УДК 614.8 DOI: 10.36535/0869-4176-2020-02-11

МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ ИНТЕРНЕТ ТЕРРОРИЗМУ

Кандидат техн. наук *В.Б. Терновсков,* кандидат эконом. наук *М.В. Данилина*
Финансовый университет при Правительстве РФ

***О.А. Никишаева,* студент магистратуры**
Российский государственный университет

В условиях глобализации и стремительного развития технологий и коммуникаций особое внимание необходимо уделять противодействию терроризму в сети Интернет. В большинстве своем в сети Интернет отсутствует государственный контроль, «царит» полная анонимность, ко всем ресурсам имеется безграничный и свободный доступ. Информация распространяется быстро, а стоимость доступа к ресурсам достаточно мала. Все это говорит о том, что Интернет – идеальная площадка для экстремизма. Рассмотрены основные механизмы терроризма в сети Интернет и возможные пути противодействия.

Ключевые слова: интернет, противодействие терроризму, соцсети.

ANTI-TERRORISM MECHANISMS

Ph.D. (Tech.) *V.B. Ternovskov*, Ph.D. (Econ.) *M.V. Danilina*
Financial University under the Government of the Russian Federation

***O.A. Nikishaeva*, student of master programme**
Russian New University

In the context of globalization and evolving development of technologies and communications, particular attention must be paid to countering terrorism on the Internet. Mostly there is no state control on the Internet, lots of possibilities to stay totally anonymous, unlimited and free access to all resources – that is how Internet looks like nowadays. Information is spreading fast, and the cost of access to resources is quite small. All this suggests that the Internet is an ideal platform for extremism. The article will examine the main mechanisms of terrorism on the Internet and possible ways to counter it.

Keywords: internet, counterterrorism, social networks.

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансовому университету при Правительстве РФ.

18 апреля 2019 года прошла Конференция по противодействию международному терроризму, где было отмечено, что «предотвращение использования сетевых технологий, средств массовых коммуникаций и социальных сетей для распространения экстремистских идей» является одной из ключевых задач не только нашей страны, но и всего мира [1].

На Конференции по противодействию международному терроризму 18 апреля 2019 года была установлено и зафиксировано много важнейших проблем. Задачу, которая является

приоритетной для всего общества, можно обозначить, как «ограничение использования социальных сетей».

Человечество шагнуло в новый 21-ый век и оказалось в луже крови. Ведь в современном мире одной из самых актуальных проблем общества является терроризм, который приобрел глобальный масштаб. В синергии с информационными технологиями, терроризм превращается не просто в гремучую смесь, а в орудие массового уничтожения. Если двадцать лет назад вербовка происходила «лицом к лицу», то сейчас достаточно просто завести страницу в социальной сети и склонить человека к неправомерным и бесчеловечным действиям против общества.

«Сегодня реальное обучение сменяется виртуальным. Члены ячейки террористов проходят обучение в онлайн-режиме. Информацию они черпают из проповедей в интернете, призывающих, например, совершать теракты на месте проживания, если у них нет возможности выехать в Сирию. Видео на YouTube научило их способам изготовления коктейля Молотова, а кураторы из ИГИЛ (запрещенная в России террористическая организация) связывались с ними с помощью мессенджера Telegram» [7]. А при помощи поисковой строки Google можно найти инструкции (причем на разных языках) и подробную информацию по становлению членом Исламского государства (ИГ).

С каждым новым днем, с каждой новой технологией исполнительным органам приходится задействовать новые, более совершенные и адаптированные технологии и методы борьбы с терроризмом. Информационная сфера активно используется для пропаганды радикальных идеологий и информационных кампаний, подрывающих национальную и международную безопасность.

Интернет – это самая лучшая среда деятельности для террористических организаций. Особенно это касается мировых сетей, где отсутствует государственный контроль, «царит» полная анонимность, ко всем ресурсам имеется безграничный и свободный доступ. Информация распространяется быстро, а стоимость обслуживания сети крайне мала – все это говорит о том, что Интернет – идеальная площадка для экстремизма. Сегодня социальные сети предоставляют огромное количество возможностей абсолютно каждому интернет-пользователю, который может общаться на огромном расстоянии. «Друзьями» могут воспользоваться и с террористическими целями. К 2018 году ИГ начало перестраивать медийно-коммуникационную структуру организации. Почти треть террористов (по аналитике японских специалистов) пользуются Telegram, меньшая доля приходится на Viber и WhatsApp. Данные мессенджеры используют закрытый протокол, скрывающий личность пользователя. «Деятельность террористов в сети может иметь различный характер:

1. Активизм – это «легитимное» использование Интернет-сети для пропаганды своих идей и привлечения последователей;

2. Хакерская деятельность – это в первую очередь хакерские атаки, проводимые с целью выведения из строя отдельных компьютерных сетей, баз данных либо сайтов, для получения доступа к секретной или государственной информации;

3. Кибертерроризм – это компьютерные атаки, спланированные с целью нанесения максимального ущерба жизненно важным объектам информационной инфраструктуры» [5].

Особенность экстремизма в Интернете заключается в том, что вербовщик не преследует меркантильных целей – ему не нужна ни квартира, ни деньги жертвы. Этот человек попросту – часть деструктивной организации, которая имеет вид, схожий с тоталитарной сектой. «Но как можно заставить человека убить себя, точно так же возможно толкнуть его на убийство других. А полученный символический капитал хорошо известен – это террор» [6].

Однако правоохранители не всегда могут спасти человека от вредоносного влияния тех или иных лиц, поэтому важно уметь самому противостоять террористической пропа-

ганде в Интернете, чтобы не попасться в сети и уберечь себя и близких. Очень часто экстремисты имеют специальную умственную и психологическую подготовку, а перед тем, как начать вербовку, они просматривают десятки «страничек» пользователей сетей – фотографии, друзей, записи на «стене», группы и сообщества для нахождения общих тем. Таким образом, люди сами выкладывают данные о себе в профиле, облегчая пропагандистам предварительный отбор наиболее подходящих кандидатов. Отбор происходит примерно так: все начинается с обычного, бытового общения – вербовщик «нащупывает» круг интересов и ищет психологические рычаги давления. После этого происходит пропаганда религиозных ценностей, затем молодые люди переходят в «закрытые группы в мессенджерах с высоким уровнем криптозащиты, где и происходит вербовка» [2]. В итоге, определяется сфера деятельности нового пособника – то ли он уезжает за границу, то ли попадает в состав «спящей» ячейки, либо же просто оказывает всяческую помощь. Иногда террористам удается завербовать людей при помощи рассылки в популярных мессенджерах: покупается база данных номеров, прописывается код для бота, который производит рассылку экстремистского материала. Для такой схемы нужен лишь телефон и одноразовая сим-карта, которую можно купить в любом переходе.

Как именно происходит поиск людей для вербовки, и какие категории лиц наиболее уязвимы? Вербовщик ИГИЛ (запрещенная в России террористическая организация) ищет в Интернете свою жертву, используя активные интернет-сообщества. Большую часть внимания он уделяет группам, которые так или иначе связаны с исламом, а также под влияние попадают сообщества маргинального характера, где проще всего найти людей, которые находятся в «подвешенном» состоянии – такие являются легкой «добычей». Под «маргинальными группами» подразумеваются объединения в соцсетях, где обсуждаются проблемы алкоголизма, наркомании, депрессии и суицидальных наклонностей. Сайты знакомств, чаты фанатов компьютерных игр, форумы – все это является инструментом в руках террориста. Самые уязвимые для вербовки – одинокие люди, которые были отвергнуты обществом, люди, выражающие социальный протест, а также те, кто имеет проблемы с родственниками или попросту является носителем слабовольного характера.

В качестве решения проблемы террора в соцсетях, например, Facebook предпринял некоторые меры по борьбе с нежелательным контентом, пропагандирующим экстремизм и террористическую деятельность. Компания внедрила новую технологию искусственного интеллекта, который блокирует «скверный» контент. Это было сделано при помощи специального алгоритма Искусственного интеллекта (ИИ), который блокировал посты в соответствии с фразами и словами из запрещенного реестра. Он был создан путём анализа пропагандистских постов боевиков. Однако, как отметили пользователи, такая система абсолютно недееспособна: «под руку» попадают и обычные люди, а экстремистский контент можно найти, используя всего лишь хештег. Таким образом, можно сделать вывод, что проблему сетевого терроризма нужно решать не на локальном уровне каких-то компаний, а на государственном и мировом.

Террор в Крайстчерче, Новая Зеландия, который убил 50 верующих мусульман, присоединяется к растущему списку атак, где использовался Интернет для распространения пропаганды убийцы. Если бы социальные сети и интернет-провайдеры надлежащим образом отслеживали сообщения подозреваемого, возможно, был бы произведен арест и предотвращена бойня. Например, если бы 8chan или Twitter имели достаточное количество скринингов или алгоритмов, способных идентифицировать, что в манифесте убийцы прямо указывалось, что он планирует совершить террор, любой из них мог бы немедленно уведомить об этом власть. Интернет, хотя он так важен для современной жизни, также может быть использован для совершения величайшего зла. Хоть законодательно Конституция защищает свободу слова, настоящие угрозы, такие как заявления террори-

стов, выражающие серьезное намерение совершать насильственные действия против отдельных лиц и групп, конституционно не защищены.

В России проблеме взаимодействия террористов и Интернета также уделяют большое внимание. «Мы живем в такие времена, когда с помощью мобильного устройства можно нарушить работу атомной станции, а информационная борьба является наиважнейшей проблемой. «Государство должно обладать необходимыми инструментами для противодействия пагубного влияния на граждан» – заявил газете «Известия» Анатолий Выборный, который является зам. главы комитета Госдумы по безопасности [4]. Поле действия террористов – социальные сети по типу «Вконтакте», «Одноклассники», «Instagram», «Facebook» и другие. Органы государственной безопасности уже внедряют свои внутренние комитеты по борьбе с терроризмом [3]. На одиннадцатом пленарном заседании Парламентской Ассамблеи ОДКБ, членом которой является и Российская Федерация, был принят закон «Об информационном противоборстве терроризму и экстремизму». Базируясь на этом модельном законе, можно сформулировать следующие рекомендации по противодействию информационному терроризму, в том числе в сети Интернет:

1. контроль сообществ и групп в социальных сетях. Сообщества, которые содержат в себе призывы к террористическим действиям/экстремизм/насилие, должны выявляться путем надзора специального органа либо же модерироваться непосредственно администрацией социальной сети;
2. ужесточение доступа к секретным государственным информационным ресурсам. В качестве защиты использовать новые информационные технологии, которые смогут уберечь базы данных/архивы/документацию от нападок хакеров и DDOS-атак;
3. система двойной идентификации пользователей в сети Интернет, регистрация в социальных сетях при помощи идентификационных документов. В данный момент в любой соцсети пользователь может создать неограниченное количество аккаунтов для самых разных целей – начиная от вербовки, заканчивая накруткой подписчиков в экстремистских сообществах;
4. проверка со стороны СМИ редакционных материалов на наличие экстремизма. Кроме сообществ и групп, в Интернете давно существуют свои цифровые СМИ («Медуза», «Дождь», «Интерфакс» и многие другие), которые также следует модерировать в соответствии с 280 статьей УК РФ (призыв к экстремизму);
5. создание «народных дружин» для противодействия терроризму в сети. Вышесказанный пример о модерации экстремистского контента в Facebook как нельзя, кстати, показывает, что на административном уровне нельзя полностью искоренить нежелательные посты и террористические сообщества. Важной частью является консолидированное общество, которое осознает всю проблему мирового терроризма и его пропаганды в сети Интернет – именно пользователи должны проявлять инициативу по уничтожению вредоносного контента, поэтому «народные дружины» - одно из самых эффективных средств [4]. Именно поэтому после неудавшегося эксперимента по удалению террористической пропаганды при помощи искусственного интеллекта, компания Facebook создала большую команду людей в противовес роботам и алгоритмам – так борьба стала более эффективной [8].

Существует несколько направлений для последующих исследований в изучении отношений между социальными сетями и терроризмом. Во-первых, террористы используют несколько языков на веб-сайтах для распространения своей пропаганды. В будущем анализ поисковых запросов Google или Яндекс может помочь собрать всю необходимую информацию для борьбы с пропагандисткой деятельностью. Во-вторых, необходимо выяснить, кто занимается поиском террористов в Интернете. С какой целью? Видят ли эти люди зло и несправедливость в окружающем мире, которые «необходимо устранить»?

В-третьих, компании Яндекс и Google предоставляют статистику интернет-запросов конкретных фраз в разных регионах, а не только по всему миру. Таким образом, в дальнейшем можно будет выяснить, в каких регионах люди чаще ищут террористические связи. С развитием этих трех направлений, ученым-социологам будет проще объяснить процессы радикализации тех или иных взглядов в конкретном обществе.

Литература

1. «Конференция по противодействию международному терроризму». URL: https://iacis.ru/activities/events/partnery/konferentsiya_po_protivodeystviyu_mezhdunarodnomu_terrorizmu_sovmestno_s_mezhdunarodnymi_parlamentsk/
2. «Бесконтактная вербовка». URL: https://ria.ru/20180228/1515459761.html
3. «Терроризм в социальных сетях». URL: https://www.arms-expo.ru/news/protivodeystvie-terrorizmu/natsionalnyy-antiterroristicheskiy-komitet-nachal-protivodeystvie-terrorizmu-v-sotsialnykh-setyakh/
4. «СМИ обяжут содействовать борьбе с экстремизмом». URL: https://iz.ru/727403
5. Яцук К.В., Мухамбетов Ж.С., Цымбалий А.О. Терроризм в сети // Молодой ученый. — 2018. — №11. — С. 59-62.
6. «Анонимность терроризма и публичность Социальных сетей. Как это может быть связано?». URL: http://c-eho.info/obshchestvo/item/2652-anonimnost-terrorizma-i-publichnost-sotsialnykh-setej-kak-eto-mozhet-byt-svyazano
7. Демидов Л.Н., Терновский В.В., Тарасов Б.А., Терновсков В.Б. Модель представления информации для применения в экономике // Экономика: вчера, сегодня, завтра. - 2016, №3
8. Поляков В.П. Развитие информационной подготовки в контексте стратегии национальной безопасности Российской Федерации // Наукоград наука производство общество. - 2016. № 2. С. 46-51.
9. Подшивалов Г.К., Терновсков В.Б., Демидов Л.Н., Тарасов Б.А. Экономическая безопасность в условиях неопределенности // Экономика: вчера, сегодня, завтра. - 2016. № 2. С. 242-257.
10. «Борьба с терроризмом в социальных сетях». URL: https://dag.life/2017/12/25/borba-s-terrorizmom-v-socialnyh-setyah/
11. «Facebook Steps Up Efforts Against Terrorism». URL https://www.wsj.com/articles/facebook-steps-up-efforts-against-terrorism-1455237595?mod=article_inline

Сведения об авторах

Терновсков Владимир Борисович, Финансовый университет при Правительстве РФ, ул. Кибальчича, 1, 8(929)9285292, vternik@mail.ru

Данилина Марина Викторовна, Финансовый университет при Правительстве РФ, ул. Кибальчича, 1, 8(910)4307831, marinadanilina@ya.ru

Никишаева Ольга Аркадьевна, студентка магистратуры Российского государственного университета, 115035, г. Москва, ул. Садовническая, д. 33, стр. 1, 8 (925) 372-72-04 , olya.nikish96@gmail.com