УДК 343.34
ББК 67.408.13
DOI 10.22394/1682-2358-2018-4-63-71

R.V. Amelin, *Candidate of Sciences (Law), Docent of the Constitutional and Municipal Law Department, Saratov State University named after N.G. Chernyshevsky*

S.E. Channov, *Doctor of Sciences (Law), Professor, Head of the Service and Labor Law Department, Povolzhsky Institute of Management named after P.A. Stolypin, Branch of the Russian Presidential Academy of National Economy and Public Administration*

CRIMINAL AND LEGAL MEANS OF COUNTERACTION TO THREATS ARISING AT USE OF THE STATE INFORMATION SYSTEMS

The existing basis of the criminal legislation, which can be applied to persons guilty of improper functioning of the state information system, is analyzed. The authors come to the conclusion that the current articles of the Criminal Code do not cover all possible cases of damage to protected public relations and propose to supplement the code with new provisions.

Key words and word-combinations: public administration, state information systems, criminal liability, unlawful access, protected information.

Р.В. Амелин, *кандидат юридических наук, доцент кафедры конституционного и муниципального права Саратовского национального исследовательского государственного университета имени Н.Г. Чернышевского (email: alan.asker@gmail.com)*

С.Е. Чаннов, *доктор юридических наук, профессор, заведующий кафедрой служебного и трудового права Поволжского института управления имени П.А. Столыпина — филиала Российской академии народного хозяйства и государственной службы при Президенте РФ (email: sergeychannov@yandex.ru)*

УГОЛОВНО-ПРАВОВЫЕ СРЕДСТВА ПРОТИВОДЕЙСТВИЯ УГРОЗАМ, ВОЗНИКАЮЩИМ ПРИ ИСПОЛЬЗОВАНИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ*

Аннотация. Анализируется база уголовно-правового законодательства, которая может быть применена к лицам, виновным в некорректном функционировании государственных информационных систем. Авторы приходят к выводу о том, что действующие статьи УК РФ не охватывают все возможные случаи причинения ущерба охраняемым общественным отношениям и предлагают дополнить кодекс новыми положениями.

Ключевые слова и словосочетания: государственное управление, государственные информационные системы, уголовная ответственность, неправомерный доступ, охраняемая информация.

* Публикация подготовлена в рамках поддержанного РФФИ научного проекта № 17-03-00082-ОГН.

Государственные информационные системы позволяют значительно повысить эффективность государственного управления в различных сферах за счет упрощения и ускорения принятия решений, возможности обработки и учета значительных массивов данных и другого. Однако как и любое другое явление, использование информационных систем в управлении влечет за собой определенные риски. В частности, они связаны с возможностью возникновения сбоев и ошибок в работе указанных систем, в результате чего управленческие процессы в лучшем случае приостанавливаются, а в худшем начинают идти по неправильному пути.

Ранее уже рассматривался вопрос о правовых последствиях сбоев и ошибок в информационных системах [1; 2]. В целом речь шла о предупреждении непреднамеренных сбоев и ошибок в государственных информационных системах, а также распределении ответственности в тех случаях, когда они все же происходят.

Однако иная с правовой точки зрения ситуация возникает, когда сбой либо ошибка (далее — некорректная работа) являются следствием чьих-либо неправомерных действий — неважно, умышленных или неосторожных. В таком случае реакция правоприменителя должна быть направлена не только на устранение юридических последствий некорректной работы, но и на наказание виновных. Принципиально возможным в такой ситуации представляется применение различных видов юридической ответственности — дисциплинарной, административной, материальной и других. В данной статье речь пойдет лишь о наиболее жестком виде ответственности — уголовной [2].

В действующем УК РФ гл. 28 «Преступления в сфере компьютерной информации» содержит в редакции от 26 июля 2012 г. четыре статьи: ст. 272 «Неправомерный доступ к компьютерной информации»; ст. 273 «Создание, использование и распространение вредоносных компьютерных программ»; ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»; ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Все они в большей или в меньшей степени могут использоваться для противодействия противоправным мерам в отношении государственных информационных систем.

Многие государственные информационные системы в настоящее время используются для ведения различных государственных реестров [3]. В силу этого неправомерное воздействие на подобные государственные информационные системы может быть также наказуемо по статьям: ст. 170 «Регистрация незаконных сделок с недвижимым имуществом»; ст. 170.1 «Фальсификация единого государственного реестра юридических лиц, реестра владельцев ценных бумаг или системы депозитарного учета»; ст. 285.3 «Внесение в единые государственные реестры заведомо недостоверных сведений».

Разумеется, незаконные действия с государственными информационными системами могут повлечь и иные уголовно-правовые последствия. Например,

получение несанкционированного доступа к Единому государственному реестру прав на недвижимое имущество и внесение в него изменений с целью получения прав на чужое недвижимое имущество может быть квалифицировано не только по ст. 170, 272, 273 УК РФ (в зависимости от обстоятельств), но и по ст. 159 «Мошенничество» и даже ст. 159.6 «Мошенничество в сфере компьютерной информации». Применительно к двум последним статьям незаконные действия с государственными информационными системами выступают как средство достижения мошеннических целей. В рамках данной статьи изучим вопросы уголовно-правовой квалификации самих преступных посягательств на указанные системы.

Прежде всего рассмотрим ситуации, когда вмешательство в работу государственной информационной системы совершается с прямым умыслом. К их числу, например, относятся внешний доступ к такой системе («хакерская атака») либо неправомерные действия по отношению к системе лица, имеющего к ней доступ на законных основаниях (оператора системы). В результате подобных незаконных действий возможны различные последствия. Так, лицо, получившее (имеющее) доступ к системе, может внести несанкционированные изменения в ее базу данных (в том числе реестр), изменив, удалив часть из них, либо добавив новые — в зависимости от преследуемой цели.

Например, Д.А. Слепчуков был осужден к лишению свободы по ст. 290 ч. 4 п. "а" УК РФ (за каждое из трех преступлений) на семь лет; ст. 285 ч. 1 УК РФ (за каждое из трех преступлений) на один год; ст. 272 ч. 2 УК РФ (за каждое из 21 преступления) на два года. Занимая должность старшего инженера-программиста <...> УГИБДД при ГУВД <...> и по роду службы выполняющего функции системного администратора базы данных автоматизированной информационно-поисковой системы (АИПС) <...>, в которой хранились сведения о составленных протоколах об административных правонарушениях, сведения о водителях транспортных средств и водительских удостоверений, транспортных средствах, розыске, протоколы изменений и просмотра, имея специальный (полный) допуск администратора базы, дающий ему право производить любые действия в базе данных, в совершенстве зная программу "<...>" (программа для администрирования баз данных "<...>", позволяющая производить любые действия с базой данных), получив деньги и используя свое служебное положение (в отношении П., Ф., Г.), а после увольнения из органов — используя имевшийся доступ к ЭВМ, находящимся в помещении УГИБДД при ГУВД <...>, он произвел незаконные уничтожение либо изменение охраняемой законом служебной информации о совершении ими административного правонарушения и лишения права управления транспортными средствами [4].

Возможны и другие варианты. Например, злоумышленник может не вносить никаких изменений в саму базу данных государственной информационной системы, а изменить программу для работы с этой базой данных таким образом, чтобы при программном обращении к ней информационная система работала некорректно, «не видела» часть информации, содержащейся в базе данных, выдавала ошибки и т.п.

В большинстве случаев указанные действия могут быть квалифицированы по одной из статей гл. 28 УК РФ (а если государственная информационная система используется для ведения единого государственного реестра, то и по соответствующим статьям). В то же время представляется, что действующее российское уголовное законодательство в этой сфере не охватывает все возможные случаи совершения противоправных действий в отношении государственных информационных систем, иногда не позволяя привлечь виновных к ответственности.

Так, если информационная система, в отношении которой были произведены противоправные действия, не используется для ведения единого государственного реестра и, при совершении указанных действий не были затронуты объекты критической информационной инфраструктуры Российской Федерации, виновный может быть привлечен к ответственности по одной из трех статей: 272, 273 и 274 УК РФ.

Статья 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Очевидно, что нарушить правила эксплуатации может лишь тот, кто обязан их соблюдать. Соответственно, субъект преступления, предусмотренного ст. 274 УК РФ, определяется как специальный. Это лицо, которое в силу должностных обязанностей имеет доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию, а также к информационно-телекоммуникационным сетям и обязано соблюдать установленные для них правила эксплуатации [5].

Если же неправомерное воздействие на государственную информационную систему, приведшее к ее некорректной работе, было осуществлено лицом, не наделенным указанными ранее правами и полномочиями, уголовная ответственность для него может наступить лишь по ст. 272 и 273 УК РФ. В судебной практике в большинстве случаев преступные действия квалифицируются одновременно по обоим статьям, поскольку доступ к компьютерной информации извне (в том числе и содержащейся в государственных информационных системах) нередко осуществляется посредством совершения действий, предусмотренных ст. 273 УК РФ. Вместе с тем неправомерный доступ к компьютерной информации может быть получен, например, методами социальной инженерии, не связанными с использованием каких-либо компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации [6]. В таком случае единственным способом наказания лица, получившего доступ к информации, остается ст. 272 УК РФ.

Данная статья в действующей редакции предусматривает уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации. В научной ли-

тературе даются различные трактовки того, что такое «охраняемая законом компьютерная информация» и «неправомерный доступ». Так, судья Верховного Суда Российской Федерации А.С. Червоткин полагает, что «под охраняемой законом информацией понимается информация, для которой установлен специальный режим ее правовой защиты, напр. государственная, служебная и коммерческая тайна, персональные данные, объекты авторского права и смежных прав» [5]. Иными словами, в такой трактовке уголовная ответственность по ст. 272 УК РФ может наступить лишь за неправомерный доступ к компьютерной информации, в отношении которой установлен законом особый режим ее охраны.

Другие ученые полагают, однако, такую позицию неправомерной. По мнению Г.А. Есакова, «информация является охраняемой законом постольку, поскольку лицо не обладает правами доступа к данной информации; характер информации, ее охрана законодательством об авторском праве и смежных правах, законодательством о государственной тайне и т.п. не имеют значения» [7].

Вполне очевидно, что первый подход значительно сужает сферу применения ст. 272 УК РФ. Однако именно он был использован в Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [8]. Согласно официальной позиции надзорного ведомства под охраняемой законом понимается информация, для которой законом установлен специальный режим ее правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т.д.). Неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты.

Конечно, Методические рекомендации Генеральной прокуратуры РФ не являются нормативным документом, тем не менее вполне очевидно, что подчиненные прокуратуры, а вслед за ними и суды ориентируются на них в правоприменительной практике. В результате из сферы уголовно-правового воздействия ст. 272 УК РФ выводятся случаи неправомерного доступа к не охраняемой особым образом компьютерной информации, даже если они повлекли последствия, указанные в ч. 1 этой статьи.

Однако такой подход может создать серьезные проблемы в уголовно-правовой охране государственных информационных систем, поскольку далеко не вся информация, размещаемая в этих системах, является конфиденциальной либо иной, в отношении которой установлены специальные меры именно правовой защиты. Напротив, по общему правилу, информация, содержащаяся в государственных информационных системах, чаще всего является общедоступной и лишь часть ее относится к конфиденциальной либо иной охраняемой. Так, п. 10 Положения о единой государственной информационной системе учета научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения [9] определяет, что сведения, содержащиеся в информационной системе, являются общедоступными, за исключением

информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации. В соответствии с ч. 4 ст. 4 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» «информация, содержащаяся в единой информационной системе в сфере закупок, является общедоступной и предоставляется безвозмездно. Сведения, составляющие государственную тайну, в единой информационной системе не размещаются».

Таким образом, например, лицо, осуществившее неправомерный доступ к информации, содержащейся в единой информационной системе в сфере закупок и осуществившее уничтожение, блокирование, модификацию либо копирование этой информации, согласно позиции Генеральной прокуратуры РФ и ряда ученых (среди которых — судьи Верховного Суда РФ), не может быть привлечено к уголовной ответственности по ст. 272 УК РФ. Кроме того, если оно не использовало при этом компьютерные программы либо иную компьютерную информацию, указанную в ст. 273 УК РФ, и не является спецсубъектом ст. 274 УК РФ, его привлечение за совершенные деяния к уголовной ответственности становится крайне сложным.

По нашему мнению, данная проблема может и должна быть решена на уровне толкования ст. 272 УК РФ официальными государственными органами, путем закрепления позиции, согласно которой под охраняемой законом информацией должна пониматься любая информация, по отношению к которой лицо не наделено правом совершать действия, указанные в ч. 1 ст. 272 УК РФ: уничтожение, блокирование, модификацию либо копирование.

Еще одна проблема уголовной ответственности за неправомерные действия в отношении государственных информационных систем носит, на наш взгляд, более глобальный характер. Ее суть состоит в том, что действующее уголовное законодательство Российской Федерации предусматривает ответственность лишь за вмешательство в функционирование действующих информационных систем. Между тем некорректная работа информационной системы может быть следствием действий, совершенных еще на этапе ее разработки, причем как умышленных, так и неосторожных.

К примеру, на этапе разработки государственной информационной системы технически возможно предусмотреть в программном обеспечении, предназначенном для ее функционирования, различные скрытые возможности, известные лишь разработчикам. В результате после внедрения такой системы она будет функционировать некорректно. Так, система автоматической обработки информации о нарушениях в области безопасности дорожного движения будет игнорировать правонарушения, совершенные транспортными средствами с определенными номерами; система проведения государственных закупок не будет обрабатывать заявки, не отвечающие определенным, указанным в ней признакам, и т.п.

Теоретически данное деяние может квалифицироваться по ст. 273 УК РФ, поскольку фактически разработчик (возможно, в сговоре с государственным заказчиком) осуществляет создание компьютерной программы, заведомо предназначенной для несанкционированного манипулирования информаци-

ей, но на практике возникают сложности. Во-первых, в связи с определением правовой природы созданного продукта (согласно определению, данному в Федеральном законе «Об информации, информационных технологиях и защите информации» государственная информационная система, строго говоря, не является программой для ЭВМ). Во-вторых, государственная информационная система создается и вводится в эксплуатацию на основании нормативного правового акта и все действия с компьютерной информацией, осуществляемые посредством такой системы, де юре являются санкционированными. Поэтому уголовная ответственность именно за разработку таких систем в настоящее время де-факто не предусмотрена.

На наш взгляд, внедрение в государственное управление информационных систем, предоставляющих скрытые преимущества определенным категориям лиц и, соответственно, ущемляющих права других граждан и организаций характеризуется даже большей степенью общественной опасности, чем, например, однократное неправомерное вмешательство в работу действующей государственной информационной системы. Представляется целесообразным дополнить гл. 28 УК РФ специальной статьей, предусматривающей уголовную ответственность за разработку и принятие в эксплуатацию государственной информационной системы, в которую умышленно были внедрены функциональные возможности, заведомо предназначенные для ее некорректного (не в соответствии с требованиями законодательства) функционирования, в случае, если эти действия повлекли существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства.

Субъектами ответственности по данной статье могут выступать различные физические и юридические лица. Помимо разработчика (разработчиков) информационной системы это могут быть должностные лица — представители заказчика (например, если они сами требовали от разработчика подобных изменений), а также третьи лица — если к представителям разработчика обращались они. Разумеется, при всем при этом должна учитываться степень вины каждого из субъектов.

Более сложен вопрос о необходимости установления мер уголовной ответственности за внедрение в эксплуатацию государственных информационных систем, которые работают некорректно не в результате сознательного внедрения в них определенного функционала, а исключительно из-за некачественного выполнения работ по их созданию. Проблема усугубляется тем, что государственный заказчик в большинстве случаев гораздо больше заинтересован в соблюдении сроков разработки, чем в реализации необходимого функционала. Даже если такой функционал предусмотрен в техническом задании на разработку системы, но не реализован должным образом, государственному заказчику может быть проще принять систему, формально исполнив возложенную на него обязанность, а не ввязываться в конфликт с недобросовестным разработчиком, грозящий привести к затягиванию сроков сдачи (а впоследствии объявить конкурс на доработку системы) [10, с. 114].

Примеров, когда в государственное управление внедряются явно недора-

ботанные информационные системы, немало. Именно такая ситуация сложилась, например, с информационной системой «Карта российской науки», разработка которой финансировалась в рамках госпрограммы «Развитие науки и технологий на 2013—2020 годы». На разработку информационной системы на первом этапе было потрачено 90 млн рублей, однако за эти средства был создан продукт, который представитель заказчика — Министерства образования и науки Российской Федерации — мог охарактеризовать лишь следующим образом: «Это макет, это даже не пилотный проект». Однако вместо того, чтобы предъявить обоснованные претензии разработчику, министерство предпочло принять систему в том состоянии, как она была, и затребовать на ее доработку (другим исполнителем) еще 79 млн рублей. В результате ряда доработок к 2017 г. на государственную информационную систему «Карта российской науки» всего было потрачено около 450 млн рублей бюджетных денег. В итоге Совет по науке при Министерстве образования и науки РФ о конкурсе научных проектов, выполняемых в рамках госзадания в подведомственных министерству вузах от 31 января 2017 г., по результатам проведения оценки деятельности работы информационной системы сделал следующее заявление: «При проведении конкурса организаторы получали связанные с проектами наукометрические параметры из так называемой «Карты российской науки». Совет считает, что за четыре года своего существования этот инструмент так и не достиг сколько-нибудь удовлетворительного качества. Значительная часть представляемых «Картой российской науки» сведений ошибочна и не может быть адекватно использована. Совет призывает Минобрнауки не использовать «Карту российской науки» для каких-либо целей» [11; 12].

В принципе, разумеется, общественная опасность ввода в эксплуатацию некорректно функционирующей государственной информационной системы в результате некачественного выполнения работ по ее разработке меньше, чем сознательная разработка информационных систем, со скрытыми функциональными возможностями, не предусмотренными действующим законодательством и техническим заданием на ее разработку. В силу этого в ряде случаев для предотвращения подобных ситуаций может быть достаточно применение мер дисциплинарной ответственности в отношении должностных лиц, осуществивших приемку недоработанной государственной информационной системы. Однако при реализации финансовоемких проектов, по нашему мнению, только дисциплинарная ответственность должностных лиц, государственных органов, ответственных за это, не всегда может достичь цели предотвращения повторения подобных ситуаций в будущем (в том числе из-за коррупционных факторов). Именно поэтому предложенная нами в гл. 28 УК РФ статья, устанавливающая уголовную ответственность за разработку и принятие в эксплуатацию некорректно функционирующих государственных информационных систем, должна распространяться на случаи, когда такие действия были совершены по неосторожности либо с косвенным умыслом, но лишь при наличии такого квалифицирующего признака как причинение крупного ущерба государству.

Библиографический список

1. *Чаннов С.Е.* Ответственность за сбои и ошибки в государственных информационных системах (по материалам судебной практики) // Вестник Поволжского института управления. 2017. № 5. С. 76–82.

2. *Крыжановская А.А.* Гражданско-правовая ответственность за вред, причиненный в связи с использованием сложных программных продуктов. М., 2010.

3. *Чаннов С.Е.* Реестр и информационная система: соотношение понятий // Информационное право. 2017. № 3. С. 4–10.

4. Определение Верховного Суда РФ от 30 янв. 2009 г. № 89-008-88. URL: https://www.zakonrf.info/suddoc/622738e2b53d041c8f82db7b063a8115/

5. Комментарий к Уголовному кодексу Российской Федерации: в 4 т. (постатейный) / А.В. Бриллиантов, А.В. Галахова, В.А. Давыдов [и др.]; отв. ред. В.М. Лебедев. М., 2017. Т. 3: Особенная часть. Раздел IX.

6. *Кабанов А.С., Лось А.Б., Суроев А.В.* Методы социальной инженерии в сфере информационной безопасности и противодействие им // Российский следователь. 2015. № 18. С. 32–37.

7. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. Г.А. Есакова. 7-е изд., перераб. и доп. М., 2017.

8. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) [Электронный ресурс]. Доступ из СПС «КонсультантПлюс».

9. О единой государственной информационной системе учета научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения: постановление Правительства РФ от 12 апр. 2013 г. № 327 (в ред. от 23 янв. 2018 г.). URL: http://www.garant.ru/products/ipo/prime/doc/71762662/

10. *Амелин Р.В.* Правовой режим государственных информационных систем / под ред. С.Е. Чаннова. М., 2016.

11. *Калинина Ю.* На скандальную «Карту российской науки» потратили 450 миллионов рублей. URL: https://www.mk.ru/politics/2018/08/02/na-skandalnuyu-kartu-rossiyskoy-nauki-potratili-450-millionov-rubley.html

12. *Шмырова В.* Загублена информационная система «Карта российской науки» стоимостью 450 миллионов. URL: http://www.cnews.ru/news/top/2018-06-29_minobrnauki_zagubilo_informatsionnuyu_sistemu_za