УДК 34.004
ББК Х06
DOI: 10.14529/law190310

ИНФОРМАЦИОННЫЕ СИСТЕМЫ КАК ИСТОЧНИК ПОВЫШЕННОЙ ОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

В. М. Жернова
Южно-Уральский государственный университет, г. Челябинск

Статья посвящена исследованию необходимости введения новых правовых и технических норм регулирования информационных систем и их последователей – новых объектов правового регулирования – кибер-физических систем. Тема исследования актуальна и находит отражение во многих основополагающих документах развития информационного права в Российской Федерации. Развитие информационных технологий приводит к повсеместной цифровизации и появлению новых объектов и сфер правового регулирования в области информационного права. Так, на сегодняшний момент в законодательстве отсутствуют термин «кибер-физические системы» и, естественно, какие-либо нормы регулирования правовых отношений, возникающих по поводу данных систем. Исследуемый объект является источником повышенной опасности, поскольку отсутствие исследований в данной сфере приводит к ранее не описанным и непредвиденным последствиям, которые должны иметь отражение в нормах технического и правового регулирования.

Ключевые слова: информационные системы, кибер-физические системы, правовое регулирование кибер-физических систем, законодательство в области регулирования информационных систем.

В эпоху индустриальной революции невозможно представить даже наипростейший бытовой процесс, который бы не задействовал информационные системы[1]. Немногим более 10 лет назад, когда Закон об информации, информационных технологиях и о защите информации вступил в силу, информационная система имела вполне четкое определение, под которым понималась «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств». На сегодняшний день, когда основополагающими документами в информационном праве являются Стратегия развития информационного общества (далее – Стратегия) и Доктрина информационной безопасности (далее – Доктрина), когда человечество осознает, что живет в эпоху индустрии 4.0, информационная система стала объектом все новых и новых исследований. И этому способствует ряд правовых и технологических факторов:

– повсеместное использование информационных систем для выполнения различных функциональных процессов;

– сбор, обработка и анализ данных проводится с помощью информационных систем;

– появление новых объектов в информационном праве с развитием информационных технологий является причиной стремительного развития информационного права в части регулирования искусственного интеллекта, робототехники, кибер-физических систем и др.

В связи с этим устоявшееся понимание информационной системы требует дополнения и актуализации, поскольку на данный момент информационная система может представлять собой самостоятельный объект регулирования, выполняющий новые функции, реализация которых приводит к новым правоотношениям, которые ранее не попадали в сферу регулирования информационного права и права в целом, поскольку стали возможны лишь с развитием цифровых технологий и их применением в обществе и промышленности. Неверная работа системы может нанести как моральный вред в виде утечки данных, материальный в виде оценочной стоимости утечки таких данных, так и вред здоровью и жизни человека – в случае реали-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16014 «Место и роль правового регулирования в развитии цифровых технологий, правовое регулирование и саморегулирование, в том числе с учетом особенностей отраслей права».

зации угрозы или неверного функционирования на производстве.

Стратегия констатирует тот необратимый факт, что «информационные и коммуникационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка». Безусловно, хранение и обработка данных в информационных системах должны соответствовать всем существующим правовым и техническим нормам, поскольку зачастую эти данные являются объектом права (речь идет не только о персональных данных, но и об информации, на основании которой может приниматься решение, так называемая «аналитическая информация», которая влияет на важные общественные процессы, и неверное формирование такой информации может привести к необратимым последствиям). Для недопущения подмены, искажения, блокирования, удаления, снятия с каналов связи и иных манипуляций с информацией развитие информационной инфраструктуры Российской Федерации осуществляется на уровне информационных систем и сопутствующих технологий. Но технологии развиваются и в целях повышения эффективности государственного управления, с развитием экономики и социальной сферы создаются новые системы сбора, обработки и хранения данных с использованием различных технологий получения данных – киберфизические системы. К такой системе можно отнести, например, единую биометрическую систему, обеспечивающую информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, включая средства для сбора, обработки и хранения данных, а также методы и алгоритмы, которые позволяют сопоставлять данные с образцами и провести между ними соответствие. Безусловно, нарушение работы такой системы может повлечь утечку данных пользователей, совершение ложных операций, потерю данных и материальных средств и т.д., то есть привести к катастрофе. В связи с этим необходимо вводить требования для предотвращения развития катастрофических действий и для минимизации последствий реализации таких катастроф, а не только требования, предъявляемые к сохранности данных системы. Сюда же можно отнести последствия от неверной работы системы, являющейся кибер-физической системой, и привести следующие примеры:

– смерть от автомобилей с автоматическим управлением (США, штат Аризона) [1];

– крушение вертолета от дрона (без жертв) [4];

– крушение боинга, причиной которого стал отказ системы и невозможность ручного пилотирования [3] и т.д.

В данном случае чрезвычайные ситуации были вызваны отказом работы системы или ее части в результате неверной работы с данными – сбор, получение, анализ информации, а также несоблюдением норм использования такой техники.

Безусловно, несанкционированное распространение данных, содержащихся в различных информационных системах, а также нарушение функциональности хотя бы одной из компонент системы могут привести к катастрофе. К сожалению, в законодательстве недостаточно полно нашел отражение данный вопрос и его возможные пути решения. Многие нормы законодательства направлены на противодействие (минимизацию) уже имеющих место фактов. Например, большая работа проделана в части противодействия вредоносному программному обеспечению – это и лицензирование, и сертификация, и использование только лицензионного программного обеспечения (в том числе противовирусного). Но, как показывает статистика [7], за несколько часов возможно обнаружение десятков новых вредоносных программ. Не каждая из таких программ сможет нанести действительный вред пользователям или организациям, но само по себе количество довольно шокирующее; также согласно статистике число вредоносных программ для атак на устройства Интернета вещей превысило семь тысяч в 2017 году [2]. Поскольку количество устройств, подключаемых к сети Интернета вещей и входящих в кибер-физические системы, экспоненциально увеличивается [6], то количество угроз на один объект также будет увеличиваться. Данный парадокс объясняется экономическим фактором – ведь стоимость защиты системы не должна превышать стоимости хранящихся и обрабатываемых в ней данных. Но в рамках реализации киберфизических систем на первый план выходит

безопасность человека, жизнь которого является высшей ценностью государства. Увеличивается объем законодательных норм, соответствие требованиям различных стандартов, в том числе и первому в России стандарту Интернета вещей [5], при увеличении количества вредоносного программного обеспечения, таким образом, общественность признает тот неочевидный факт, что увеличение норм и требований не спасает информационные системы, и тем более не спасет системы Интернета вещей и кибер-физические системы от влияния вредоносного обеспечения. Сбор информации об угрозах, ошибках – это работа не с ограниченным числом объектов, а с безграничным. Необходимо изменить подход к проектированию, эксплуатации и модернизации информационных систем, киберфизических систем в целях обеспечения их катастрофоустойчивости.

Требования к катастрофоустойчивости информационных систем неявно прослеживаются в некоторых документах, регламентирующих использование информационных систем (в частности, в банковской сфере): к обеспечению бесперебойности осуществления перевода электронных денежных средств операторами электронных денежных средств; одним из важных условий является наличие регламента действий – требования к составлению плана действий и мероприятий в случае наступления катастрофы, а также перечень и периодичность проведения регламентных работ по обеспечению отказоустойчивости. Как видно, опять меры являются постмерами, направленными на снижение негативных последствий.

На наш взгляд, очень важным пунктом в процессе разработки системы является определение перечня функционала, которым обладает данная система. Многие руководящие документы ФСТЭК регламентируют работу с недекларированными возможностями в программном обеспечении. Такие возможности появляются в ходе использования непроверенного программного обеспечения, которое используется изначально либо появляется в результате модернизации. То есть одной из главных задач в части обеспечения катастрофоустойчивости становится написание такого технического задания, которое бы содержало описание всего возможного функционала, реализуемого системой, что свело бы к минимуму появление недекларированных возможностей. С другой стороны, данное решение препятствует задачам масштабируемости, особенно в сфере Интернета вещей. Функционал системы имеет конечное множество возможных состояний – если состояние не описано или неизвестно, тогда это проблема, особенно если нет путей ликвидации (сокращение, минимизация) последствий после наступления такого состояния и наступления неизвестного состояния, что, по большей части, и является наступлением катастрофы.

На сегодняшний день в рамках ГОСТ документов существуют требования к организации площадок для систем, дата-центров и т.д., но эти требования действительны еще со времен СССР. Для катастрофоустойчивых решений информационных и кибер-физических систем необходимо обновить и разработать новые требования именно к физическому устройству системы, поскольку работа с данными – семантической сущностью – системы ведется непрерывно – постоянное обновление закона о персональных данных, появление закона об объектах критической информационной инфраструктуры, где одним из главных принципов обеспечения безопасности критической информационной инфраструктуры является приоритет предотвращения компьютерных атак. Но разве будут в сохранности данные, если физическая целостность системы будет нарушена?

Согласно Доктрине национальным интересом в информационной сфере являются обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации, что является неотъемлемыми компонентами современных систем. Исследователи определяют [8], что с правовой точки зрения решением некоторых вопросов поставленной задачи может являться:

– введение основ законодательства о киберфизических системах, в том числе понятие и классификация таких систем, ответственность, защите данных при использовании их в различных частях системы (как персональные данные, так и данные на основании которых принимается дальнейшее решение).

С другой стороны, необходимы нововведения в части технического регулирования для обеспечения катастрофоустойчивости

информационных систем и кибер-физических систем.

Литература

1. Беспилотный Uber сбил женщину в Аризоне из-за особенностей программы. URL: https://meduza.io/news/2018/05/08/bespilotnyy-uber-sbil-zhenschinu-v-arizone-iz-za-osobennostey-programmy-avtopilot-zametil-ee-no-prodolzhil-dvizhenie.

2. Вредоносная программа (зловред). URL: http://www.tadviser.ru/index.php/.

3. Крушение «Боинга» в Эфиопии. URL: https://www.bbc.com/russian/news-47745048.

4. Первая авиакатастрофа с участием мультикоптера. URL: https://habr.com/ru/post/4102 85/.

5. ПНСТ-2019 «Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала NB-Fi)».

6. Согласно прогнозам, к 2022 году количество подключенных устройств к ИВ составит более 50 млрд. URL: http://www.tadviser.ru/index.php/Интернет_вещей_Internet_of_Things_(IoT).

7. Список вирусов в антивирусной базе. URL: https://updates.drweb.com/.

8. Незнамов, А. В.Стратегия регулирования робототехники и киберфизических систем / А. В. Незнамов, В. Б. Наумов. URL: https://urfac.ru/?p=63.

Жернова Влада Михайловна – кандидат юридических наук, доцент кафедры защиты информации, Южно-Уральский государственный университет, г. Челябинск. E-mail: zhernovavm@susu.ru.

Статья поступила в редакцию 24 мая 2019 г.

DOI: 10.14529/law190310

INFORMATION SYSTEMS AS A SOURCE OF INCREASED DANGER IN DIGITALIZATION CONDITIONS

V. M. Zhernova
South Ural State University, Chelyabinsk, Russian Federation

The article is devoted to the study of the need to introduce new legal and technical regulations for the regulation of information systems and their followers – new objects of legal regulation – cyber-physical systems. The topic of the research is relevant and is reflected in many fundamental documents of the development of information law in the Russian Federation. The development of information technology leads to widespread digitalization and the emergence of new objects and areas of legal regulation in the field of information law. So, at the moment, the term “cyber-physical systems” is missing in the legislation, and there are any norms regulating legal relations arising in connection with these systems. The object under study is a source of increased danger, since the lack of research in this area leads to previously undescribed and unintended consequences, which should be reflected in the norms of technical and legal regulation.

Keywords: information systems, cyber-physical systems, legal regulation of cyber-physical systems, legislation in the field of information systems regulation.

References

1. *Bespilotnyj Uber sbil zhenshhinu v Arizone iz-za osobennostej programmy* [Unmanned Uber shot down a woman in Arizona because of the features of the program] Available at: meduza.io/news/2018/05/08/bespilotnyy-uber-sbil-zhenschinu-v-arizone-iz-za-osobennostey-programmy-avto-pilot-zametil-ee-no-prodolzhil-dvizhenie.

2. *Vredonosnaja programma (zlovred)* [Malicious software (malware)]. Available at: www.tadviser.ru/index.php/Stat'ja:Vredonosnaja_programma_(zlovred).

3. *Krushenie "Boinga" v Jefiopii* [Boeing wreck in Ethiopia]. Available at: www.bbc.com/russian/news-47745048

4. *Pervaja aviakatastrofa s uchastiem mul'tikoptera* [The first crash involving a multicopter]. Available at: habr.com/ru/post/410285//

5. *PNST-2019 «Informacionnye tehnologii. Internet veshhej. Protokol besprovodnoj peredachi dannyh na osnove uzkopolosnoj moduljacii radiosignala NB-Fi)»* [PNST-2019 «Information Technologies. Internet of things. Wireless data transmission protocol based on narrowband modulation of the radio signal NB-Fi)»].

6. *Soglasno prognozam, k 2022 godu kolichestvo podkljuchennyh ustrojstv k IV sostavit bolee 50 mlrd* [According to forecasts, by 2022 the number of connected devices to the IoT will be more than 50 billion.]. Available at:
www.tadviser.ru/index.php/Internet_veshhej_Internet_of_Things_(IoT)

7. *Spisok virusov v antivirusnoj baze* [List of viruses in the anti-virus database]. Available at: updates.drweb.com/.

8. Neznamov A. V., Naumov V. B. *Strategija regulirovanija robototehniki i kiberfizicheskih sistem* [Regulation strategy for robotics and cyber-physical systems]. Available at: urfac.ru/?p=63.

Vlada Mikhailovna Zhernova – Candidate of Sciences (Law), Associate Professor of Information Security Department, South Ural State University, Chelyabinsk, Russian Federation. E-mail: zhernovavm@susu.ru.

Received 24 May 2019.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Жернова, В. М. Информационные системы как источник повышенной опасности в условиях цифровизации / В. М. Жернова // Вестник ЮУрГУ. Серия «Право». – 2019. – Т. 19, № 3. – С. 67–71. DOI: 10.14529/law190310.

FOR CITATION

Zhernova V. M. Information systems as a source of increased danger in digitalization conditions. *Bulletin of the South Ural State University. Ser. Law*, 2019, vol. 19, no. 3, pp. 67–71. (in Russ.) DOI: 10.14529/law190310.