УДК 343.9.01 DOI: 10.37468/2307-1400-2022-1-23-28

КИБЕРТЕРРОРИЗМ КАК ВАЖНЕЙШАЯ УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ И ОСНОВЫ ЕГО ПРЕДУПРЕЖДЕНИЯ

Кобец Петр Николаевич[1]

[1] Всероссийский научно-исследовательский институт МВД России, Москва, Россия

АННОТАЦИЯ

С невероятным мощным развитием телекоммуникационных сетей, которые мы наблюдаем в третьем десятилетии XXI столетия, становится все более распространенным и международный кибертерроризм. В результате этого явления, отдельные лица, или же целые международные террористические группы и организации стремятся благодаря анонимности, которая предоставлена им киберпространством, осуществлять различные виды угроз безо всякой угрозы идентификации этих преступников, их возможного захвата, или же вообще физической ликвидации, как это происходит в случаях устранения реальных, а не виртуальных террористических атак. Сегодня международными террористическими группами, все чаще используют такие инструменты для совершения атак, как DoS и DDoS атаки – отказы в обслуживании, а также и другие преступные методы, среди которых фишинг, онлайн-мошенничество и др. В настоящее время международный кибертерроризм представляет собой серьезную угрозу не только для экономики всего мирового сообщества, но и опасен для различных объектов критической инфраструктуры. В этой связи кибертерроризм имеет самый высокий уровень угрозы национальной безопасности сравнению с другими возможными атаками международных террористов. В этой связи автором предложен комплекс мер, которые необходимо предпринять для предотвращения атак международных кибертеррористов.

Ключевые слова: национальная безопасность, кибертерроризм, противодействие терроризму, информационная безопасность, компьютерная преступность, цифровизации общества, борьба с преступностью, глобализация, правоохранительные органы, международное сотрудничество, право.

CYBERTERRORISM AS THE MOST IMPORTANT THREAT TO THE NATIONAL SECURITY OF THE RUSSIAN FEDERATION AND ITS MAIN WARNINGS

Kobets P. N.[1]

[1] National research institute of Russia ministry of the interior, Moscow, Russia

ABSTRACT

With the incredible and powerful development of telecommunications networks that we are witnessing in the third decade of the 21st century, international cyber-terrorism is also becoming more widespread. As a result of this phenomenon, individuals or entire international terrorist groups and organizations seek, thanks to the anonymity provided to them by cyberspace, to carry out various types of threats without any threat of identifying these criminals, their possible capture, or even physical elimination, as this happens in cases of elimination of real, not virtual, terrorist attacks. Today, international terrorist groups are increasingly using such tools to carry out attacks as DoS and DDoS attacks – denial of service, as well as other criminal methods, including phishing, online fraud, etc. Currently, international cyberterrorism poses a serious threat not only to the economy of the entire world community, but is also dangerous for various critical infrastructure facilities. In this regard, cyberterrorism has the highest level of threat to national security compared to other possible attacks by international terrorists. In this regard, the author proposes a set of measures that must be taken to prevent attacks by international cyberterrorists.

Keywords: national security, cyberterrorism, countering terrorism, information security, computer crime, digitalization of society, crime control, globalization, law enforcement agencies, international cooperation, law.

Приставка кибер происходит от греческого слова кибернан, что означает управлять или контролировать. Следует отметить, что общественный интерес к кибертерроризму возник еще в конце 1990-х гг., когда этот термин был придуман Барри К. Коллином, например, «онлайн-системы создают киберпространство, в котором люди могут общаться друг с другом (по электронной почте), проводить исследования или просто делать покупки в интернет магазине, при этом, как и физическое пространство, киберпространство содержит объекты (файлы, сообщения электронной почты, графику и т. д) и различные способы транспортировки и доставки» [1, p. 15]. «Физический и виртуальный миры по своей сути являются несопоставимыми мирами. Сейчас именно пересечение, конвергенция этих двух миров формирует средство кибертерроризма, новое оружие, с которым мы сталкиваемся» [2, с. 43].

Однако «в отличие от реального пространства, исследование киберпространства не требует никаких физических движений, кроме нажатия клавиш на клавиатуре или перемещения мыши» [3, с. 114]. Вообще-то термин киберпростран-

ство был придуман автором научной фантастики Уильямом Гибсоном в рассказе Горящий хром, а позже использован в его романе Нейромант вышедшем в свет в 1984 г. Данный термин относится к виртуальному миру, созданному внутри компьютера, а также и к телекоммуникационным сетям, к которым он подключен, к так называемой компьютерной реальностью. Кроме того, данный термин включает в себя внутреннюю память компьютера и его коммуникации [4, с. 153].

По мере приближения к 2000-м гг. страх и неуверенность в связи вероятностью атак кибертеррористов только увеличивались. Громкие террористические атаки в начале XXI столетия и «последовавшие за этим войны с терроризмом со стороны всего мирового сообщества привели к постоянному освещению в средствах массовой информации (далее – СМИ) потенциальных угроз кибертерроризма в последующее двадцатилетие» [5, с. 119]. В условиях третьего десятилетия XXI столетия «в основном в различных СМИ часто обсуждается возможность крупной атаки с использованием компьютерных сетей для саботажа критически важных инфраструктур с целью подвергнуть опасности человеческие жизни или вызвать разрушение в национальном масштабе либо напрямую, либо путем подрыва национальной экономики» [6, с. 73].

Анализ различных источников литературы свидетельствует о наличии возможных вероятных сценариев катастроф, которые могут быть вызваны атаками международных кибертеррористов [7, с. 48]. При этом, конечно же встречаются и скептические оценки различных исследователей утверждающих, что сценарии возможных атак кибертеррористов, в частности, на объекты критически важной инфраструктуры, и как следствие ядерные аварии и взрывы на химических заводах и других опасных производствах не могут быть реалистичны. Такие оценки основываются на том, что предсказанные последствия террористических атак не происходят, и поэтому указанные выше критики, безо всякого на то основания, проводимую борьбу с кибертерроризмом называют кибертеррористической шумихой.

В рассматриваемом контексте, подобным экспертам хочется ответить, что напрасно ими ставится под сомнение, как возможные опасности и их последствия, так и вся теория угроз международных кибертеррористов. По большому счету минимизация подобных атак со стороны террористических организаций, объясняется только тем, что правоохранительные службы активно противодействуют всей террористической преступности, предотвращая в том числе и кибертерроризм, и в этой связи нельзя не отметить насколько нам всем повезло, что пока мировое сообщество находится под надежной защитой от потенциальных угроз кибертеррористов на объекты критически важной инфраструктуры [8, с. 19].

Кроме того, несмотря на обширные исследования кибертерроризма, большая часть литературных источников, в силу ряда причин все еще не содержит реалистичной оценки всех его потенциальных угроз. В частности, в «случае кибертеррористической атаки на общественную инфраструктуру» [9, с. 227], такую, как объекты атомной энергетики или же центры по управлению воздушным движением, посредством взлома их компьютерных систем террористами, не делаются конкретные оценки в отношении возможного ущерба и жертвах подобных кибертеррористических атак, поскольку данные о таких террористических акциях, в том числе и потенциальных, имеют ограниченный характер.

С каждым годом мировое сообщество становится все более зависимым от телекоммуникационных сетей и Интернета, эта зависимость растет в мировом масштабе, в том числе создавая прочную основу для дальнейшего развития международного кибертерроризма, которая все активнее реализуется как прямая угроза национальной безопасности нашего государства [10, с. 11]. Для международных кибертеррористов кибер-атаки «имеют явные преимущества перед физическими атаками, поскольку их можно проводить удаленно, анонимно и относительно дешево, и они не требуют значительных вложений в различные виды вооружения» [11, с. 131], набора и подготовки новых рекрутов, взрывчатые вещества или

адептов террористического движения. В следствие проведения актов кибертерроризма эффект может быть просто ошеломляющим.

Сегодня с полной ответственностью можно утверждать о том, что международный кибертерроризм входит в число самых серьезных потенциальных угроз безопасности в мире. Его опасность становится более важной, чем проблематика, связанная с ядерным оружием или различными международными локальными конфликтами. Вследствие широкого и повсеместного распространения Интернета, и различных телекоммуникационных технологий, цифровая террористическая деятельность представляет угрозу для всей экономической или социальной глобальной системы [12, с. 28].

Одними из наиболее серьезных проблем международной кибербезопасности являются DDoS-атаки. Отказ в обслуживании DoS – это метод, с помощью которого кибертеррористы пытаются нарушить нормальную деятельность конкретного хоста (например, веб-сайта, сервера, сети, устройства Интернета вещей и др.), переполняя его интернет-трафиком, также известным как запросы. Общая цель состоит в том, чтобы сделать хост недоступным для законных запросов пользователей и превратить целевую систему в неработоспособную. Распределенный отказ в обслуживании – DDoS добавляет уровень сложности, вводя поток трафика из нескольких источников. Эта крупномасштабная кибертеррористическая деятельность значительно осложняет обстановку и очень затрудняет различение законного пользовательского трафика от вредоносного трафика. В настоящее время ежегодно происходят миллионы атак типа «отказ в обслуживании», а такие перерывы в обслуживании могут стоить сотни тысяч долларов. В сложившейся ситуации чрезвычайно важно поддерживать безопасность и резервирование критически важных систем, чтобы они оставались в сети во время DoS и DDoS атак.

Кроме того, важно отметить, что кибертеррористы обладающие хорошими техническими знаниями могут найти способы доступа к критически важным компьютерным системам и соответственно редактировать учетные записи, переформатировать данные и даже выключать целые системы [13, с. 7]. Высокопрофессиональные компьютерные специалисты в состоянии использовать тактику фишинга, например, они могут звонить в офисы и выдавать себя за технических специалистов для получения паролей для доступа к рассматриваемым системам. Используя комбинации традиционных методов взлома, таких как фишинговые сайты и социальная инженерия кибертеррористы могут взять под контроль номер любого мобильного телефона, убедив оператора назначить номер новому телефону (это известно, как замена SIM-карты) и убедить сотрудников, что он является ИТ-специалистом компании [14, с. 80].

Подобная социальная инженерия позволяет кибертеррористам получать доступ к конфиденциальной информации, которая позволяет в дальнейшем осуществлять террористическую акцию [15, с. 183]. Данная террористическая тактика должна служить предупреждением для государственных организаций и различных частных компаний о том, что кибератаки не всегда совершаются только онлайн. Физическая безопасность доступа к информации может быть столь же важна, как и кибербезопасность. Не стоит забывать о том, что ряд компаний подключены к тысячам отдельных сторонних ресурсов, которые имеют хотя бы одну критическую уязвимость. В сложившейся ситуации им необходимо более эффективно управлять своей сетевой безопасностью выстраивая ее основные приоритеты, при этом постоянно ее совершенствовать, чтобы обеспечить безопасность личных данных и иных важнейших цифровых информационных баз.

Ряд исследований кибертерроризма в период пандемии COVID-19 свидетельствуют о его особенностях [16, с. 179]. Оценки, сделанные специалистами Интерпола относительно воздействия пандемии COVID-19 на рост киберпреступности свидетельствуют о значительном сдвиге целей террористов, которые до этого события, гораздо чащи совершали атаки на частных лиц и

предприятий, а с 2020 г. постепенно стали переходить на атаки в отношении крупных государственных корпораций, правительственных организаций, а также иные критические инфраструктуры. Сделанные экспертами Интерпола выводы свидетельствуют о том, что помимо DoS и DDoS атак «около двух третей стран-членов, которые ответили на глобальный опрос о киберпреступности, сообщили о значительном использовании тем COVID-19 для фишинга и онлайн-мошенничества с момента вспышки пандемии» [17]. Озвученные специалистами Интерпола выводы, также еще раз подчеркнули необходимость более тесного сотрудничества между государственным и частным секторами по борьбе с потенциальными киберугрозами.

Поскольку система Интернет продолжает все больше совершенствоваться и развиваться, а телекоммуникационные системы по-прежнему представляют повышенную опасность в связи с их активным использованием кибертеррористами, становится все более сложным оказывать противодействие этой серьезной угрозе, которая может при определённых обстоятельствах вообще положить конец человечеству. Высоко подготовленные в техническом плане кибертеррористы «имеют гораздо более легкий доступ к незаконному участию в киберпространстве благодаря возможности получить доступ к части Интернета, известной как даркнет» [18, с. 20]. Он представляет из себя «скрытые сети, которые существуют параллельно друг другу и обеспечивают анонимность разными техническими средствами. Например, крупнейшая из них построена на принципах TOR (The Onion Router), или луковой маршрутизации» [19, с. 43]. Указанная выше часть Интернета, на сегодняшний день в плане развития кибертеррористических угроз чрезвычайно опасна, поскольку осуществлением мер предупредительного воздействия кибертерроризма в ней, в силу определенных причин, существенно отличаются от обычной части всем хорошо известного Интернета.

Можно предположить, что развитие телекоммуникационных систем и цифровых технологий, только увеличит вероятность совершения числа случаев кибертерроризма [20, с. 545]. В этой связи следует ожидать, что они будут происходить «с помощью атак типа отказ в обслуживании, вредоносных программ и других методов, которые сегодня нам пока что еще трудно представить, при этом нельзя не отметить, что привлекательность цифрового оружия аналогична привлекательности ядерного потенциала» [21, с. 53], потому, как это один из возможных способ нанесения террористической атаки для террористических групп и организаций не обладающих реальным вооружением, и не имеющих достаточного финансирования.

Во время выступления, сделанного 22 октября 2020 г. на пленарном заседании дискуссионного клуба «Валдай», лидером нашей страны Президентом Российской Федерации В.В. Путиным была высказана позиция о важности безопасной работы в киберпространстве. Им также было отмечено о необходимости помнить, что на нашей планете идет процесс формирования бесконечного цифрового пространства, а население Земли стремится к быстрейшему его освоению. При этом Президент Российской Федерации подчеркнул, что эпидемия COVID – 19 стимулировала дальнейшее совершенствование дистанционных электронных технологий, а коммуникация на основе системы Интернет стала всеобщим достоянием. В этой связи важно, обеспечить бесперебойное и безопасное функционирование не только телекоммуникационной инфраструктуры, но и всего киберпространства [22].

Для эффективного противодействия кибертерроризму, в сложившейся ситуации чрезвычайно важно больше уделять внимания превентивным мерам, которые будут создавать сложности для интернет-атак кибертеррористов, а также стремиться к тому, чтобы вообще их сделать невозможными для выполнения. Важно расширять все необходимые усилия по поддержке субъектов, обслуживающих операционные системы критически важной государственной инфраструктуры, в снижении возможных рисков и угроз осуществимых в отношении них и повышая их кибербезопасности. Необходимо повы-

шать осведомленность операторов обозначенных систем о кибер-рисках и потенциальных уязвимостях, а также о мерах по смягчению последствий, которые необходимо использовать по повышению устойчивости жизненно важных инфраструктурных систем. Важно совершенствовать законодательные меры по борьбе с терроризмом [23, с. 17], в том числе и рассматриваемой сфере. Также следует укреплять потенциал правоохранительных органов по реагированию на киберпреступность [24, с. 5], поддерживая координацию между всеми правоохранительными службами, а также некоторыми международными партнерами, в частности с представителями правоохранительных органов государств – участников СНГ. При этом также следует стремиться к укреплению потенциала правоохранительных органов в сфере раскрытия и расследования киберпреступлений, и иной преступной деятельности международных террористических групп и организаций.

Список литературы

1. *Collin B.* C. The Future of Cyber Terrorism // Crime & Justice International. – 1997. – Vol. 13, No. 2. March. – P. 15-18.
2. *Мазуров В.А.* Кибертерроризм: понятие, проблемы противодействия // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2010. – № 1-1(21). – С. 41-45.
3. *Майоров А.В.* Понятие и структура системы противодействия преступности // Правопорядок: история, теория, практика. – 2014. – № 1(2). – С. 112-116.
4. *Айсханова Е. С.* Причины и мотивы роста киберпреступности как глобального явления современности // Вестник Чеченского государственного университета. – 2017. – № 4(28). – С. 153-155.
5. *Кобец П.Н., Власов Д.В.* Опыт и проблемы борьбы с международным терроризмом // Реформирование государственного управления и местного самоуправления в Российской Федерации: региональный аспект: Сборник статей, Пермь, 06 октября 2006 г. – Пермь: ПРИПИТ, 2006. – С. 117-123.
6. *Кобец П.Н.* О важности рассмотрения на учебных занятиях по криминологии особенностей противодействия экстремизму и терроризму // Активизация деятельности студентов в сфере учебной, научной и общественной жизни образовательного учреждения: Материалы межвузовской научно-практической конференции, Москва, 27 апреля 2006 г. – М.: Московский институт права, 2006. – С. 71-78.
7. *Карпова Д.Н.* Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – № 8. – С. 46-50.
8. *Кобец П.Н.* Противодействие терроризму в информационной сфере: опыт и проблемы // Научный портал МВД России. – 2021. – № 3(55). – С. 18-26.
9. *Мухачев С.В., Баева М.А.* Хакеры как инструмент информационной войны // Новая наука: Проблемы и перспективы. – 2016. – № 115–3. – С. 225-229.
10. *Бегишев И.Р.* Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов // Информационная безопасность регионов. – 2010. – № 1(6). – С. 9-13.
11. *Бураева Л.А.* Мировой опыт противодействия экстремизму и терроризму в глобальном информационном пространстве // Теория и практика общественного развития. – 2015. – № 18. – С. 131-134.
12. *Степанова О.А.* Актуальные проблемы противодействия кибертерроризму: монография. – М.: Акад. Генеральной прокуратуры, 2014. – 99 с.
13. *Услинский Ф.А.* Кибертерроризм в России: его свойства и особенности // Право и кибербезопасность. – 2014. – № 1. – С. 6-11.
14. *Маслакова Е.А.* Кибертерроризм как новая форма терроризма // Наука и практика. – 2015. – № 2(63). – С. 79-81.
15. *Ковлагина Д.А.* Информационный терроризм // Вестник Саратовской государственной юридической академии. – 2013. – № 6(95). – С. 181-184.
16. *Кобец П.Н.* Особенности кибер-преступности в период пандемии COVID-19:

состояние и дальнейший прогноз // Ученые записки Казанского юридического института МВД России. – 2021. – № 2(12). – С. 177-182.

17. INTERPOL report shows alarming rate of cyberattacks during COVID-19 [Электронный ресурс] – Режим доступа: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (дата обращения 15.02.2022).

18. *Майоров А. В.* Правовые основы защиты жертв преступности в России // Виктимология. – 2016. – № 2(8). – С. 16-21.

19. Что такое даркнет, как туда попасть и почему не стоит этого делать [Электронный ресурс] – Режим доступа: https://lifehacker.ru/chto-takoe-darknet/ (дата обращения 15.02.2022).

20. *Белоножкин В.И.* Информационная сущность и структура терроризма // Информация и безопасность. – 2007. – Т. 10. – № 4. – С. 541-546.

21. *Кобец П.Н.* О необходимости совершенствования процесса подготовки специалистов в сфере информационных технологий для противодействия киберпреступности // Прикладные цифровые технологии и системы XXI века: экономика, менеджмент, управление персоналом, информационная безопасность, право: Материалы региональной научно-практической конференции, Владимир, 17 декабря 2021 г. – Владимир: Владимирский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», 2022. – С. 50-55.

22. Путин призвал добиваться бесперебойной и безопасной работы киберпространства [Электронный ресурс] – Режим доступа: https://tass.ru/politika/9790943 (дата обращения 15.02.2022).

23. *Кобец П.Н., Кундетов А.И.* О необходимости совершенствования отечественного законодательства об ответственности за терроризм // Терроризм и экстремизм как угрозы национальной безопасности России: идеологические, социокультурные и правоприменительные аспекты противодействия: XVIII Международная научно-практическая конференция, Нальчик, 23–24 мая 2014 г. – Нальчик: Краснодарский университет МВД России, Северо-Кавказский институт повышения квалификации (филиал), 2015. – С. 15-30.

24. *Федоров А.В., Сергеев Д.Н.* Основные тенденции международного терроризма и меры борьбы с ним // Российский следователь. – 2016. – № 24. – С. 3-9.

Статья поступила в редакцию 17 февраля 2022 г.
Принята к публикации 20 марта 2022 г.

Ссылка для цитирования: Кобец П. Н. Кибертерроризм – как важнейшая угроза национальной безопасности Российской Федерации и основы его предупреждения // Национальная безопасность и стратегическое планирование. 2022. № 1(37). С. 23-28. DOI: https://doi.org/10.37468/2307-1400-2022-1-23-28

Сведения об авторах:

КОБЕЦ ПЕТР НИКОЛАЕВИЧ – *доктор юридических наук, профессор, главный научный сотрудник, Всероссийский научно-исследовательский институт МВД России, г. Москва, Россия*
e-mail: pkobets37@rambler.ru