УДК 355/359:004

КИБЕРБЕЗОПАСНОСТЬ КАК ФАКТОР СОХРАНЕНИЯ СУВЕРЕНИТЕТА СТРАНЫ

[1]Юмашев Д.В., [2]Задворная Е.В., [1]Юмашева Е.В.

[1]Краснодарское высшее военное училище им. генерала армии С.М. Штеменко, Краснодар, e-mail: denisumashev@bk.ru;

[2]Кубанский государственный университет, Краснодар, e-mail: lifeislove1989@mail.ru

В статье рассмотрен особый вид террористической деятельности – кибертерроризм как глобальная проблема современности. Авторы исследуют способы применения интернета в качестве средства распространения информации, пропаганды террористических действий, сбора сведений и вербовки и т. д. Возрастающие масштабы использования террористами киберпространства вызывает необходимость создания механизмов противодействия международным угрозам. Подняты вопросы отсутствия единых путей решения существующей проблемы со стороны руководителей разных стран. В целях сохранения суверенитета стран неприемлемо применение двойных стандартов, политизация террористической деятельности, использование экстремистов для достижения сиюминутных геополитических корыстных задач. Авторами предлагаются рекомендации по объединению совместных усилий и выработке единых подходов по антитеррористической борьбе в области сетевой безопасности. Разногласия в политической сфере не должны стать преградой в разработке эффективных мер для решения транснациональной проблемы.

Ключевые слова: террористические атаки, кибертерроризм, IT-преступления, компьютерные атаки

CYBER SECURITY AS THE FACTOR OF PRESERVATION OF THE COUNTRY'S SOVEREIGNTY

[1]Yumashev D.V., [2]Zadvornaya E.V., [1]Yumasheva E.V.

[1]Krasnodar Higher Military School. General of the Army S.M. Shtemenko, Krasnodar, e-mail: denisumashev@bk.ru;

[2]Kuban State University, Krasnodar, e-mail: lifeislove1989@mail.ru

The article considers a special kind of terrorist activity – cyber terrorism as a global problem of the present. The authors examine the ways in which the Internet is used as a means of disseminating information, propagating terrorist activities, collecting information and recruiting, etc. The increasing use of cyberspace by terrorists calls for the creation of mechanisms to counter international threats. The issues of the absence of common ways of solving the existing problem on the part of the leaders of different countries were raised. In order to preserve the sovereignty of countries, it is unacceptable to use double standards, politicize terrorist activities, use extremists to achieve immediate geopolitical self-interest. The authors offer recommendations on combining joint efforts and developing common approaches to the antiterrorist struggle in the field of network security. Disagreements in the political sphere should not become an obstacle in the development of effective measures to solve the transnational problem.

Keywords: terrorist attacks, cyberterrorism. IT crimes, computer attacks

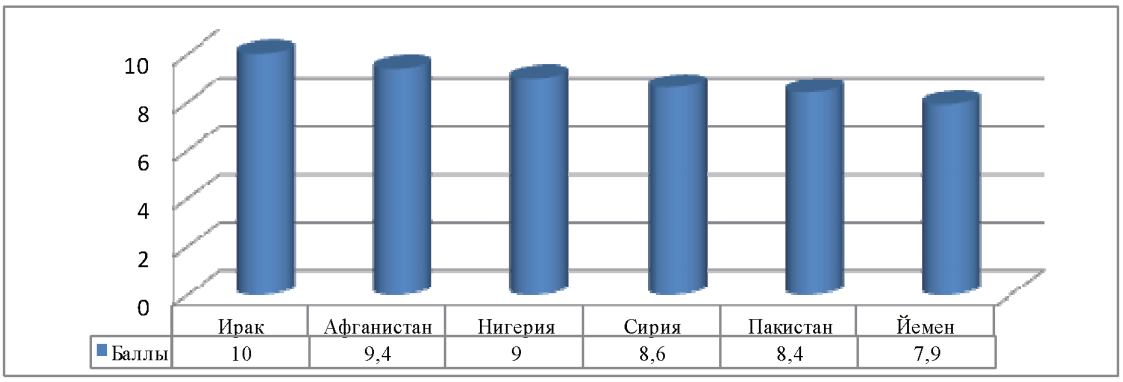
Современный мир сталкивается с угрозами экономического, социального, экологического, информационного и военного характера, международным терроризмом, экстремизмом, сепаратизмом, и т. д.

Терроризм в последнее время занимает главенствующие позиции в современной реальности. На нашей Планете еженедельно происходят акты террора. Хакеры ИГИЛ взламывают аккаунты социальных сетей Министерства обороны США; растет конфликт традиционной исламской и современной постхристианской культур в Европе; медиа с российским участием становятся мишенями в полномасштабной информационной войне на Украине и это лишь отдельные примеры.

Лондонский Институт экономики и мира совместно с Университетом Мэриленда 15 ноября обнародовали Отчет о состоянии глобального терроризма в 2017 году (The Global Terrorism Index 2017) [1].

Международные эксперты рейтинг страны по уровню терроризма оценивают по количеству терактов, размеру материального ущерба, числу пострадавших и погибших. Рейтинг возглавляют шесть государств с наивысшим уровнем влияния терроризма на жизнь, представленные на рисунок.

К странам с высоким уровнем терроризма относятся Сомали, Индия, Турция, Ливия, Египет, Судан, Украина и другие. Среди западноевропейских государств наибольшая террористическая активность наблюдается во Франции (6 баллов и 23-е место). Соединенные Штаты Америки занимают 32–е место (5,4 балла), Россия – 33-е (5,3 балла), Великобритания – 35-е (5,1 балла) [1].



Государства с наивысшим уровнем влияния терроризма на жизнь

Характерной особенностью террористических атак современного периода стало серьезное расширение географии, увеличение количества терактов возрастание жертв, рост размеров материального ущерба.

Сегодня терроризм принял масштабы государственности – Исламское государство (террористическая организация, запрещенная в РФ), халифат с собственной территорией, населением, человеконенавистнической идеологией. Массовым террористическим атаками сегодня подвергаются не только страны ближневосточного и центрально-азиатского региона, но и прежде благополучной Европы, государства с отлаженной системой внутренней безопасности: Россия, США, Франция, Великобритания, Китай и др. Миграционные потоки способствуют распространению зла по всему миру под видом беженцев или трудовых мигрантов.

Высокое техническое и информационное сопровождение террористических атак способствует их эффективности и затрудняет противодействие терроризму, повышает его опасность для мирового сообщества, а также для общества, государства и личности.

Мировая преступность благодаря информационным сетям заняла статус транснациональных организаций, тщательно законспирированных сообществ фанатиков-единомышленников с железной дисциплиной и развитой финансовой инфраструктурой.

Современный терроризм выступает как средство информационной войны, цель которой направлена даже не на уничтожение людей, а на устрашение и деморализацию живых по факту террористических атак. Усилия террористов направлены на масштабное освещение их действий в средствах массовых коммуникаций и массовой информации, иначе цель не будет достигнута. Цель террористов заключается в манипулирования общественным сознанием.

Экстремисты работают над созданием всемирной террористической сети «Автономный джихад», более известный под названием «слипперы». Вербуя своих агентов по всему миру с помощью информационной «паутины», они создают террористическую «паутину» зла, готовую на местах в определенный момент наносить точечные удары.

Международная террористическая сеть использует традиционные каналы связи и обычных месенджеров для координации своих действий. При подготовке и совершении теракта 3 апреля в Санкт-Петербурге эмиссар ИГИЛ из-за рубежа руководил с помощью WhatsApp и Telegram действиями смертника.

Экстремисты успешно ведут идеологическую пропаганду в глобальной Сети, где к настоящему времени насчитывается более десяти тысяч их сайтов. В социальных сетях, широко используемых молодежью, создаются закрытые группы, где бандиты ведут психологическую обработку и вовлечение в свои ряды, привлечение финансовых средств, обучение тактике ведения боевых действий и совершения терактов. Подобные аккаунты сегодня исчисляются несколькими сотнями тысяч. Лица, попавшие под влияние радикальных идей, не проявляют явной активности до момента исполнения преступления, что требует от спецслужб применения всего спектра оперативных возможностей в целях выявления и предотвращения действий указанных категорий лиц.

Особо остро стоит вопрос о расширении сотрудничества террористов с хакерским сообществом и организации с их помощью собственных «киберподразделений». Современный мир становится свидетелем совершенствования технического уровня и изощренности современных кибератак. Оценивая прежний опыт киберпреступлений, направленных на государственные информационные ресурсы, можно предположить о переориентации вектора экстремистов на жизненно важные инфраструктурные объекты с возможностью совершения техногенных аварий и экологических катастроф. Однако это предположение может явиться реальностью.

Количество киберпреступлений в России с 2013 г. по 2016 г. увеличилось в шесть раз. В 2016 году было зафиксировано 66 тыс. IT-преступлений.

Общий ущерб от преступлений в сфере информационных технологий за первую половину 2017 г. превысил 18 млн. долл. США. В минувшем году в России две трети преступлений классифицируются, как преступления экстремистской направленности и каждое девятое преступление террористического характера совершены с использованием сети [2].

Первостепенная задача спецслужб заключается в предупредительных превентивных действиях, направленных на недопустимость распространения зла.

Совместными действиями спецслужб Казахстана, Узбекистана, Таджикистана, Киргизии, Китая, Индии, Южной Кореи, Чехи, Австрии, Сербии и России предотвращены ряд терактов, установлены и задержаны члены МТО.

В целях предотвращения террористических угроз необходимо создание единого антитеррористического информационного пространства с использованием Международного банка данных по противодействию терроризму, созданного ФСБ, который содержит информацию об иностранных террористах, попавших в поле зрения спецслужб. Сегодня важно активное содействие партнеров в его формировании и расширении. В России совершенствуется законодательная база, запрещающая использование современных средств связи в целях организации и координирования террористических атак. Был принят закон о предоставлении профильным ведомствам ключей для дешифрования трафика электронных сообщений. При этом операторы связи обязаны хранить информацию и предоставлять ее по запросу правоохранительных органов. Данные нововведения подверглись резкой критике в нашей стране. Однако принятый подход ни в коей мере не направлен на ущемление прав и свобод граждан. При этом следует помнить, что свободы не бывает без безопасности.

Эффективность противодействия международным компьютерным атакам в большей степени зависит от организации взаимодействия национальных служб, реагирующих на компьютерные инциденты. В этих целях необходимо создание международного запрета на разработку вредоносного программного обеспечения. Жизненно важен контроль со стороны государства над каберпространством, на которое покушаются МТО. Необходимо приведение национальной нормативно-правовой базы в соответствие с возможными угрозами информационной безопасности со стороны международного терроризма. Компьютерные атаки имеют международный характер, что требует межгосударственного взаимодействия спецслужб.

В борьбе с международным терроризмом ООН является связующим звеном между рядом государств. 24 мая была принята Резолюция Совбеза в поддержку «Всеобъемлющей рамочной стратегии противодействия распространению террористических идей». Она содержит конкретные предложения. На состоявшемся 4 и 5 октября в Краснодаре XVI Совещании руководителей спецслужб, органов безопасности и правоохранительных органов иностранных государств – партнеров ФСБ России, в котором приняли участие представители спецслужб 74 стран мира, было принято Заявления в поддержку указанной Резолюции. В нем отражены ключевые позиции, касающиеся сотрудничества спецслужб, включая конкретные санкции в отношении стран, которые замечены в финансировании террористических группировок. Сегодня как никогда ранее необходимо укрепление взаимного доверия между странами и сплочение рядов мирового сообщества против главнейшего зла человечества – терроризма.

Список литературы

1. Глобальный индекс терроризма. Гуманитарная энциклопедия [Электронный ресурс] // Центр гуманитарных технологий, 2006–2017 (последняя редакция: 16.11.2017). – URL: http://gtmarket.ru/ratings/global-terrorism-index/info.

2. Число киберпреступлений в России выросло за три года в шесть раз [Электронный ресурс]. – URL: https://www.vedomosti.ru/technology/news/2017/ 08/24/730839–chislo.