УДК 343.46
ББК Х408.14
DOI: 10.14529/law200418

ПРОБЛЕМЫ ПРАВОВОГО ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ НА КИБЕР-ФИЗИЧЕСКИЕ СИСТЕМЫ

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

Повсеместное использование кибер-физических систем требует ответственного отношения к их проектированию и эксплуатации как со стороны разработчиков, так и со стороны обслуживающего персонала. Ошибки в работе людей, чья деятельность связана с кибер-физическими системами, способствуют увеличению числа кибератак на них. Отсутствие норм об ответственности в отношении возможности создания и реализации кибератак позволяет злоумышленникам наносить ущерб работе кибер-физических систем. Отсутствие достаточных норм регулирования в сфере создания программного обеспечения является одной из наиболее актуальных проблем при регулировании деятельности, связанной с кибер-физическими системами. В статье поднимаются вопросы и предлагаются меры по минимизации последствий от кибератак на кибер-физические системы.

Ключевые слова: кибератаки, кибер-физические системы, ответственность, искусственный интеллект.

Развитие цифровых технологий, применение кибер-физических систем (далее – КФС) и использование искусственного интеллекта приводят к повышению уровня жизни отдельных групп населения, экономическому росту ряда сфер экономики и в то же время способствуют прекращению функционирования ряда направлений деятельности, где преимущественно используется физический труд[1]. Новейшие технологии призваны обеспечить человечество всем необходимым, в том числе и обеспечить безопасность личности, общества и государства. Одной из разновидностей технологий, активно внедряемых в ряде сфер общественной жизни, являются КФС. На сегодняшний день трудно представить не только производство, но и бытовую жизнь человека без них. Их безопасное функционирование сегодня обеспечивается не только техническими, организационными и физическими средствами. Государством ставится активная задача по внедрению правовых средств, в первую очередь в сфере противодействия киберугрозам в отношении КФС [5].

Кибер-физические системы с точки зрения существующей системы объектов информационной среды представляют собой сложные информационные системы, декомпозиционный анализ которых позволяет изучить правовую природу не только объекта в целом, но и отдельных компонентов. Так, неотъемлемым компонентом КФС является программное обеспечение (программы для ЭВМ, базы данных). Сложность анализа программного обеспечения в данном случае заключается в том, что в КФС происходят двунаправленные информационные процессы, получающие и обрабатывающие информацию, а также формирующие ответные действия системы на основании полученной информации зачастую без участия человека. Поэтому так важно обратить внимание на специальное правовое регулирование отношений по созданию, использованию программного обеспечения КФС, которое порождает такие процессы.

Сложная организация исследуемого объекта может являться причиной возникновения некоторых видов уязвимостей, характерных для таких групп объектов, как информационные системы, распределенные базы данных, сеть Интернет и др. Также это приводит к возможности реализации множества соответствующих угроз. Инциденты информационной безопасности становятся неотъемлемой частью функционирования КФС [4]. Чаще всего целью злоумышленников выступают так называемые кибер-компоненты, то есть часть КФС, ответственная за прием и передачу данных (прежде всего различные интерфейсы), а также обработка и хранение информации. Именно эта часть КФС и представляет наибольший инте-

[1] Работа выполнена при финансовой поддержке Совета по грантам Президента Российской Федерации (грант МД-2209.2020.6) «Развитие системы правовых средств обеспечения кибербезопасности в Российской Федерации».

рес с точки зрения правового обеспечения противодействия кибератакам на нее [1].

Применение КФС в различных сферах жизнедеятельности человека влечет разнообразные риски, к которым можно отнести риск физической целостности человека, риск нарушения неприкосновенности частной жизни, риск неправомерного доступа, модификации или удаления информации, риск повышения электронных отходов и др. Самым актуальным на данный момент, по нашему мнению, является риск кибератак, реализация которого может привести к утечке данных, нарушению работы оборудования или его полной остановке и т.д. Возможность реализация кибератак происходит в том числе и из-за несовершенства программного обеспечения КФС. Также стоит отметить, что риск-ориентированный подход к формированию среды регулирования различных объектов, в том числе и КФС, только набирает обороты в России, в отличие от ряда западных стран [2].

Так, за рубежом сегодня принимаются документы, направленные на правовое регулирование использования искусственного интеллекта (далее – ИИ) в обеспечении кибербезопасности. Перед государствами стоит ряд задач как по решению отдельных, наиболее актуальных вопросов, связанных с применением ИИ и робототехники, так и по глобальному определению перспектив системного анализа и регулирования использования ИИ в различных сферах общественной жизни, а также необходимости обеспечения системы безопасности личности, общества и государства от возможных угроз выхода ИИ из-под контроля человека [6, 7, 8].

В последние два года в России принят ряд стратегических документов, направленных на регулирование технологий ИИ, в том числе КФС, например, Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г., утвержденная распоряжением Правительства РФ от 19 августа 2020 г. № 2129-р. Можно констатировать, что происходит попытка регулирования технологий ИИ, но нет регулирования базиса, основы ИИ – программного обеспечения. При этом очень часто законодатель не может четко определить предметную сферу регулирования отношений в сфере программного обеспечения, ограничиваясь преимущественно гражданско-правовым регулированием имущественного оборота программ для ЭВМ и баз данных. В то же время необходимо различать, с одной стороны, регулирование отношений в части неверно работающей статической программы, в которой можно выявить ошибку стандартными методами тестирования, исправить и перезапустить; с другой стороны, регулирование КФС с элементами ИИ, где исход работы не предсказуем, а, следовательно, не составляет возможности определить степень причиняемого вреда и юридическую ответственность.

Отдельные вопросы, связанные с проектированием, использованием и выводом из эксплуатации, обеспечением безопасности компонентов КФС, сегодня регулируются в рамках информационного законодательства, и норм иных отраслей законодательства. Так, на КФС распространяются общие требования к информационным системам и информационным технологиям, которые предъявляются Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации), Гражданским кодексом РФ, Уголовным кодексом РФ, Кодексом РФ об административных правонарушениях, Федеральным законом «О коммерческой тайне», Федеральным законом «О персональных данных» и др.

В Российской Федерации, на наш взгляд, регулирование в сфере программного обеспечения, в том числе и для КФС, является недостаточным по целому ряду направлений: вопросы использования ИИ, программ для ЭВМ при использовании больших данных, нейронных сетей, вопросы распределения юридической ответственности между разработчиками, пользователями и иными субъектами, связанными с программами для ЭВМ, и др. Кроме того, понятие «программное обеспечение» не закреплено в законодательстве. Имеется только понятие «программа для ЭВМ», которое в рамках применения в КФС не в полной мере отражает сущность «киберчасти» КФС. Возможно, вследствие того, что основные концептуальные документы в сфере робототехники и ИИ направлены на регулирование самих технологий, не уделяется достаточное внимание базовым объектам и процессам, таким как программное обеспечение для КФС, разработка, тестирование, внедрение, эксплуатация и модернизация программного обеспечения, в том числе в рамках КФС.

Действующее законодательство также направлено на противодействие созданию и применению вредоносных программ, то есть таких

программ, выполнение которых намеренно приносит ущерб субъектам – производителю лицензионного продукта, владельцам различных файлов и т.д. В таких случаях легко определить круг лиц, вступающих в отношения, возможно подсчитать реальную сумму ущерба.

Программное обеспечение для КФС специфично и ново для российского законодательства, поскольку довольно затруднительно, а порой и невозможно подсчитать потенциальный риск от нарушения прав при его использовании или определить виновных субъектов. Во многом в связи с этим сегодня столь распространены кибератаки. Они обусловлены также рядом непреднамеренных ошибок в программном обеспечении КФС или ошибок, специально разрабатываемых программистами. Сегодня руководящие документы Федеральной службы по техническому и экспортному контролю РФ устанавливают классификацию программного обеспечения по уровню контроля отсутствия в нем недекларированных возможностей, но они применяются только к информационным системам, содержащим информацию ограниченного доступа, что подтверждается, например, руководящим документом «Защита от несанкционированного доступа к информации», утвержденным решением председателя Государственной технической комиссии при Президенте РФ от 4 июня 1999 г. № 114.

Ответственность за разработку программного обеспечение для КФС должны нести не только разработчики и программисты. После разработки программное обеспечение тестируется специальной командой тестировщиков, цель которых и есть выявление ошибок или недекларированных возможностей. Особую часть в формировании распределения ответственности составляет тот факт, является ли программное обеспечение свободно распространяемым или нет.

Одним из основных препятствий для успешного формирования института ответственности в данной сфере является то, что устройство, дефект которого причинил ущерб, может считаться не физическим объектом, а услугой. Другая сторона вопроса заключается в том, следует ли интерпретировать понятие объекта как включающее программное обеспечение, или то, должно ли последнее квалифицироваться как услуга без элемента встраивания в материальный продукт. Эта неопределенность представляет собой серьезную проблему, поскольку технологически продвинутые приложения часто отображают как программное обеспечение и аппаратные элементы, которые тесно связаны в своем функционировании (например, как в случае подключенные и автоматизированные решения для вождения, где функции автономного вождения представляют собой новаторский аспект приложения, отличающий его от традиционных автомобилей), в то время как в других случаях полагаются [2].

Использование программного обеспечения зачастую сопровождается принятием лицензионного соглашения, правовой режим которого не вполне ясен. Согласно соглашению с конечным пользователем предоставляется программное обеспечение, и оно обычно имеет своей целью освободить поставщика или разработчика от любой ответственности. Разработчики и поставщики программного обеспечения используют лицензионные соглашения по ряду причин. Типичное лицензионное соглашение с конечным пользователем предусматривает неисключительный характер лицензии, цель и срок ее предоставления, а также возможность или невозможность передачи ее другим лицам. При этом большинство лицензионных соглашений содержит оговорки, направленные на ограничение или исключение ответственности поставщика или разработчика [3].

Возможны ситуации, когда происходит разделение обязанностей, и за разработку и обслуживание системы отвечают различные люди и организации, которые могут вложить недекларированные возможности. Ответственность же в данном случае должен нести разработчик программ, как лицо, заложившее в нее такие возможности и осознававшее то, что в дальнейшем она будет запущена в работу. При этом, впрочем, крайне проблемно будет выявить и доказать факт незнания оператором указанных особенностей работы программ и сетей, поскольку такие программные особенности могут быть достоверно выявлены только в изначальной или декомпилированной версии программы [9].

В связи с использованием ИИ возможны проблемы адаптации его действий к требованиям конкретных ситуаций, а также сбои в алгоритмах обучения, что тоже может повлечь за собой последствия, исход которых не был указан в спецификации программы. В данном случае со всей очевидностью при квалификации необходимо будет исключить

прямой умысел в отношении таких «дополнительных» последствий: в зависимости от осознания возможности их наступления и принимаемых по этому поводу мер вина может быть выражена в форме косвенного умысла либо в форме неосторожности по причине легкомыслия или небрежности [9].

Требуется чрезвычайно ответственное отношение разработчиков, проектировщиков и производителей программного обеспечения для КФС. Ответственность должна быть направлена на выполнение ими своих обязанностей и обеспечения безопасного функционирования КФС.

Кроме введения ответственности за разработку программного обеспечения для КФС, необходимо предусмотреть ответственность за ненадлежащее обслуживание и сопровождение систем. Также следует учесть, что пользователи своими умышленными или неумышленными действиями могут привести к нежелательным последствиями работы КФС.

Нарушение работы программного обеспечения нередко становится целью злоумышленников. Разделяют два вида программного обеспечения:

1) обеспечивающее функционирование самой сети КФС – программное обеспечение отвечает за обработку событий, логику;

2) отвечающее за интерактивное взаимодействие с пользователем посредством командного языка. Оно, как правило, используется для внешнего или удаленного управления устройствами.

На выбор программного обеспечения для работы с КФС и ее компонентами пользователь зачастую повлиять никак не может, привязан к единственному варианту, поэтому правильным будет знать об уязвимостях такого программного обеспечения. Кроме того, пользователь также должен придерживаться норм, содержащихся в инструкциях и иных технических документах, устанавливающих порядок работы с КФС, чтобы не повлечь своими действиями нежелательных последствий.

Существующее законодательство в сфере КФС направлено лишь на защиту компьютерных систем, а также информацию в них (чаще всего, если это персональные данные или иная информация ограниченного доступа). Важно развивать нормативное регулирование в части охраны не только компьютерной составляющей, но и всех компонентов КФС. Отсутствие таких норм является фактором, существенно сдерживающим развитие КФС, обусловливает во многом их информационную уязвимость перед кибератаками.

Литература

1. Singh, Ajeet & Jain, Anurag. (2018). Study of Cyber Attacks on Cyber-Physical System. SSRN Electronic Journal. DOI: 10.2139/ssrn.3170288.

2. Bertolini A. Artificial Intelligence and Civil Liability / European Union. – Brussels, 2020, 136 p.

3. Moore R. The consumer rights bill and software liability: an evolution or revolution? Law journal of the Higher school of economics: annual review. 2013, pp. 46–52.

4. Ogie R. I. Cyber Security Incidents on Critical Infrastructure and Industrial Networks ICCAE '17. Proceedings of the 9th International Conference on Computer and Automation Engineering, 2017, pp. 254–258.

5. Минбалеев, А. В. Доктрина информационной безопасности Российской Федерации: современное состояние и перспективы развития / А. В. Минбалеев // Вестник УрФО. Безопасность в информационной сфере. – 2016. – № 3 (21). – С. 62–66.

6. Минбалеев, А. В. Проблемы регулирования искусственного интеллекта / А. В. Минбалеев // Вестник Южно-Уральского государственного университета. Серия: Право. – 2018. – Т. 18. – № 4. – С. 82–87.

7. Минбалеев, А. В. Трансформация регулирования цифровых отношений / А. В. Минбалеев // Вестник Университета имени О. Е. Кутафина – 2019. – № 12 (64). – С. 31–36.

8. Минбалеев, А. В. Регулирование использования искусственного интеллекта в России / А. В. Минбалеев // Информационное право. – 2020. – № 1. – С. 36–39.

9. Тирранен, В. А. Преступления с использованием искусственного интеллекта / В. А. Тирранен // Развитие территорий. – 2019. – № 3 (17). – С. 10–13.

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 17 октября 2020 г.

DOI: 10.14529/law200418

PROBLEMS OF LEGAL COUNTERACTION TO CYBER ATTACKS ON CYBER-PHYSICAL SYSTEMS

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

The widespread use of cyber-physical systems requires a responsible attitude to their design and operation, both on the part of developers and on the part of maintenance personnel. Errors in the work of people whose activities are related to cyber-physical systems contribute to an increase in the number of cyber attacks against them. The lack of liability norms regarding the possibility of creating and implementing cyber attacks allows attackers to damage the operation of cyber-physical systems. The lack of sufficient regulation in the field of software development is one of the most pressing problems in the regulation of activities related to cyber-physical systems. The article raises questions and proposes measures to minimize the consequences of cyber attacks on cyber-physical systems.

Keywords: cyber attacks, cyber-physical systems, responsibility, artificial intelligence.

References

1. Singh, Ajeet & Jain, Anurag. (2018). Study of Cyber Attacks on Cyber-Physical System. SSRN Electronic Journal. DOI: 10.2139/ssrn.3170288.

2. Bertolini A. Artificial Intelligence and Civil Liability / European Union. – Brussels, 2020, 136 p.

3. Moore R. The consumer rights bill and software liability: an evolution or revolution? Law journal of the Higher school of economics: annual review. 2013, pp. 46–52.

4. Ogie R. I. Cyber Security Incidents on Critical Infrastructure and Industrial Networks ICCAE '17. Proceedings of the 9th International Conference on Computer and Automation Engineering, 2017, pp. 254–258.

5. Minbaleyev A. V. [The information security doctrine of the Russian Federation: current state and development prospects]. *Vestnik UrFO. Bezopasnost' v informatsionnoy sfere [Bulletin Of The Ural Federal District. Security in the information sphere]*, 2016, no. 3 (21), pp. 62–66. (in Russ.)

6. Minbaleyev A. V. [Regulatory problems of artificial intelligence]. *Vestnik YUzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Pravo [Bulletin of the South Ural State University. Series Law]*, 2018, Vol. 18, no. 4, pp. 82–87. (in Russ.)

7. Minbaleyev A. V. [Transformation of the regulation of digital relations]. *Vestnik Universiteta imeni O. E. Kutafina (MGYUA) [Bulletin of the University named after O. E. Kutafin (MSAL)]*, 2019, no. 12 (64), pp. 31–36. (in Russ.)

8. Minbaleyev A. V. [Regulation of the use of artificial intelligence in Russia]. *Informatsionnoye pravo [Information law]*, 2020, no. 1, pp. 36–39. (in Russ.)

9. Tirranen V. A. [Crimes with the use of artificial intelligence]. *Razvitiye territoriy [Development of territories]*, 2019, no. 3 (17), pp. 10–13. (in Russ.)

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 17 October 2020.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Жернова, В. М. Проблемы правового противодействия кибератакам на кибер-физические системы / В. М. Жернова // Вестник ЮУрГУ. Серия «Право». – 2020. – Т. 20, № 4. – С. 104–108. DOI: 10.14529/law200418.

FOR CITATION

Zhernova V. M. Problems of legal counteraction to cyber attacks on cyber-physical systems. *Bulletin of the South Ural State University. Ser. Law*, 2020, vol. 20, no. 4, pp. 104–108. (in Russ.) DOI: 10.14529/law200418.