УДК 342.7

© Дмитрий Игоревич Кузьмин
канд. экон. наук, доцент кафедры правового обеспечения государственного и муниципального управления, Владимирский филиал РАНХиГС

ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ КОНСТИТУЦИОННЫХ ПРАВ ГРАЖДАН ПРИ ПРОТИВОДЕЙСТВИИ КИБЕРТЕРРОРИЗМУ

Аннотация: концепция «чистого» кибертерроризма предполагает, что террористическая деятельность осуществляется полностью (или в первую очередь) в виртуальном мире. Интернет предоставляет много разных способов анонимно встречаться с «единомышленниками» относительно безопасным способом. Таким образом, возможно, что такая среда может способствовать созданию совершенно новых террористических групп, которым не требуются значительные финансовые ресурсы, и участники могут самоорганизоваться быстро и легко с помощью анонимности киберпространства. Именно этот чистый кибертерроризм имеет в виду большинство авторов, когда обсуждают опасности, создаваемые кибертеррористом, в этой связи возникает понимание отсутствия значительных барьеров для самозащиты. С другой стороны, права человека - это те права, которые считаются настолько основополагающими для человеческого достоинства и благополучия, что каждый человек должен обладать этими правами. Ни один актор, даже правительство, не должен нарушать права человека, потому что они являются основополагающими. Права человека не предоставляются правительством или другим учреждением, каждый человек обладает ими с рождения. Права человека являются неотъемлемыми, то есть человек не может их отдать или отобрать. Поэтому в данном исследовании ставится задача выявить соотношение прав человека и средств борьбы с кибертерроризмом.

Annotation. The concept of “pure” cyber terrorism implies that terrorist activity is carried out completely (or primarily) in the virtual world. The Internet provides many different ways to anonymously meet like-minded people in a relatively safe way. Thus, it is possible that such an environment can contribute to the creation of completely new terrorist groups that do not require significant financial resources, and participants can organize themselves quickly and easily with the help of anonymity in cyberspace. It is this pure cyberterrorism that most authors have in mind when discussing the dangers posed by the cyberterrorist, in this regard, there is an understanding of the absence of significant barriers to self-defense. On the other hand, human rights are those rights that are considered so fundamental to human dignity and well-being that every person must have these rights. No actor, not even a government, should violate human rights, because they are fundamental. Human rights are not granted by the government or other institution, each person possesses them from birth. Human rights are inalienable, that is, a person cannot give them away or take them away. Therefore, this study aims to identify the relationship between human rights and means of combating cyberterrorism.

Ключевые слова: гражданин, права, кибертерроризм, Конституция РФ, противодействие.

Keywords: Citizen, rights, cyber-terrorism, Constitution, counteraction.

Возможности и предпочтительная тактика террористических групп развиваются с течением времени. Терроризм носит асимметричный характер, и его история - это одно из

многократных изменений в стратегии нападений, с целью преодолеть существующие силы безопасности.

Потенциальных исполнителей актов кибертерроризма можно разделить на несколько основных групп, из которых наиболее значимыми для данного исследования являются негосударственные террористические организации и национальные кибергруппы [13].

Возможности и угрозы, создаваемые этими группами, оцениваются как характеризуемые различными мотивациями, способностями и приоритетами. Возможно различить три фазы террористических кибервозможностей:

а) обеспечение - онлайн-действия, которые поддерживают операции террористических групп, такие как реклама и пропаганда, вербовка, разведка, тайная связь между членами, а также распространение руководств и ноу-хау [3, 5];

б) разрушительные - онлайн-действия, которые нарушают информационные технологии противников, в том числе активные кибернарушения сетей; распространение вредоносных программ; эксфильтрация цифровой информации; мошенничество (фишинг); атаки типа «отказ в обслуживании» и другие хакерские операции с информационными технологиями [1, 2];

с) деструктивные - кибератаки, которые вызывают физические повреждения или травмы посредством воздействия на системы диспетчерского управления и сбора данных; отключение систем управления и безопасности [4, 8, 9].

Почти все действующие сегодня террористические организации демонстрируют кибервозможности - у них есть свои собственные веб-сайты, учетные записи в социальных сетях, они используют интернет-технологии для общения и упрощения управления операциями.

Деструктивные кибервозможности, вероятно, потребуют от группы обладать более продвинутым набором навыков, специфичных для понимания информационных систем и того, как они взаимодействуют с физическим миром. Как правило, для получения этого уровня кибернавыков требуются технические знания, такие как процесс проектирования или управления соответствующими системами, а также опыт работы в области вычислительной техники и хакерства [6].

Трудно оценить, насколько быстро террористические группы могут приобрести необходимые навыки для осуществления разрушительных кибератак в будущем. Операции по обеспечению национальной безопасности во многих странах направляют значительные ресурсы на предотвращение приобретения террористическими группами новых наступательных возможностей и агрессивное разрушение их достижений и лидерства. Частные корпорации, такие как Facebook, Twitter, Telegram и YouTube, также расширили свои антитеррористические меры, чтобы уменьшить распространение экстремистского контента, доступного в интернете.

Все системы, по сути, уязвимы, но наше понимание этих уязвимостей и способы их устранения или противодействия в значительной степени ограничены изменчивым характером соответствующих технологий. Быстрое развитие цифровой экономики обеспечивает растущую платформу для кибератак от всех типов акторов [10].

Уязвимости могут существовать в аппаратном и программном обеспечении, сетевых протоколах и языках программирования и присутствовать как местно, так и удаленно. Уязвимости, обнаруженные в аппаратных и сетевых протоколах, сложно нивелировать из-за проблем, связанных с обратной совместимостью, и поэтому они могут быть широко масштабируемы. Если язык программирования содержит уязвимость, она может быть

воспроизведена в любом программном обеспечении или системе, написанной с его использованием [11].

Некоторые критические зависимости носят временный характер и не остаются постоянными. Например, стадион является гипотетически ценной целью для кибертерроризма во время события, но не тогда, когда он пуст. Тем не менее атака может быть подготовлена до события и автоматизирована, чтобы произойти в определенное время. Временность, следовательно, работает как для атакующих, так и для защитников.

В распределенной системе, такой как интернет, важно понимать, что многие протоколы зависят от глобально распределенных систем. В мире, где возникновение деструктивного кибертерроризма вызывает серьезную обеспокоенность, роль временного лага необходимо рассматривать в гораздо более коротком периоде. В настоящее время существуют устройства, которые временно имеют решающее значение для безопасности и благополучия граждан.

По этой причине инновационные методы написания как правительственных, так и корпоративных политик безопасности могут позволить сегментировать риск, а не определять его лишь географически.

Инструменты киберпреступности также являются инструментами кибертерроризма, следовательно, потенциальный кибертеррорист может приобретать разнообразные услуги и возможности из даркнета, при этом участники трансфера не будут предупреждены о том, что они собираются участвовать в цепочке поставок при подготовке террористического акта [7].

Однако террористические группы, со своей стороны, могут опасаться использования таких подпольных рынков из-за риска подвергнуться разведывательной деятельности со стороны правоохранительных органов. Таким образом, существуют некоторые аспекты киберпространства, которые способствуют противодействию терроризму, и их использование является важной частью борьбы с растущей угрозой [12, 14].

Закон универсален, он распространяется на всех, и к нему следует относиться одинаково. На языке прав это означает, что каждый человек имеет право обратиться к соответствующим нормам и что они имеют право на равное отношение к другим людям. Это фундаментальные права, потому что они гарантируют, что все остальные права в Конституции РФ будут применяться ко всем универсально и в равной степени. Конституция РФ определяет несколько других прав, связанных с этими основными правами универсальности и равенства. Право быть свободным от дискриминации связано с универсальностью и равенством. В этом праве указывается, что закон или правительство не должны по-разному относиться к человеку в зависимости от его цвета кожи, расы, пола, языка, религии или многих других факторов.

Ландшафт киберпространства разнообразен и сложен. Интернет, существующий сегодня, значительно отличается от того, который может существовать завтра, с точки зрения количества развернутых систем, «безопасных», уязвимых или скомпрометированных. Число действующих лиц, угроз и их рост или снижение неизвестны, а количество инструментов, находящихся в их распоряжении, трудно прогнозируемо и требует много времени для отслеживания и исследования. При этом органы власти должны понимать, что любое противодействие должно быть ограниченно рамками защиты прав и законных интересов граждан, в том или ином статусе оказывающихся вовлеченными в акты кибертерроризма.

Список литературы

1. Батуева Е. В. Виртуальная реальность: концепция угроз информационной безопасности США и её международная составляющая [Электронный ресурс] // Вестник МГИМО. - 2014. - № 3 (36). URL: https://cyberleninka.ru/article/n/virtualnaya-realnost-kontseptsiya-ugroz-

informatsionnoy-bezopasnosti-ssha-i-eyo-mezhdunarodnaya-sostavlyayuschaya (дата обращения: 15.04.2019).
2. Бураева Л. А. Кибертерроризм в молодежной среде [Электронный ресурс] // Бизнес в законе. - 2016. - № 2. URL: https://cyberleninka.ru/article/n/kiberterrorizm-v-molodezhnoy-srede (дата обращения: 15.04.2019).
3. Бураева Л. А. О некоторых вопросах обеспечения кибербезопасности в современных условиях [Электронный ресурс] // Теория и практика общественного развития. - 2015. - № 13. URL: https://cyberleninka.ru/article/n/o-nekotoryh-voprosah-obespecheniya-kiberbezopasnosti-v-sovremennyh-usloviyah (дата обращения: 15.04.2019).
4. Гавло В. К., Мазуров В. А. Уголовно-правовые и криминолого-криминалистические аспекты противодействия терроризму [Электронный ресурс] // Известия АлтГУ. - 2011. - № 2-2. URL: https://cyberleninka.ru/article/n/ugolovno-pravovye-i-kriminologo-kriminalisticheskie-aspekty-protivodeystviya-terrorizmu (дата обращения: 15.04.2019).
5. Галушкин А. А. К вопросу о кибертерроризме и киберпреступности // Вестник РУДН. Серия «Юридические науки». - 2014. - № 2. URL: https://cyberleninka.ru/article/n/k-voprosu-o-kiberterrorizme-i-kiberprestupnosti (дата обращения: 15.04.2019).
6. Диденко А. И. Противодействие кибертерроризму [Электронный ресурс] // Отечественная юриспруденция. - 2016. - № 11 (13). URL: https://cyberleninka.ru/article/n/protivodeystvie-kiberterrorizmu (дата обращения: 15.04.2019).
7. Зинченко Ю. П., Шайгерова Л. А., Шилко Р. С. Психологическая безопасность личности и общества в современном информационном пространстве [Электронный ресурс] // Национальный психологический журнал. - 2011. - № 2. URL: https://cyberleninka.ru/article/n/psihologicheskaya-bezopasnost-lichnosti-i-obschestva-v-sovremennom-informatsionnom-prostranstve (дата обращения: 15.04.2019).
8. Капитонова Е. А. Особенности кибертерроризма как новой разновидности террористического акта [Электронный ресурс] // Известия вузов. Поволжский регион. Общественные науки. - 2015. - № 2 (34). URL: https://cyberleninka.ru/article/n/osobennosti-kiberterrorizma-kak-novoy-raznovidnosti-terroristicheskogo-akta (дата обращения: 15.04.2019).
9. Карамова Э. И., Фомин С. М. К вопросу о кибертерроризме в глобализирующемся мире [Электронный ресурс] // Социально-политические науки. - 2016. - № 3. URL: https://cyberleninka.ru/article/n/k-voprosu-o-kiberterrorizme-v-globaliziruyuschemsya-mire (дата обращения: 15.04.2019).
10. Кошечкина Е. А. К вопросу о проблемах противодействия кибертерроризму [Электронный ресурс] // ОНВ. ОИС. - 2017. - № 4. URL: https://cyberleninka.ru/article/n/k-voprosu-o-problemah-protivodeystviya-kiberterrorizmu (дата обращения: 15.04.2019).
11. Мазуров В. А. Кибертерроризм: понятие, проблемы противодействия [Электронный ресурс] // Доклады ТУСУР. - 2010. - № 1-1 (21). URL: https://cyberleninka.ru/article/n/kiberterrorizm-ponyatie-problemy-protivodeystviya (дата обращения: 15.04.2019).
12. Мороз Н. О. Международно-правовая квалификация кибертерроризма [Электронный ресурс] // Вестник Марийского государственного университета. Серия «Исторические науки. Юридические науки». - 2016. - № 2 (6). URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovaya-kvalifikatsiya-kiberterrorizma (дата обращения: 15.04.2019).
13. Фарвазова Ю. Р. Актуальные аспекты совершенствования правового регулирования незаконного использования информационного пространства в террористических целях

[Электронный ресурс] // Армия и общество. - 2013. - № 5 (37). URL: https://cyberleninka.ru/article/n/aktualnye-aspekty-sovershenstvovaniya-pravovogo-regulirovaniya-nezakonnogo-ispolzovaniya-informatsionnogo-prostranstva-v (дата обращения: 15.04.2019).
14. Чжэн И Сотрудничество РФ и КНР в борьбе с кибертерроризмом [Электронный ресурс] // Вестник МГОУ. - 2018. - № 2. URL: https://cyberleninka.ru/article/n/sotrudnichestvo-rf-i-knr-v-borbe-s-kiberterrorizmom (дата обращения: 15.04.2019).