Правовое регулирование противодействия кибертерроризму в условиях четвертой промышленной революции Legal Regulation of Countering Cyberterrorism in the Context of the Fourth Industrial Revolution

Н. Г. Жаворонкова,
заведующий кафедрой
экологического и природоресурсного права
Московского государственного юридического университета имени О.Е. Кутафина (МГЮА),
доктор юридических наук, профессор
javoron49@mail.ru

Ю. Г. Шпаковский,
профессор кафедры
экологического и природоресурсного права
Московского государственного юридического университета имени О.Е. Кутафина (МГЮА),
доктор юридических наук, профессор
yurii-rags@yandex.ru

N. G. Zavoronkova,
Doctor of Law, Associate professor,
Head of Ecological and
Natural Resources Law Department
of the Kutafin Moscow State Law University (MSAL)

Y. G. Shpakovskii,
Doctor of Law, Professor of the
Ecological and Natural Resources Law Department
of the Kutafin Moscow State Law University (MSAL)

© Н. Г. Жаворонкова, Ю. Г. Шпаковский, 2020

Аннотация. Проблема обеспечения кибербезопасности в условиях ускоренного внедрения цифровых технологий в деятельности систем государственного управления и бизнеса является актуальной. Авторами показано, что разработка и внедрение цифровых технологий в России должны проводиться с учетом необходимости обеспечения национальной безопасности.

Ключевые слова: цифровая экономика, цифровизация, национальная безопасность, чрезвычайные ситуации, кибертерроризм.

Abstract. The Problem of ensuring cybersecurity in the context of accelerated implementation of digital technologies in the activities of public administration and business systems is relevant. The authors show that the development and implementation of digital technologies in Russia should take into account the need to ensure national security.

Keywords: digital economy, digitalization, national security, emergencies, cyberterrorism.

DOI: 10.17803/2587-9723.2020.3.160-166

Многие страны, в том числе и Россия, считают цифровую экономику ключевым элементом стратегии развития на ближайшие годы. Действительно, распространение нового технологического уклада кардинальным образом меняет всю систему управления глобальными социально-экономическими процессами.

В современном мире стремительное развитие мировых информационных технологий, повсеместное применение методов электронного управления большинством технологических процессов послужило фактором для появления нового вида терроризма — электронного терроризма (кибертерроризма), проявляющегося

в несанкционированном вмешательстве в работу телекоммуникаций, программного обеспечения, изменении компьютерных данных. Эти действия могут вызывать нарушение работы ключевых элементов инфраструктуры государства, экономики и создают опасность для жизни людей, экономического ущерба или иных опасных последствий. Отечественный и зарубежный опыт свидетельствует, что экономический ущерб от таких действий может быть весьма значительным или даже критическим для крупных предприятий и компаний.

Примеров кибератак немало. Достаточно обратиться к событиям весны 2020 г. в России. DDoS-атака на сайт Мэрии Москвы (mos.ru) в апреле 2020 г. шла в том числе из-за рубежа. Это привело к серьезным сбоям в оформлении электронных пропусков москвичей, которые необходимы для перемещения по столице. По мнению экспертов, атаки на портал Мэрии или попытки его взлома могут быть связаны с попыткой злоумышленниками завладеть данными москвичей или с тем, чтобы дезорганизовать работу Мэрии Москвы¹.

В современном мире создаются объективные условия для роста киберпреступности и кибертерроризма. Это связано с проблемами четвертой промышленной революции. С одной стороны, становится возможным появление частных трансграничных систем управления экономическими, социальными и политическими процессами, затрагивающими национальные интересы государств и их объединений. Основу для таких систем обеспечивают глобальные социально-информационные, торгово-информационные сети и криптовалюты, интернет вещей и прочие обезличенные информационные средства совершения транзакций, выводящие международную торговлю и финансы за пределы национальных юрисдикций. С другой стороны, появляются новые возможности тотального контроля в глобальном масштабе².

Выход один — внедрять инновации с осторожностью, поскольку любая технология представляет собой риск с точки зрения кибербезопасности.

В настоящее время в Государственной Думе рассматривается законопроект об экспериментальном правовом режиме для внедрения технологий искусственного интеллекта в Москве³. Законопроект предусматривает проведение в Москве эксперимента по установлению с 1 июля 2020 г. специального правового режима «в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта,

а также последующего использования результатов его применения». Условия, требования, порядок разработки, создания, внедрения и реализации технологий искусственного интеллекта, а также механизм обработки обезличенных персональных данных будут регламентироваться Правительством Москвы. Цель эксперимента — кардинально упростить условия для компаний — разработчиков искусственного интеллекта и установить понятные и четкие правила развития технологий на его основе. Искусственный интеллект легко работает с огромными массивами данных, в том числе помогая принимать решения и освобождая людей от рутинных задач. При этом многие аспекты применения технологии сегодня законодательно не урегулированы. Учитывая, что искусственный интеллект способен к самообучению и делает это быстрее, чем человек, скорость появления новых цифровых решений будет только увеличиваться.

Москва выбрана для проведения эксперимента как лидер по внедрению высоких технологий в России, так как внедрение искусственного интеллекта происходит во многих сферах: с его помощью, например, в столице уже тестировали возможность выявления рака легких у пациентов⁴.

В марте-апреле 2020 г. в России, как и во многих странах мира сложилось непростая ситуация в связи с эпидемией коронавируса. Сложность обстановки диктует требования обеспечить в условиях карантинных мероприятий дистанционную работу многих сфер деятельности: образования, экономики, государственного управления и других с использованием элементов искусственного интеллекта.

В чем специалисты видят опасность? У России нет своей собственной элементной базы, ничего не производится отечественного для того, чтобы собирать искусственный интеллект. Россия все закупает у западных партнеров, которые в любой момент могут стать противниками. В этом определенный риск. В России в подавляющем большинстве сфер используются исключительно иностранные программные продукты, в которых может быть скрытно заложена возможность дистанционного отключения. Огромное количество людей в России пользуется устройствами компании «Apple», которая в критический момент может дистанционно заблокировать выпущенные гаджеты. Иностранные компании имеют возможность отслеживать «посещения граждан в социальных сетях», отслеживают даже работу человека

¹ URL: <http://yandex.ru/search/?lr=213&clid=2363721-92&win=419&text>.

² Харичкин И. К. Проблемы обеспечения национальной безопасности в условиях становления цифровой экономики в России // Аллея науки. 2017. № 6 (22).

³ URL: <http://tass.ru/ekonomika/7895645>.

⁴ URL: <http://www.rbc.ru/newspaper/2020/02/10/5e3c44b99a7947e1a97fb230>.

на клавиатуре. Это дает возможность собирать обширные сведения. В условиях эпидемии, при дистанционной работе большинства структур, имеется возможность собирать обширные сведения и данные. Собственно на этом и базируется механизм компьютерного терроризма.

В научной литературе понятие «компьютерный терроризм» («кибертерроризм») рассматривается как использование компьютерных и телекоммуникационных технологий (прежде всего Интернета) в террористических целях. Большинство авторов в понятие «кибертерроризм» вкладывают комплекс незаконных действий в киберпространстве, создающих угрозу государственной безопасности, личности и обществу. Основной целью кибертерроризма является влияние на решение социальных, экономических и политических задач.

Некоторые исследователи выделяют различные способы для совершения кибератак:

- незаконный доступ к засекреченным данным государственного и военного характера, банковским данным и персональной информации;
- нанесение ущерба элементам, составляющим киберпространство, например разрушение энергетических сетей, создание помех, внедрение вирусных программ для разрушения аппаратных средств;
- кража, повреждение, уничтожение важной информации, программных комплексов путем взламывания защиты, распространения компьютерных вирусов;
- раскрытие и шантаж публикацией секретной информации;
- захват защищенных каналов средств массовой информации, преследующий цель дезинформации, демонстрации силы террористов и объявления требований;
- уничтожение, манипулирование линиями связи и т.д.

Особую проблему и обеспокоенность вызывает уязвимость компьютерных систем управления инфраструктурой жизнеобеспечения (транспорт, атомные электростанции, водоснабжение и энергетика), подключенных к Интернету.

За последние несколько лет «цифровой» тренд оказал значительное влияние на мировое развитие. Многие зарубежные компании уверенно идут по пути цифровизации бизнеса. В этом плане для России цифровые технологии абсолютно актуальны как для компаний, так и для страны в целом. Смена парадигмы глобального экономического

развития, переход к очередному технологическому укладу, кардинальная смена организации промышленного производства объективно приведут к формированию экономики, которая откроет новые направления экономического роста, повысит экономическую эффективность производства и расширит возможности потребления, создавая новые сферы экономической деятельности⁵.

Уникальность четвертой промышленной революции (Industry.4.0), заключается не только в темпах развития и широком охвате, но и в растущей гармонизации и интеграции большого количества различных научных дисциплин и открытий. Другими словами, особенность Industry.4.0 — формирование цифровой экономики, нового уклада жизни и новой основы для развития всего общества.

Анализируя изменения, продуцируемые четвертой промышленной революцией, ряд ученых разделяют их на пять критических моментов и последующих состояний: переломный момент, положительный эффект, отрицательный эффект, неопределенный эффект и глубинное изменение в действии. Это свидетельствует о том, что в настоящее время «отсутствует также последовательная, позитивная концепция на глобальном уровне, которая могла бы определить возможности и вызовы четвертой промышленной революции для предотвращения негативной реакции общества на происходящие кардинальные изменения⁶.

Указом Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» определено, что при реализации национальной программы «Цифровая экономика Российской Федерации» необходимо уже к 2024 г. обеспечить создание системы правового регулирования цифровой экономики, основанного на гибком подходе в каждой сфере.

Программой «Цифровая экономика Российской Федерации» к базовым направлениям отнесены нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технических заделов, информационная инфраструктура и информационная безопасность⁷. Основная цель — сформировать новую регуляторную среду, обеспечивающую благоприятный правовой режим для возникновения и развития современных технологий и цифровой экономики, предусматривающую:

- создание постоянно действующего механизма управления изменениями и компетенциями

⁵ Жаворонкова Н. Г., Шпаковский Ю. Г. Экологические и энергетические проблемы четвертой промышленной революции: правовые аспекты // *Lex russica*. 2019. № 10 (155). С. 53—62.

⁶ См., например: Жаворонкова Н. Г., Шпаковский Ю. Г. Экологические и энергетические проблемы четвертой промышленной революции ; Они же. Правовые аспекты обеспечения экологической безопасности топливно-энергетического комплекса современной России // *Нефтяное хозяйство*. 2015. № 8. С. 122—124.

⁷ Распоряжение Правительства РФ от 12 февраля 2019 г. № 195-р.

(знаниями) в области регулирования цифровой экономики;

- снятие ключевых правовых ограничений и создание отдельных правовых институтов, направленных на решение первоочередных задач формирования цифровой экономики;
- формирование комплексного законодательного регулирования отношений, возникающих в связи с развитием цифровой экономики;
- принятие мер, направленных на стимулирование экономической деятельности, связанной с использованием современных технологий, сбором и использованием данных;
- формирование политики по развитию цифровой экономики на территории Евразийского экономического союза, гармонизацию подходов к нормативному правовому регулированию, способствующих развитию цифровой экономики на пространстве Евразийского экономического союза;
- создание методической основы для развития компетенций в области регулирования цифровой экономики.

В рамках реализации Указа Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», в том числе с целью решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством РФ на базе программы «Цифровая экономика Российской Федерации» сформирована национальная программа «Цифровая экономика Российской Федерации», утвержденная протоколом заседания президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам от 4 июня 2019 г.

Национальная программа «Цифровая экономика Российской Федерации» содержит разделы: «Нормативное регулирование цифровой среды», «Кадры для цифровой экономики», «Информационная инфраструктура», «Информационная безопасность», «Цифровые технологии», «Цифровое государственное управление»⁸.

Следует заметить, что повышение цифровизации всех сфер экономики и жизнедеятельности государства объективно предполагает зависимость устойчивости функционирования этих сфер от кибератак.

Кибератаки могут воздействовать на информационное пространство компьютера, в котором находятся сведения, хранятся материалы фи-

зического или виртуального устройства. Атака обычно поражает носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя. Усиление тенденции взаимодействия всех типов инфраструктуры отражает рост потенциально-го числа точек проникновения атак в объекты, ставшие жизненно важными для современного общества.

Один из самых печально известных случаев кибератаки на критическую инфраструктуру за всю историю — это Stuxnet. Предположительно это была согласованная атака американских и израильских спецслужб, направленная на срыв ядерной программы Ирана. Этот случай стал катализатором, который заставил мировую общественность узнать о разновидностях угроз⁹.

В результате подобных атак, помимо всего прочего, могут быть похищены технические характеристики объектов критической инфраструктуры и огромный объем других критически важных данных. Это означает необходимость принятия специальных мер защиты такой инфраструктуры.

Следует заметить, что для экономики любого современного государства характерна высокая зависимость от деятельности ТЭК. И чем экономически более развито государство, тем больше оно зависит от деятельности и надежности функционирования объектов ТЭК. Сложность современных технологических цепочек, их взаимозависимость можно проследить на крупнейших энергетических авариях.

Для Российской Федерации проблемы аварийности ТЭК актуальны. Если в небольших городах, сельских районах нашей страны к проблемам отключения электричества привыкли, особенно в летний период: из-за гроз, ураганов происходят обрывы ЛЭП, то для крупных городов и мегаполисов энергетические аварии — крупная чрезвычайная ситуация.

Наибольшую опасность представляют системные аварии, характеризующиеся выходом из строя объектов критически важных объектов энергетики с серьезными последствиями для населения и объектов экономики (блэкауты). В России самый крупный блэкаут имел место 25 мая 2005 г. в Москве, в результате него была отключена подача электроэнергии не только в столице, но также в Тульской, Калужской и Рязанской областях. Несколько десятков тысяч человек оказались заблокированы в остановившихся поездах московского метро и лифтах, было нарушено железнодорожное

⁸ Паспорт национальной программы «Цифровая экономика Российской Федерации», утвержденный президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам; протокол от 24 декабря 2018 г. № 16; протокол заседания президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9.

⁹ URL: <http://pcpro100.info/samye-krupnye-kiberataki/>.

сообщение, парализована работа многих коммерческих и государственных организаций.

Следует заметить, что за последнее десятилетие в энергосистемах мира произошло более четырех десятков крупных системных аварий.

Причины этих чрезвычайных ситуаций разные, но остается фактом, что инициирование системных аварий вследствие незаконных вмешательств в деятельность объектов ТЭК является вполне возможной реальией сегодняшнего дня¹⁰. С точки зрения кибертерроризма объекты ТЭК являются наиболее важными, так как особенности последствий компьютерных террористических актов на этих объектах состоят в массовом характере поражающего воздействия (в отношении большого числа людей, на значительных территориях), а также возможности наступления многоплановых разрушительных и дестабилизирующих последствий как регионального, так и глобального характера, например инициирование сбоев в работе системы аварийной защиты реактора на АЭС¹¹.

В этой связи важно, что Стратегия национальной безопасности России основным содержанием энергетической безопасности определяет устойчивое обеспечение спроса достаточным количеством энергоносителей стандартного качества, эффективное использование энергоресурсов путем повышения конкурентоспособности отечественных производителей, предотвращение возможного дефицита топливно-энергетических ресурсов, создание стратегических запасов топлива, резервных мощностей и комплектующего оборудования, обеспечение стабильности функционирования систем энерго- и теплоснабжения¹².

На сегодняшний день Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» установил организационные и правовые основы в сфере обеспечения безопасности объектов ТЭК в Российской Федерации, за исключением объектов атомной энергетики, в целях предотвращения актов незаконного вмешательства, определил полномочия федеральных органов государственной власти и органов государственной власти субъектов РФ в указанной сфере.

Важным является анализ зарубежного опыта в рассматриваемой сфере. Так, в США к проблеме кибертерроризма подходят двояко. Его рассматривают как угрозу общественной безопасности

и угрозу национальной безопасности. Для борьбы с угрозой общественной безопасности власти стремятся проводить такую политику, которая позволяет минимизировать общий ущерб от кибертерроризма, где затраты определяются как сумма последствий успешных терактов и ресурсов, необходимых для их предотвращения. Но в борьбе с угрозами национальной безопасности экономические вопросы отходят на второй план. С такими угрозами в США борются системно и на высоком уровне, выделяя для этого столько ресурсов и средств, сколько себе может позволить государство. Реакция США на события «9/11» как раз и есть реакция на угрозу национальной безопасности.

В Китае в борьбе с киберпреступностью используют несколько мер и средств. Так, в 2015 г. были приняты законодательные акты: о национальной безопасности КНР, о безопасности в Интернете, о борьбе с терроризмом. Согласно принятым законодательным актам правительство КНР обеспечивает гарантии по выявлению различных видов террористической информации на просторах Сети. Граждане и общественные организации также вовлечены в борьбу с неправомерными действиями кибертеррористов. Так, например, во время Олимпиады в Пекине 2008 г. была запущена система поощрений граждан за предоставление какой-либо информации о возможных терактах. Также используются специальные технологии, которые помогут фиксировать и вычислять потенциальные угрозы: увеличение числа камер видеонаблюдения, защита критических технологий (производство нефтепродуктов, химически опасных веществ и проч.).

Согласно китайским законам операторы интернет-ресурсов несут ответственность за легитимность информации.

В России в борьбе с кибертерроризмом важное значение имеет организационный механизм выявления этих преступлений. Главная роль в противодействии преступлениям в сфере компьютерной информации отводится ФСБ России и МВД России, в структуре которых имеются специальные подразделения. Так, в интересах противодействия кибертерроризму приказом директора ФСБ России в 2018 г. был создан Национальный координационный центр по компьютерным инцидентам (НКЦКИ)¹³.

¹⁰ Жаворонкова Н. Г., Шпаковский Ю. Г. Конституционно-правовые аспекты обеспечения энергетической безопасности России // Право и государство: теория и практика. 2016. № 1 (133).

¹¹ Шпаковский Ю. Г. Организационно-правовые проблемы обеспечения безопасности и защищенности критически важных объектов // URL: <http://lib.secuteck.ru/articles2/Regandstan/organizatsionno-pravovye-problemy-obespecheniya-bezopasnosti-i-zaschischennosti-kriticheski-vazhnyh-obektov>.

¹² Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации».

¹³ Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам» (зарегистрирован 6 сентября 2018 г. № 52109).

Центр является составной частью сил, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. НКЦКИ, согласно приказу, имеет право направлять уведомления и запросы субъектам критической информационной инфраструктуры, а также другим органам и организациям, в том числе иностранным, по вопросам, связанным с обнаружением, предупреждением и ликвидацией последствий компьютерных атак и реагированием на компьютерные инциденты.

Серьезность кибертеррористической угрозы не может игнорироваться ни Россией, ни другими странами. Комплексная реализация соответствующих мер в России будет способствовать обеспечению международной безопасности от кибертеррористических угроз, а также защите интересов государства, общества, личности. Особенно это актуально сейчас, когда Россия стоит на пороге формирования нового цифрового уклада жизнедеятельности. Внедрение цифровых технологий в сферу безопасности — это процесс необратимый.

В рамках реализации программы цифровой экономики будут меняться характер и структура управленческих процессов в сфере безопасности, какие-то рутинные процедуры будут уходить, заменяться искусственным интеллектом, роботами. Кроме того, генерирование больших объемов информации приводит к появлению большого количества киберрисков. И все возникающие проблемы, такие как нормативное правовое регулирование, требуют скорейшего решения.

По нашему мнению, в этой связи требуют реализации следующие направления:

Разработка и реализация концепции первоочередных мер по совершенствованию правового регулирования в сфере компьютерной безопасности в рамках развития цифровой экономики. Необходимо определить: перечень ключевых действующих правовых ограничений, препятствующих цифровизации в сфере безопасности, и обосновать предложения по их устранению.

Принятие нормативных правовых актов, устраняющих ключевые правовые ограничения в отдельных отраслях законодательства, препятствующие развитию цифровизации сферы безопасно-

сти в рамках цифровой экономики. По мнению В. А. Вайпана, «новая регуляторная среда должна быть нацелена на создание правовых условий для формирования единой цифровой среды доверия, позволяющей обеспечить участников управленческого процесса средствами доверенных цифровых дистанционных коммуникаций»¹⁴. При этом для формирования единой цифровой среды доверия В. А. Вайпан предлагает нормативно закрепить такие вопросы, как удаленное подтверждение личности, правовое признание электронного взаимодействия и др.

Цифровизация управленческой деятельности как в режиме повседневной деятельности, так и в режиме «чрезвычайной ситуации», «чрезвычайного положения». Это потребует перестройки и замены аналоговых (физических) систем сбора и обработки данных об обстановке при чрезвычайной ситуации технологическими системами. В широком смысле — это процесс переноса в цифровую среду функций и деятельности управленческих процессов, ранее выполнявшихся людьми и организациями. Это потребует внесения изменений и дополнений в ряд федеральных законов, а также нормативных правовых актов Правительства РФ, регламентирующих деятельность в области национальной, экономической, информационной, экологической безопасности. В этих законодательных и иных нормативных правовых актах должны найти отражение вопросы формирования современных благоприятных правовых условий для внедрения в управленческий процесс аддитивных технологий, технологий блокчейн, технологий больших данных (big data), технологий Всеобщего интернета («интернета всего», the Internet of Everything), интернета вещей (Internet of Things), технологий виртуальной реальности (virtual reality, VR, искусственная реальность), технологий искусственного интеллекта и др.

В заключение следует отметить, что внедрение технологий цифровой экономики в сферу безопасности — это процесс необратимый. Масштаб и размах происходящих изменений объясняют остроту восприятия дизруптивных инноваций на сегодняшний момент. И это потребует принятия серьезных решений и масштабных программ защиты информационной среды от кибертеррористической угрозы.

¹⁴ Вайпан В. А. Основы правового регулирования цифровой экономики. 6 января 2018 г. // URL: <http://отрасли-права.рф/article/26874>.

БИБЛИОГРАФИЯ

1. Жаворонкова Н. Г., Шпаковский Ю. Г. Конституционно-правовые аспекты обеспечения энергетической безопасности России // Право и государство: теория и практика. — М., 2016. — № 1 (133).
2. Жаворонкова Н. Г., Шпаковский Ю. Г. Новая Доктрина энергетической безопасности России: вопросы стратегического планирования // Проблемы национальной стратегии. — 2019. — № 4.
3. Жаворонкова Н. Г., Шпаковский Ю. Г. Правовые аспекты обеспечения экологической безопасности топливно-энергетического комплекса современной России // Нефтяное хозяйство. — 2015. — № 8. — С. 122—124.
4. Жаворонкова Н. Г., Шпаковский Ю. Г. Правовые проблемы антитеррористической защиты объектов ТЭК современной России // Противодействие терроризму: проблемы XXI века. — 2011. — № 4.
5. Жаворонкова Н. Г., Шпаковский Ю. Г. Цифровизация в сфере экологической безопасности: административно-правовые аспекты // Юрист. — 2019. — № 4.
6. Жаворонкова Н. Г., Шпаковский Ю. Г. Экологические и энергетические проблемы четвертой промышленной революции: правовые аспекты // Lex russica. — 2019. — № 10 (155). — С. 53—62.
7. Степанов О. А. Противодействие кибертерроризму в цифровую эпоху : монография. — М., 2020.
8. Шваб К. Четвертая промышленная революция. — М. : Эксмо, 2016.