: dis. ... cand. jurid. sciences. Moscow, 2016. 232 p.
2. Cybersecurity and Internet governance: documents and materials for Russian regulators and experts / responsible. ed. M. M. M. Kasenova; comp. O. V. Demidov, M. B. Kasenova. Moscow: Statute, 2013. 464 p.
3. Egorov I. Yuri Chaika spoke about the fight against Internet crime // Rossiyskaya gazeta. 2017 No 7356 (190).
4. Pechnikov N. P. Problems of theory and practice of prosecutor's supervision over the procedural activity of the bodies of preliminary investigation // Issues of modern science and practice. University of. V. I. Vernadsky. 2012. No 38. P. 101—105.
5. Kazarin O. V, Tarasov A. A. Modern concepts of cybersecurity of leading foreign states // Herald of the RSUH. Series "Documentology and Archival Studies. Computer science. Information security and information security". 2013. No 2. P. 58—63
6. Medvedeva S. V., Mentyukova M. A. Features of classification and composition of circumstances that exclude the legal responsibility of the individual // Questions of modern science and practice. University of. V. I. Vernadsky. 2015. No 1 (55). 150 p.
7. Electronic Communications Privacy Act of 1986, ECPA. URL: http://dorothy.as.arizona.edu/ LAW/ref5.html (reference date: 05/02/2018).
8. The National Strategy to Secure Cyberspace. URL: http://www.whitehouse.gov/pcipb/ (reference date 05/02/2018).
9. State Cybersecurity Strategies. URL: https:// www.securitylab.ru (reference date: 05/02/2018).
10. Germany passes strict cyber-security law to protect "critical infrastructure". URL: https: // www. rt.com/news (reference date: 05/02/2018).
11. Volevodz A. G. Counteracting Computer Crimes: The Legal Basis of International Cooperation. Moscow: Yurlitinform, 2001. 496 p.
12. Site of the Council of Europe. URL: https: // search.coe.int (circulation date 22.01.2018).
13. Zheludkov M. A. Features of the implementation in Russia of international experience on protection from mercenary crimes committed in cyberspace // Bulletin of Economic Security. 2016. No 5. P. 191—195
14. Ozhegov S. I., Shvedova N. Yu. The explanatory dictionary of the Russian language. Moscow: Az, 1992. URL: http://lib.ru/DIC/OZHEGOW (reference date: 22/01/2018).
15. Information resource "China Space". URL: http://www.chinaspace.ru (reference date: 01/06/2018).