

КИБЕРТЕРРОРИЗМ – НОВАЯ И НАИБОЛЕЕ ОПАСНАЯ ФОРМА ТЕРРОРИЗМА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ БЕЛОРУССКОГО ГОСУДАРСТВА

Д. В. Драгун

*студент специальности «Политология» юридического факультета БГУ,
Минск, Беларусь*

Введение. В условиях стремительного развития и внедрения технологий Четвертой промышленной революции цифровизация становится важнейшим условием дальнейшего преобразования общества. Изменения охватывают различные стороны жизни: будь то политика, государственное управление, микро- и макроэкономика, образование, наука или культура.

Особую актуальность данные тенденции приобретают на современном этапе развития белорусского государства. Так, одним из основных направлений внутренней политики Республики Беларусь является обеспечение развития процессов информатизации, которая, согласно Стратегии развития информатизации в Республике Беларусь на 2016-2022 гг., состоит в трансформации сфер человеческой деятельности под воздействием информационно-коммуникационных технологий, включая формирование цифровой экономики, развитие информационного общества и совершенствование электронного правительства Республики Беларусь [1, 2].

Существование данных тенденций отмечал Президент Республики Беларусь в Послании белорусскому народу и Национальному собранию 21 апреля 2017 г.: «... мир не стоит на месте. Нам нужно более активно внедрять информатизацию в сфере бытовых услуг, торговле, жилищно-коммунальном хозяйстве, на транспорте, сокращать бумажный документооборот за счет повсеместного использования технологий электронного правительства» [3].

Потенциал, перспективность и успехи цифровизации белорусского государства отмечены международным IT-сообществом. Согласно исследованию ООН «Электронное правительство 2018: Применение электронного правительства для формирования устойчивого и гибкого общества», в 2018 г. Республика Беларусь заняла 38-е место из 193 стран мира в рейтинге по индексу готовности к электронному правительству. За 2 года Беларусь поднялась на 11 позиций [4].

Вышеизложенное подчеркивает актуальность исследования процессов цифровизации социума под углом зрения политической науки. Особое внимание следует уделять новым рискам, вызовам и угрозам, порождаемым цифровой трансформацией и затрагивающим вопросы обеспечения национальной безопасности, прав, свобод и

законных интересов индивида. В первую очередь речь идет о киберпреступности. В последние годы Управлением по раскрытию преступлений в сфере высоких технологий Министерства внутренних дел Республики Беларусь отмечается взрывообразный рост ее уровня: в 2017 г. было зарегистрировано 3 099 преступлений в сфере высоких технологий, но уже спустя 2 года это число увеличилось втрое и составило 10 539 преступлений, среди них 2 492 – преступления против информационной безопасности государства и общества [5]. Наиболее опасным среди таких киберпреступлений, по моему мнению, следует считать кибертерроризм.

Основная часть. Республика Беларусь является одной из немногих стран, признавших кибертерроризм угрозой информационному суверенитету и информационной безопасности и закрепивших его определение на легальном уровне в Концепции информационной безопасности: кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти, либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка [6].

Кибертерроризм – современное явление. О его существовании впервые было заявлено в конце 80-х годов XX столетия, на заре формирования киберпространства, а первый кибертеррористический акт был совершен 10 лет спустя, 3 июня 1998 г., хактивистской группой Milw0rm, которая парализовала работу Индийского центра атомных исследований, получив доступ к удаленным ресурсам управления инфраструктурой обогащения ядерного топлива.

Но в чем же состоят причины повышенной опасности данной формы терроризма? Ответ на данный вопрос, в том числе, лежит в плоскости выяснения политологических аспектов сущностных характеристик исследуемого явления. Рассмотрим некоторые особенности кибертерроризма, которые в современных реалиях позволяют называть его наиболее опасной формой терроризма.

Во-первых, в силу всеобъемлющей интеграции цифровых технологий в жизнь социума расширяется число критически важных объектов информатизации, деструктивное информационное воздействие на которые способно причинить ущерб национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах, а также создать в

обществе атмосферу страха и дестабилизировать общественный порядок. К таким объектам относятся:

1. Автоматизированные системы управления производством, распределением и потреблением электроэнергии.

2. Общегосударственная автоматизированная информационная система, предназначенная для обеспечения взаимодействия государственных организаций между собой, а также с иными субъектами посредством ресурсов сети Интернет.

3. Автоматизированная информационная система единого расчета и информационного пространства (ЕРИП), информационные системы проведения безналичных (межбанковских) расчетов.

4. Другие критически важные объекты информатизации.

Во-вторых, убытки в результате осуществления кибертеррористических актов причиняются большему числу людей, чем при использовании традиционных террористических методов. Это связано с тем, что удельный вес населения и организаций, использующих сеть Интернет, по данным Национального статистического комитета Республики Беларусь за 2018 г., составляет 79.1 % и 96.7 % соответственно. При этом удельный вес населения, использующего сеть Интернет для осуществления финансовых операций, составляет 32.2 %, а для осуществления взаимодействия с органами государственного управления посредством общегосударственной автоматизированной информационной системы – 13.1 % [7].

В-третьих, кибертерроризм характеризуется большей экономичностью по сравнению с традиционными террористическими методами ведения борьбы. Для подготовки и реализации кибертеррористического акта требуется компьютер и стабильное и быстрое Интернет-соединение, что, как правило, обходится намного дешевле и легче в приобретении традиционных видов вооружения. Кроме того, такой метод борьбы не предполагает гибели нападавшего, как это имеет место с террористами-смертниками.

В-четвертых, кибератаки осуществляются анонимно с помощью различных способов анонимизации в сети Интернет (например, VPN, динамические IP-адреса, асимметричное шифрование и тому подобное), что затрудняет возможность идентификации личности кибертеррориста правоохранными органами.

В-пятых, транснациональный характер киберпространства позволяет осуществлять кибертеррористические акты удаленно, без непосредственного физического контакта с целью. Это создает дополнительные трудности для уголовно-правового преследования кибертеррористов, поскольку в настоящее время действенные

международно-правовые механизмы взаимодействия антитеррористических органов в сфере противодействия кибертерроризму находятся на этапе формирования.

Вышеназванные особенности кибертерроризма приводят к становлению его важным фактором политического процесса и увеличению числа кибертеррористических актов. Кроме того, «традиционные» террористические организации используют возможности сети Интернет для координации своих действий и рекрутирования новых членов из различных социальных слоев населения, в первую очередь – образованной молодежи, поскольку осуществление кибертеррористической деятельности возможно только при наличии специализированных навыков в сфере программирования.

Тем не менее, несмотря на постулируемую сложность противодействия кибертерроризму, в Республике Беларусь предпринимаются действенные шаги по формированию системы обеспечения информационной безопасности. Так, 18 марта 2019 г. была принята Концепция информационной безопасности Республики Беларусь, сформировавшая нормативно-правовой базис системы обеспечения информационной безопасности. В ближайшее время был принят целый ряд законодательных актов, направленных на уточнение и конкретизацию ее положений. Среди таких актов особо отметим Указ Президента от 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации», которым определяются меры по технической и криптографической защите информации, а также критерии отнесения тех или иных объектов инфраструктуры к критически важным объектам информатизации.

Однако, по моему мнению, эффективное противодействие киберпреступности и кибертерроризму исключительно затрудняется, если пользователи сети Интернет пренебрегают базовыми правилами цифровой грамотности. Эта проблема в полной мере характерна и для Республики Беларусь, что отмечается, в том числе, Министерством внутренних дел Республики Беларусь. В связи с этим Управлением по раскрытию преступлений в сфере высоких технологий МВД были разработаны правила информационной безопасности, которые в доступной форме информируют население о необходимости использования надежных паролей, защищенного Wi-Fi-сигнала, верифицированного программного обеспечения. Особое внимание уделяется безопасности банковских карт и финансовых транзакций [8].

В данной контексте представляется необходимым внедрение в учебные программы подготовки специалистов профессионально-технического, средне-специального и высшего образования

специализированных дисциплин, формирующих у обучающихся «цифровые» навыки. В связи с этим отмечу положительный опыт кафедры политологии юридического факультета Белорусского государственного университета по формированию навыков политико-правового позиционирования в условиях цифровизации белорусского государства, осуществляемому, в том числе, посредством преподавания дисциплины «Политика в сфере цифровой трансформации». В рамках данной дисциплины закладываются базовые знания о технологиях, трендах и направлениях политики в сфере цифровой трансформации; зарубежном и отечественном опыте и правовых основах формирования и реализации политики в сфере цифровой трансформации; угрозах, вызовах, рисках и перспективах политики в сфере цифровой трансформации [9, с. 3–6].

Заключение. На современном этапе общественно-политическое, социально-экономическое и научно-технологическое развитие Республики Беларусь неразрывно связано с процессами цифровизации. Потенциал, перспективность и успехи информатизации белорусского государства отмечены международным IT-сообществом. Однако поступательная цифровизация порождает и качественно новые риски, вызовы и угрозы информационной цивилизации.

Наиболее опасной из таких угроз считаю новую форму терроризма – кибертерроризм. Опасность кибертерроризма лежит в самой сущности данного явления: он характеризуется универсальностью – кибератакам так или иначе могут подвергнуться все важнейшие объекты инфраструктуры; широким охватом – 79.1 % физических и 96.7 % юридических лиц являются пользователями сети Интернет; экономичностью – средства осуществления кибератак гораздо бюджетнее классического вооружения; анонимностью – в сети Интернет существует множество способов сокрытия своей личности; удаленностью – для осуществления кибертеррористических актов не требуется физического контакта кибертеррориста с объектом атаки.

Тем не менее, при всей постулируемой опасности кибертерроризма эффективное противодействие ему возможно. Так, в Республике Беларусь полным ходом идет процесс институционализации системы обеспечения информационной безопасности. Однако полноценную работоспособность она проявит лишь при высоком уровне цифровой грамотности населения, с чем в Республике Беларусь наблюдаются определенные проблемы. Для повышения ее уровня считаю необходимым внедрение в учебные программы подготовки специалистов профессионально-технического, средне-специального и высшего образования специализированных дисциплин, формирующих у

обучающихся «цифровые» навыки. Положительный опыт в данной сфере может быть почерпнут у кафедры политологии юридического факультета Белорусского государственного университета, где разработана специализированная дисциплина «Политика в сфере цифровой трансформации», направленная на развитие навыков политико-правового позиционирования в условиях цифровизации белорусского государства.

Библиографические ссылки

1. Стратегия развития информатизации в Республике Беларусь на 2016–2022 годы [Электронный ресурс] : Протокол заседания Президиума Совета Министров Респ. Беларусь, 3 нояб. 2015 г., № 26 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

2. Об утверждении Программы социально-экономического развития Республики Беларусь на 2016–2020 годы [Электронный ресурс] : Указ Президента Респ. Беларусь, 15 дек. 2016 г., № 466 // Нац. правовой Интернет-портал Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2020. URL: <http://www.pravo.by/document/?guid=12551&p0=P31600466&p1=1>. (дата обращения: 13.05.2020).

3. Лукашенко А. Г. Послание белорусскому народу и Национальному собранию, 21 апр. 2017 г. [Электронный ресурс] // Официальный интернет-портал Президента Республики Беларусь. 2017. URL: http://president.gov.by/ru/news_ru/view/ezhegodnoe-poslanie-k-belorusskomu-narodu-i-natsionalnomu-sobraniju-16059/. (дата обращения: 13.05.2020).

4. Исследование ООН: Электронное правительство 2018 / Департамент по экономическим и социальным вопросам Организации Объединенных Наций ; сост.: В. Акваро, М. Бартелеми [и др.]. Нью-Йорк, 2018.

5. Статистика УРПСВТ // Министерство внутренних дел Республики Беларусь [Электронный ресурс]. 2020. URL: <https://www.mvd.gov.by/ru/page/upravlenie-poraskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/statistika-urpsvt>. (дата обращения: 27.03.2020).

6. Об утверждении Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1 : в ред. постановления Совета Безопасности Респ. Беларусь от 18.03.2019 г. // Национальный правовой Интернет-портал Республики Беларусь. URL: <http://www.pravo.by/document/?guid=12551&p0=P219s0001&p1=1>. (дата обращения: 08.04.2020).

7. Информационное общество в Республике Беларусь / под общ. ред. И.В. Медведевой ; Нац. Статистический комитет Респ. Беларусь Минск, 2019.

8. Профилактика киберпреступлений // УВД Могилевского облисполкома [Электронный ресурс]. 2020. URL: <https://mogilev.mvd.gov.by/ru/news/2566>. (дата обращения: 26.03.2020).

9. Политика в сфере цифровой трансформации: учебная программа УВО по учебной дисциплине для специальности 1-23 01 06 «Политология» / Белорус. гос. ун-т ; юрид. фак-т, Кафедра политологии ; сост. Е. М. Ильина. Минск, 2020.