УДК 002:004.056+347.775.03
ББК Ч865.2
DOI: 10.14529/law180314

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ПОНЯТИЕ, ОСНОВАНИЯ ВОЗНИКНОВЕНИЯ, ВИДЫ)

Т. А. Полякова
Институт государства и права РАН, г. Москва,
Д. Д. Савенкова
Управление противодействия кибермошеничеству ПАО «Сбербанк», г. Москва

Авторы статьи предлагают определить понятие юридической ответственности, основания наступления и виды юридической ответственности за совершение правонарушений в области информационной безопасности, а также рассматривают актуальные вопросы правоприменения. Актуальность затрагиваемой темы связана с объективными процессами массового перехода существенной части правоотношений в цифровую среду, тенденцией «цифровой трансформации» преступности и незащищенностью рядовых граждан от противоправных действий в цифровой среде. Проведен анализ такого вида юридической ответственности, как административная, а также регулирующих ее норм. Предлагается совершенствование нормативно-правовой базы, продолжение научных исследований в области информационного права, направленных на изучение общих вопросов ответственности в области информационной безопасности.

Ключевые слова: информационная безопасность, информационные правонарушения, кибератаки, цифровое развитие, юридическая ответственность, административная ответственность.

Проблема обеспечения информационной безопасности в условиях перехода к глобальному информационному обществу приобрела особую актуальность[1]. Все большее количество систем принятия решений и бизнес-процессов в ведущих отраслях экономики и сфере государственного управления реализуется либо планируется к реализации с использованием информационных технологий. В настоящее время в различных информационных системах консолидируется значительный объем информации, в том числе касающийся вопросов государственной политики и обороны, финансовой и научно-технической сферы, а также частной жизни граждан Российской Федерации.

При формировании информационного общества одним из принципов является верховенство права, а соответственно актуальными являются и вопросы юридической ответственности за правонарушения в информационной сфере [7, с. 287]. При этом вся система правового регулирования отношений в информационной сфере нацелена на обеспечение эффективности отношений, укрепление гарантий соблюдения прав субъектов правоотношений [6, с. 373].

В современных условиях развития цифровизации и глобализации особенно справедливо утверждение выдающегося юриста В. Ф. Яковлева, о том что право постоянно развивается и становится все более сложным и дифференцированным. Совершенствуется правовая ответственность, появляются новые ее варианты. Но для того, чтобы вопросы ответственности решались правильно и законодателем, и правоприменителем, следует исходить из того, что есть общее понятие ответственности как общеправовой категории. Однако ответственность в разных отраслях права отличается большим своеобразием [10, с. 5].

Представляется, что в условиях развития информационного общества, появления новых вызовов и угроз вопросы юридической ответственности приобретают особое значение. Многим ученым различных отраслей права, занимавшимся исследованиями в данной области, так и не удалось привести к об-

[1] Статья написана в рамках государственного задания по теме «Новые вызовы и угрозы в информационном пространстве: правовые проблемы обеспечения информационной безопасности».

щему знаменателю единое, общее понятие юридической ответственности. Так, по мнению С. С. Алексеева, «ответственность – государственное принуждение, выраженное в праве, выступает как внешнее воздействие на поведение, основанное на организованной силе государства…» [1, с. 106]. В целом же на этот счет в общей теории права имеется множество точек зрения. Есть точка зрения, что юридическая ответственность – это «прежде всего, государственное принуждение к исполнению требований права, содержащее осуждение деяний правонарушителя государством и обществом» [9, с. 6]. С. Н. Братусь считал, что юридическая ответственность – это «исполнение обязанности посредством государственного принуждения, например уплата суммы долга заемщиком на основе решения суда» [3, с. 85, 94]. Н. В. Витрук полагал, что «юридическая ответственность как мера государственного принуждения осуществляется на основе и в рамках закона, то есть она является правовой формой государственного принуждения» [4, с. 432].

Отдельного внимания заслуживает точка зрения И. Л. Бачило, которая определяла юридическую ответственность как «применение компетентным государственным органом санкции правоохранительной нормы и наступление отрицательных последствий в рамках закона для правонарушителя в виде установленных вида и меры наказания, соразмерных нанесенному ущербу (вреду)» [6, с. 373–374].

Однако, несмотря на различные позиции известных ученых-правоведов и дискуссий, ведущихся в российской науке, мы полагаем, что юридическую ответственность в информационной сфере можно рассматривать как реакцию государства на совершенное правонарушение в зависимости от тяжести содеянного, имеющую общеобязательный и принудительный характер.

Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества. Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

Исходя из положений Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646, институт юридической ответственности в информационной сфере необходимо рассматривать как систему норм и процедур, реализуемых в целях пресечения правонарушений и установления вида, формы и мер наказания за совершенные и доказанные преступления или иные правонарушения, посягающие на информацию, объекты информатизации, информационные системы, сайты в информационно-телекоммуникационной сети «Интернет», сети связи, информационные технологии, субъекты, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, с учетом их социального вреда и вины правонарушителя.

Доктрина содержит перечень угроз, совокупность средств, способных обеспечить надежную защиту информационной безопасности государства, а также прямое указание на то, что общественные отношения в области обеспечения информационной безопасности как никогда нуждаются в правовом регулировании в связи с динамикой развития информационного общества, институализацией правовых институтов в области обеспечения информационной безопасности, являющейся важной составляющей национальной безопасности Российской Федерации.

26 октября 2017 г. на расширенном заседании Совета Безопасности Президентом Российской Федерации В. В. Путиным отмечено: «Мы должны четко представлять тенденции развития глобальной информационной сферы, прогнозировать потенциальные угрозы и риски. И главное – наметить дополнительные меры, которые позволят нам не просто своевременно выявлять угрозы, а активно реагировать на них» [5]. Вместе с тем рост угроз в информационном пространстве повышается, число рисков увеличивается, а негативные последствия разного рода компьютерных атак носят уже не локальный, а действительно глобальный характер и масштаб. Неслучайно Глава государства выражает обеспокоенность по поводу современных киберугроз и состояния защищенности информационного пространства.

Обращает на себя внимание и Стратегия научно-технологического развития Российской Федерации, утвержденная Указом Президента РФ от 1 декабря 2016 г. № 642, в которой прямо указывается на то, что новые

внешние угрозы национальной безопасности, обусловленные ростом международной конкуренции и конфликтности, глобальной и региональной нестабильностью, и усиление их взаимосвязи с внутренними угрозами национальной безопасности, являются одними из наиболее значимых больших вызовов с точки зрения научно-технологического развития Российской Федерации.

Данные обстоятельства формируют актуальность совершенствования и развития правового регулирования в области противодействия новым вызовам и угрозам национальной безопасности, информационной безопасности личности и общества в целом, которое нежизнеспособно без использования передовых цифровых технологий.

Государственная программа «Информационное общество» (2011–2020 годы), утвержденная Постановлением Правительства РФ от 15 апреля 2014 г. № 313 (далее по тексту – Программа), разработана для создания целостной и эффективной системы использования информационных технологий, при которой граждане получают максимум выгод. Ожидаемые результаты реализации Программы впечатляют – это и осуществление взаимодействия государства, граждан и бизнеса преимущественно на основе применения информационно-телекоммуникационных технологий, и обеспечение высокой степени интеграции Российской Федерации в мировое информационное общество, и создание на всей территории Российской Федерации современной информационно-телекоммуникационной инфраструктуры, обеспечивающей доступность качественных услуг связи и широкополосного доступа к информационно-телекоммуникационной сети «Интернет» не менее чем для 95 % граждан страны, а также обеспечение прав и основных свобод человека в информационном обществе, достижение такого уровня развития технологий защиты информации, который обеспечивает неприкосновенность частной жизни, личной и семейной тайны, безопасность информации ограниченного доступа.

Положительные стороны реализации Программы, безусловно, очевидны – государство создает все необходимые условия для интенсивного развития информационного общества. В то же время такая всеобщая информатизация и стремительные изменения в данной сфере требуют повышенного внимания к себе со стороны научных исследований в области правового обеспечения информационной безопасности. Новые вызовы и угрозы, трансграничность глобального информационного общества обусловливают актуальность научных исследований, поиск и развитие новых подходов к их противодействию.

Стремительное развитие информационных технологий и глобальной сети Интернет уже сегодня поставило под угрозу не только отдельно взятых ее пользователей, но и информационную безопасность целых государств, поскольку и государство, и граждане становятся уязвимыми для посягательств из любой точки земного шара в условиях трансграничности и развития информационного обмена посредством Интернета.

В связи с этим увеличиваются и факторы риска. Во-первых, неизбежно увеличивается зависимость общества от информационных технологий, что в свою очередь обусловливает его уязвимость к различным видам информационных посягательств. Во-вторых, с ростом количества пользователей всемирной сети Интернет возрастает потенциальная возможность стать жертвой использования информационных технологий в преступных целях.

Таким образом, транснациональный характер угроз и ущерб от их применения формируют у государства и общества в целом отношение к проблеме обеспечения информационной безопасности как к действительно глобальной проблеме, требующей больших совместных усилий со стороны всеобщего мирового сообщества.

Принятие ряда новых нормативных правовых актов информационного законодательства Российской Федерации обозначило заложение правового фундамента для дальнейших практических шагов в направлении обеспечения информационной безопасности, предупреждения и пресечения правонарушений в информационной сфере, в том числе и путем установления юридической ответственности за их совершение.

Несмотря на то, что компьютерная преступность (киберпреступность) возникла относительно недавно, с развитием информационных технологий это явление превратилось в глобальную проблему, поставив под угрозу не только отдельно взятых пользователей всемирной сети Интернет, но и информационную безопасность целых государств, поскольку и государство, и граждане становятся уязвимы-

ми для посягательств из любой точки земного шара в условиях трансграничности и развития информационного обмена посредством Интернета. В мае 2017 года всего за три дня вирус-шифровальщик WannaCry атаковал 200 тыс. компьютеров в 150 странах мира и прошелся по сетям университетов в Китае, заводов Renault во Франции и Nissan в Японии, телекоммуникационной компании Telefonica в Испании и железнодорожного оператора Deutsche Bahn в Германии. Указанные примеры подтверждают, что традиционных мер безопасности уже недостаточно для защиты промышленных сред от киберугроз [2].

Следует отметить, что правонарушения, совершаемые в Интернете, не требуют особых усилий и затрат. Злоумышленникам достаточно иметь компьютер, программное обеспечение и подключение к информационной сети. В настоящее время не требуется даже глубоких технических познаний: в Интернете существуют специальные форумы, закрытые чаты в мессенджерах, которые, к сожалению, позволяют приобрести вредоносное компьютерное программное обеспечение для совершения правонарушений, похищенные номера кредитных карт, персональные и идентификационные данные пользователей, а также воспользоваться услугами по помощи в совершении электронных хищений и атак на компьютерные системы различных объектов.

Открытый доступ к сети Интернет позволяет совершать компьютерные преступления именно с ее использованием, поскольку установить лицо, совершившее правонарушение, достаточно затруднительно. Анонимность сети Интернет, уязвимость беспроводного доступа и использование прокси-серверов дают возможность существенно затруднить обнаружение злоумышленников – для совершения преступления может использоваться так называемая «цепочка серверов», о чем также есть масса информации в открытом доступе в Интернете, и этому навыку легко можно научиться [8]. Также противоправные деяния могут быть совершены и при помощи выхода в Интернет через точки общего доступа (рестораны, кафе, общественный транспорт). Современные технологии используются для взлома чужой беспроводной сети Wi-Fi.

Расследование правонарушений, совершенных в глобальной сети, обычно требует быстрого анализа и сохранения электронных данных, которые по своей природе достаточно уязвимы и могут быть быстро уничтожены злоумышленниками. Это обусловлено одной из отличительных черт, присущих компьютерной преступности, – для совершения такого деяния, порой, злоумышленнику требуется времени меньше минуты. Кроме того, никто не ограничивает преступника в выборе места, где он будет использовать свои технические устройства при совершении противоправных действий. И это является еще одной особенностью, присущей компьютерной преступности, – как правило, компьютерные преступления носят трансграничный характер.

В этой связи актуальным является вопрос о территориальной юрисдикции в случае совершения правонарушения на территории другого государства. Это определяет необходимость привлечения к ответственности за противоправные действия компьютерного злоумышленника как со стороны государства, на территории которого он использовал технические устройства при совершении противоправных действий, так и со стороны государства, которому или гражданам которого причинен ущерб. Данные обстоятельства прямо указывают на необходимость совершенствования и модернизации нормативно-правовой базы. Если говорить о таком основании привлечения к ответственности, то в данном случае здесь подразумевается наличие / отсутствие в деянии (как действии, так и бездействии) правонарушителя состава правонарушения в информационной сфере, предусмотренного соответствующего нормами права.

Основополагающие положения законодательства в информационной сфере содержатся в Конституции Российской Федерации. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» является основным в силу того, что именно в его ч. 1 ст. 10 закреплено положение о разрешении на территории Российской Федерации свободного распространения информации при соблюдении требований, установленных законодательством Российской Федерации. Этот же закон содержит отдельную ст. 17, которая так и называется: «Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации».

Нарушение положений иных нормативных правовых актов, регулирующих общественные отношения в информационной сфере, также может повлечь за собой наступление

юридической ответственности (к примеру, федерального законодательства о банках и банковской деятельности, о связи, о персональных данных, о доступе к информации, о средствах массовой информации).

Правонарушения в информационной сфере разграничиваются по степени опасности и квалифицируются с токи зрения наступления общественно-опасных последствий, которые такие деяния могут за собой повлечь. Разделить по данному критерию информационные правонарушения возможно на преступления, административные правонарушения и проступки (служебные и дисциплинарные). При квалификации действий виновного субъекта информационного правонарушения важно разграничивать его прямой умысел с действиями, которые по неосторожности в результате повлекли за собой наступлений общественно-опасных последствий. По нашему мнению, именно цели и мотив деяния субъекта определяют вид применяемой к такому субъекту юридической ответственности, а именно: уголовная, административная или гражданско-правовая.

Административная и гражданско-правовая ответственность, в отличие от уголовной ответственности, не предусматривают наказание в виде лишения свободы за противоправную информационную деятельность.

Как и УК РФ, КоАП РФ разграничивает составы информационных правонарушений по разным разделам. Наибольшее число составов (более 40), охватывающих проблемы информации и средств связи, содержится в главе 13 «Административные правонарушения в области связи и информации».

Анализ составов информационных правонарушений показал, что все правонарушения, за которые главой 13 КоАП РФ установлена административная ответственность, в зависимости от области воздействия субъекта можно разделить на три группы: в области связи; в области средств массовой информации; посягающие на установленный законом порядок сбора, хранения, использования, распространения и защиты информации ограниченного доступа, а также порядок применения информационных технологий.

Однако нормы, предусматривающие юридическую ответственность за правонарушения в информационной сфере, содержатся и в других главах КоАП РФ. К ним можно отнести следующие: «Отказ в предоставлении информации» (ст. 5.39), «Сокрытие или искажение экологической информации» (ст. 8.5), «Использование служебной информации на рынке ценных бумаг» (ст. 15.21), «Разглашение сведений о мерах безопасности» (ст. 17.13) и др.

Анализ показывает, что ответственность за отказ в предоставлении информации предусмотрена не только ст. 5.39 КоАП РФ, но и ст. 140 УК РФ, за отказ в предоставлении гражданину информации предусмотрена уголовная ответственность. Таким образом, приведенный пример свидетельствует о необходимости разграничения административной и уголовной ответственности. Полагаем, что в данном случае разграничение следует проводить по объективной стороне, прежде всего по последствиям правонарушающих деяний. Для состава преступления необходимо, чтобы подобные деяния причинили вред правам и законным интересам граждан. Такая формулировка уголовно-правовых последствий недостаточно четкая и корректная, поскольку неправомерный отказ в предоставлении гражданину информации, образующий состав административного правонарушения, тоже причиняет вред его праву на получение информации.

За последние несколько лет глава 13 КоАП РФ была существенно обновлена, дополнена новыми составами административных правонарушений. С 1 июля 2017 г. было введено семь новых составов правонарушений в ст. 13.11 (вместо одного ранее). Суть данных новелл сводится к тому, что штрафы за нарушения порядка обработки персональных данных стали крупнее, а диспозиция нарушений, за которые назначается ответственность, – более конкретной.

Указанные изменения, внесенные в главу «Административные правонарушения в области связи и информации», свидетельствуют о том, что сохраняется тренд усиления на государственном уровне жесткости административных наказаний; законодатель реагирует на изменения в обществе, и меры административной ответственности за правонарушения в области связи и информации постоянно находятся в развитии.

С появлением объектов критической информационной инфраструктуры Российской Федерации, вслед за уголовной ответственностью, установленной в качестве наказания за неправомерное воздействие на такие объекты, нуждается в научных исследованиях вопрос о

целесообразности введения соответствующей статьи и в КоАП РФ. Необходимо продолжать научные исследования информационного права, направленные на изучение общих вопросов ответственности информационной безопасности, субъектов и объектов исследования. Также необходимо активное вовлечение органов государственной власти в части внедрения и разработки новых учебных программ на всех уровнях образовательной системы, что будет способствовать формированию правового фундамента для дальнейших практических шагов в направлении обеспечения информационной безопасности.

Литература

1. Алексеев, С. С. Социальная ценность права в советском обществе / С. С. Алексеев. – М., 1971. – 223 с.

2. Аудитория пользователей интернета в России в 2017 году составила 87 млн. человек. URL: http://2017.russianinternetforum.ru.

3. Братусь, С. Н. Юридическая ответственность и законность / С. Н. Братусь. – М., 1978. – 208 с.

4. Витрук, Н. В. Общая теория юридической ответственности / Н. В. Витрук. – М., 2009. – 432 с.

5. Заседание Совета Безопасности. URL: http://www.kremlin.ru/events/president/news/24.

6. Информационное право: учебник / под ред. И. Л. Бачило. – М.: Издательство Юрайт, 2016. – 419 с.

7. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / под ред. Т. А. Поляковой, А. А. Стрельцовой. – М.: Издательство Юрайт, 2016. – 325 с.

8. Прокси в цепочке. URL: https://xakep.ru/2001/08/24/13400/.

9. Самощенко, И. С. Сущность юридической ответственности в советском обществе / И. С. Самощенко, М. Х. Фарукшин. – М., 1974. – 44 с.

10. Сачков, И. Почему WannaCry оказался опасней других вирусов-шифровальщиков. URL: https://www.group-ib.ru/blog/wanna-cryptor.

11. Яковлев, В. Ф. О понятии правовой ответственности / В. Ф. Яковлев // Журнал российского права. – 2014. – № 1. – С. 5–7.

Полякова Татьяна Анатольевна – доктор юридических наук, главный научный сотрудник, и.о. заведующего сектором информационного права и международной информационной безопасности Института государства и права РАН, г. Москва. E-mail: polyakova_ta@mail.ru.

Савенкова Дарья Дмитриевна – менеджер департамента безопасности Управления противодействия кибермошеничеству ПАО «Сбербанк», г. Москва. E-mail: 5hdd@mail.ru.

Статья поступила в редакцию 7 июня 2018 г.

DOI: 10.14529/law180314

TOPICAL PROBLEMS OF LEGAL RESPONSIBILITY IN THE SPHERE OF PROVIDING INFORMATION SECURITY (CONCEPT, BASIS OF EMERGENCE, TYPES)

T. A. Polyakova,
Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation

D. D. Savenkova
Security Department of Sberbank, Moscow, Russian Federation

The author proposes to define the concept of legal liability, the grounds for the offense and the types of legal responsibility for committing offenses in the field of information security, and considers current issues of law enforcement.

The problem is now becoming ever more relevant and related to the objective processes of mass transition of a significant part of the legal relationship in the digital environment, the trend of "digital transformation" of crime and the vulnerability of ordinary citizens from illegal actions in the digital environment. An analysis of this type of legal responsibility as an administrative one, as well as regulating its norms, has been carried out. It is proposed to improve the regulatory and legal framework, continue research in the field of information law aimed at studying general issues of responsibility in the field of information security.

Keywords: information security, information offenses, cyberattacks, digital development, legal liability, administrative responsibility.

References

1. Alekseev S. S. *Social'naya cennost' prava v sovetskom obshchestve* [Social value of law in Soviet society]. Moscow, 1971, 223 p.

2. *Auditoriya pol'zovatelej interneta v Rossii v 2017 godu sostavila 87 mln. chelovek* [The audience of Internet users in Russia in 2017 amounted to 87 million people]. Available at: http://2017.russianinternetforum.ru.

3. Bratus' S. N. *Yuridicheskaya otvetstvennost' i zakonnost'* [Legal responsibility and legality]. Moscow, 1978, 208 p.

4. Vitruk N. V. *Obshchaya teoriya yuridicheskoj otvetstvennosti* [General theory of legal liability]. Moscow, 2009, 432 p.

5. *Zasedanie Soveta Bezopasnosti* [Security Council meeting]. Available at: http://www.kremlin.ru/events/president/news/55924.

6. Bachilo I. L. *Informacionnoe pravo* [Information law]. Moscow, 2016, 419 p.

7. Polyakova T. A., Strel'cova A. A. *Organizacionnoe i pravovoe obespechenie informacionnoj bezopasnosti* [Organizational and legal support of information security]. Moscow, 2016, 325 p.

8. *Proksi v cepochke* [Chain proxy]. Available at: https://xakep.ru/2001/08/24/13400/.

9. Samoshchenko I. S., Farukshin M. H. *Sushchnost' yuridicheskoj otvetstvennosti v sovetskom obshchestve* [The essence of legal responsibility in the Soviet society]. Moscow, 1974, 44 p.

10. Sachkov I. Pochemu WannaCry okazalsya opasnej drugih virusov-shifroval'shchikov. Available at: https://www.group-ib.ru/blog/wannacryptor.

11. Yakovlev V. F. [On the concept of legal responsibility]. *Zhurnal rossijskogo prava [Journal of Russian law],* 2014, no. 1, pp. 5–7. (in Russ.)

Tatyana Anatolyevna Polyakova – Doctor of Law, chief research officer, acting. Head of the Information Law Branch of the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation. E-mail: polyakova_ta@mail.ru.

Daria Dmitrievna Savenkova – Manager the Security Department of Sberbank, the Division of counter-computer fraud, Moscow, Russian Federation. E-mail: 5hdd@mail.ru.

Received 7 June 2018.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Полякова, Т. А. Актуальные проблемы юридической ответственности в сфере обеспечения информационной безопасности (понятие, основания возникновения, виды) / Т. А. Полякова, Д. Д. Савенкова // Вестник ЮУрГУ. Серия «Право». – 2018. – Т. 18, № 3. – С. 88–94. DOI: 10.14529/law180314.

FOR CITATION

Polyakova T. A., Savenkova D. D. Topical problems of legal responsibility in the sphere of providing information security (concept, basis of emergence, types). *Bulletin of the South Ural State University. Ser. Law*, 2018, vol. 18, no. 3, pp. 88–94. (in Russ.) DOI: 10.14529/law180314.