ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 323.283

КИБЕРТЕРРОРИЗМ КАК ОДНА ИЗ УГРОЗ СОВРЕМЕННОМУ МИРУ

София Сергеевна Чепец
Студентка Московского государственного юридического университета имени О.Е. Кутафина
chepecsofa2001@yandex.ru

Аннотация

Наряду с технологиями развиваются и новые виды преступлений. Интернет - огромное цифровое поле для нового вида террористической деятельности - кибертерроризма. Автор приводит примеры такого рода преступлений, оценивает масштабы опасности кибертерроризма, анализирует его законодательное закрепление и выявляет возможные пути предупреждения и противодействия.

Ключевые слова: кибертерроризм, террористическая деятельность, государство, Интернет, социальные сети, экстремизм, информационные технологии.

CYBERTERRORISM AS ONE OF THE DANGER TO THE MODERN WORLD

Sofia S. Chepets
Student of the Kutafin Moscow State Law University

ABSTRACT

Along with technology, new types of crime are also developing. The Internet is a huge digital field for a new type of terrorist activity - cyber terrorism. The author gives examples of such crimes, evaluates the scale of the danger of cyberterrorism, analyzes its legislative consolidation and identifies possible ways to prevent and counteract.

Keywords: cyberterrorism, terrorist activities, state, Internet, social networks, extremism, information technology.

В сети, при всех ее плюсах и полезности, рождается уязвимость общественных и государственных интересов. Это выражается в активном использовании Интернета для организации массовых погромов, беспорядков, хакерских атак и киберпреступлений. Новые технологии – новое поле для терроризма. Только теперь еще и цифрового.

Целью данного исследования является определение масштабов опасности такого нового вида террористической деятельности, как кибертерроризм, сравнение показателей преступлений террористической направленности, совершаемых с помощью цифровых технологий за 2018-2019 гг., анализ способов регулирования кибертерроризма с

юридической точки зрения и выявление возможных путей предупреждения и противодействия этого рода преступлений.

Под самим кибертерроризмом следует понимать экстремистские атаки на компьютерную информацию, вычислительные системы, аппаратуру передачи данных, иные составляющие информационной инфраструктуры, которые совершаются определенными лицами или группами. Они проникают в атакуемые системы и, перехватывая управление, осуществляют деструктивные воздействия [5].

Социальные сети и технологии используются террористами для планирования и пропаганды терактов, и так как преступники отдают себе отчет в немалой уязвимости социальных сетей, они осуществляют свою деятельность в основном на закрытых платформах и каналах. Они предпринимают все возможные меры для защиты от спецслужб: экстремисты тщательно, в несколько этапов фильтруют всех желающих присоединиться.

За последние семь лет количество преступлений с использованием IT-технологий возросло более чем в двадцать раз [7]. Интернет, как пространство, не имеющее границ, и как средство коммуникации огромного количества людей, является идеальной средой для преступной деятельности и активно используется международными террористическими организациями для решения широкого круга задач. Это и распространение экстремистской идеологии, и радикализация потенциальных сторонников, подстрекательство, привлечение и вербовка отдельных лиц, финансирование терроризма, обучение и подготовка экстремистов, планирование и организация терактов [7].

Опасность цифрового терроризма заключается в том, что в связи с новизной такого вида террористической деятельности его угроза не может быть однозначно оценена, развитие нельзя спрогнозировать, он не имеет никаких сдерживающих рамок и набирает обороты параллельно развитию технологий. Главная цель террористов – привлечь как можно больше людей, транслировать свои идеи в общество насколько это возможно. А цифровые технологии и Интернет – идеальное поле для этого. Распространенными способами цифрового терроризма является хищение данных из баз, взлом и искусственная перегрузка сервисов, внедрение вирусов, захват каналов с целью транслирования своей информации. Примером может послужить прошлогодняя ситуация, суть которой состояла в массовой рассылке с зарубежного сервиса писем властям нескольких российских регионов с угрозами минирования государственных учреждений.

Такого рода хакерство может использоваться и для развязывания межгосударственных войн и конфликтов. Так, в апреле 2007 года, на фоне обострения отношений между Россией и Эстонией из-за переноса военных захоронений, хакеры взломали сайты практически всех государственных органов, банков, вследствие чего их работа приостановилась на две недели, а все следы, благодаря стараниям хакеров, указывали на Москву и даже на IP-адрес Кремля.

Стоит заметить, что в Российской Федерации за январь - декабрь 2019 г. было зарегистрировано 1 806 преступлений террористического характера, что на 7,6% больше, чем в 2018 г. Из общего числа около 15% совершены с использованием компьютерных и телекоммуникационных технологий. По сравнению с 2018 г. количество указанных преступлений увеличилось на 68,5% [6].

Несколько лет назад имела место череда взломов российских сайтов хакерами-исламистами. Террористы закрывали некоторые разделы сайтов, опубликовывая вместо важной информации в этих разделах пропагандистские лозунги и оскорбления

политических деятелей. Такого рода деятельность вполне может использоваться для получения опыта и последующей атаки сайтов органов власти и государственных корпораций.

На данный момент единственным правовым актом, затрагивающим вопросы регулирования цифрового терроризма, является Конвенция о преступности в сфере компьютерной информации, принятая Советом Европы в 2001 году. [1] Но данный акт охватывает недостаточный на сегодняшний день объем компьютерных преступлений и уделяет большее внимание вторжению в компьютерные системы, перехвату данных и т.д., не уделяя внимания совершению этих действий в экстремистских целях. За 19 лет появилось множество новых технологий, услуг и значительно расширилось киберпространство. Именно поэтому конвенция не может эффективно регулировать развитие кибертерроризма. [3]

В российском уголовном законодательстве отсутствует понятие «кибертерроризм». Уголовная ответственность за совершение террористического акта предусмотрена статьей 205 УК РФ, но квалифицирующего признака, связанного с совершением преступления в киберпространстве, российское уголовное законодательство не предусматривает. Однако в Уголовном кодексе содержится статья, предусматривающая ответственность за совершение деяния, максимально приближенного по смыслу к понятию «кибертеррakt» — статья 274.1 УК РФ о неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации. Данное преступление направленно на прерывание критически важных процессов, протекающих в медицинских и научных учреждениях, банках, шахтах, различных заводах, стратегических объектах и т.д. Введен в действие Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также создан орган ГосСОПКА (глобальная система сбора и обмена информацией о компьютерных атаках на территории РФ, за ее создание отвечает 8-й центр ФСБ). Государство пытается максимально обезопасить критически важные объекты инфраструктуры и граждан от любых проявлений терроризма. [4]

Можно прийти к выводу, что цифровые технологии помогают экстремистам в реализации задуманных планов, которые перетекают в кибертерроризм как реальную угрозу для отдельных стран и всего мирового сообщества, а высокотехнологичные теракты в состоянии породить проблемы мирового масштаба. [8] И для того, чтобы этого не допустить, необходимо выработать существенные меры предупреждения и предотвращения. Киберпреступность – это особая преступность, для предупреждения и противодействия которой требуется создание специальных подразделений.

Экономически развитые государства вырабатывают систему противодействия кибертерроризму. Например, Пентагон планирует возможные превентивные кибератаки для защиты американских стратегических интересов, КНР осуществляет разработку правового документа для определения мер осуждения и наказания за хакерство, а в Израиле создано специальное подразделение по борьбе с кибертерроризмом в целях отражения кибератак, которые могут парализовать системы жизнеобеспечения страны. [2]

Для решения проблем борьбы с киберпреступностью странам необходимо объединяться, как, например, в апреле 2012 г., когда проводилось совещание в Астане стран-членов Шанхайской организации сотрудничества, где был подписан Протокол о сотрудничестве, который определил основные направления взаимодействия МВД России и министерств общественной безопасности стран ШОС на ближайшую перспективу, а также были определены меры по борьбе с преступностью в сфере информационных технологий и противоправного пользования интернетом. В борьбе с использованием Интернета в

террористических целях интересен опыт разведки МИ-6 из Великобритании. Британская разведка взломала один из сайтов террористической группировки «Аль-Каида». Вместо инструкций по сбору самодельной бомбы сотрудники МИ-6 разместили рецепт приготовления пирожных.

Такой вид терроризма приносит ущерб, исчисляемый триллионами. Но, самое страшное, что террористы, развиваясь, могут получать доступ к управлению транспортом, оружием массового уничтожения, секретным данным и прочим объектам, захват которых приведет к катастрофам и смерти сотен, тысяч и даже миллионов людей.

Для противодействия этой большой опасности требуется сотрудничество всех государств на высшем уровне, совершенствование законодательства, как национального, так и международного, создание специальных международных организаций, целью которых будет являться поиск и реализация путей, способов и средств ее решения. Конечно, в первую очередь необходимо бороться с любой преступностью в реальном мире. Тогда злоумышленников станет меньше и в виртуальном пространстве.

Список литературы

1. «Конвенция о преступности в сфере компьютерной информации» от 23.11.2001 (с изм. от 28.01.2003). Будапешт.
2. Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая: Дис. ... канд. полит. Наук. - М. - 2015. - 207 с.
3. Чернядьева Н.А. О международных подходах правового регулирования борьбы с кибертерроризмом // Информационное право. 2016. № 2. С. 26 - 29.
4. Гончаров А.М. Противодействие кибертерроризму [Электронный ресурс]/ Гончаров А.М. - RTM Group, 2020. Режим доступа: https://rtmtech.ru/articles/protivodejstvie-kiberterrorizmu/ (дата обращения 23.11.2020).
5. Журавель В. П. Зарубежное военное обозрение. - 2018. №5. С. 12-15.
6. Состояние преступности в Российской Федерации за январь - декабрь 2019 года// МВД России ФКУ «Главный информационно-аналитический центр». М. - 2019.
7. URL: https://rg.ru/2020/10/20/v-sovbeze-rf-prognoziruiut-sereznuiu-aktivizaciiu-terroristov.html - В Совбезе РФ прогнозируют серьезную активизацию террористов - «Российская газета» №237 от 20.10.2020 (дата обращения 23.11.2020).
8. Максимов С. Кибертерроризм приравняли к оружию массового поражения [Электронный ресурс]/ Максимов С. – «ИнфоШОС», 2010. Режим доступа: URL: http://www.infoshos.ru/ru/?idn=7168 (дата обращения: 28.11.2020).

References

1. «Convention on Crime in the Field of Computer Information», 23.11.2001 (as amended on 28.01.2003). Budapest.
2. Batueva E.V. American concept of threats to information security and its international political component: Dis. Cand. polit. Science. - M. - 2015 . - 207p.
3. Chernyadyeva N.A. On international approaches to legal regulation of the fight against cyber terrorism // Information law. 2016. №2. P. 26 - 29.
4. Goncharov A.M. Countering cyber terrorism [Electronic resource]/ Goncharov A.M. - RTM Group, 2020. Access mode: https://rtmtech.ru/articles/protivodejstvie-kiberterrorizmu (date of access 23.11.2020).
5. Zhuravel V.P. Foreign military review. 2018. №. 5. P. 12-15.

6. The state of crime in the Russian Federation in January - December 2019 // Ministry of Internal Affairs of Russia PKU «Main information and analytical center». M. - 2019.
7. URL: https://rg.ru/2020/10/20/v-sovbeze-rf-prognoziruiut-sereznuiu-aktivizaciiu-terroristov - The Security Council of the Russian Federation predicts a serious activation of terrorists – «Rossiyskaya Gazeta» №. 237 of 20.10.2020 (date of access 23.11.2020).
8. Maksimov S. Cyberterrorism was equated to a weapon of mass destruction [Electronic resource] / Maksimov S. – «InfoSCO», 2010. Access mode: URL: http://www.infoshos.ru/ru/?idn=7168 (date of access: 28.11.2020).