УДК 343.85
МРНТИ 10.81.71

Д.Б. Кайназарова, А.А. Калиев
Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Косшы, Республика Казахстан

К ВОПРОСУ ВЫЯВЛЕНИЯ И РАССЛЕДОВАНИЯ ТЕРРОРИСТИЧЕСКИХ И ЭКСТРЕМИСТСКИХ ПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ

Аннотация. В статье рассматриваются проблемы выявления и расследования экстремистских и террористических преступлений, совершаемых с помощью глобальной сети Интернет. Авторы статьи обращают внимание читателя на использование возможностей всемирной паутины преступными организациями, в том числе экстремистской и террористической направленности, способы сокрытия незаконных действий с целью передачи сообщений и вовлечения общества в противозаконную деятельность.

В то же время авторы дают рекомендации для правоохранительных органов по выявлению противоправной деятельности в сети интернет и пресечению экстремистских и террористических преступлений, совершаемых посредством сети Интернет. К их числу можно отнести мониторинг интернет-пространства путем использования искусственного интеллекта для анализа огромного количества информации, содержащейся на интернет-ресурсах, социальных графов для изучения профилей конкретных пользователей социальных сетей с целью выявления лиц, совершающих преступления экстремистского и террористического характера.

Авторы акцентируют внимание на необходимость профессионального обучения сотрудников правоохранительных органов для повышения эффективности их работы по выявлению и пресечению экстремистской и террористической деятельности в Интернет-пространстве.

Ключевые слова: террористическое преступление; экстремистское преступление; мониторинг; социальный граф; искусственный интеллект; блокчейн; сайт; IP-адрес; анализ данных; расследование; выявление.

Д.Б. Қайназарова, А.А. Қалиев
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Қосшы қ., Қазақстан Республикасы

ИНТЕРНЕТ ЖЕЛІСІНДЕ ТЕРРОРИСТІК ЖӘНЕ ЭКСТРЕМИСТІК ҚЫЛМЫСТАРДЫ АНЫҚТАУ ЖӘНЕ ТЕРГЕУ МӘСЕЛЕСІНЕ

Аннотация. Мақалада ғаламдық Интернет желісі арқылы жасалған экстремистік және террористік қылмыстарды анықтау және тергеу мәселелері қарастырылады. Мақала авторлары оқырманның назарын қылмыстық ұйымдардың бүкіләлемдік ғаламтор мүмкіндіктерін, соның ішінде экстремистік және террористік бағытты, хабарламалар беру және қоғамды заңсыз әрекеттерге тарту мақсатында заңсыз әрекеттерді жасыру тәсілдерін пайдалануға аударады.

Сонымен бірге авторлар құқық қорғау органдарына интернет желісіндегі заңсыз әрекеттерді анықтау және Интернет желісі арқылы жасалған экстремистік және террористік қылмыстардың жолын кесу бойынша ұсыныстар береді. Оларға Интернет-ресурстардағы ақпараттың үлкен көлемін талдау үшін жасанды интеллектті, экстремистік және террористік сипаттағы қылмыс жасаушыларды анықтау мақсатында әлеуметтік желілерді нақты пайдаланушылардың профильдерін зерттеуге арналған әлеуметтік графтарды талдау арқылы интернет-ресурстерді бақылау кіреді.

Авторлар құқық қорғау органдарының қызметкерлерін Интернет – кеңістіктегі экстремистік және террористік әрекеттерді анықтау және жолын кесу жөніндегі жұмыстарының тиімділігін арттыру үшін кәсіби оқыту қажеттілігіне назар аударады.

Түйінді сөздер: террористік қылмыс; экстремистік қылмыс; мониторинг; әлеуметтік граф; жасанды интеллект; блокчейн; сайт; IP-мекенжай; деректерді талдау; тергеу; анықтау.

D.B. Kainazarova, A.A. Kaliyev
The Academy of Law Enforcement Agencies under the Prosecutor General's Office of the Republic of Kazakhstan, Kosshy c., the Republic of Kazakhstan

TOWARDS THE DETECTION AND INVESTIGATION OF TERRORIST AND EXTREMIST CRIMES ON THE INTERNET

Abstract. The article deals with the problems of identifying and investigating extremist and terrorist crimes committed using the global Internet. The authors of the article draw the reader's attention to the use of the possibilities of the World Wide Web by criminal organizations, including extremist and terrorist ones, ways to conceal illegal actions in order to transmit messages and involve society in illegal activities.

At the same time, the authors provide recommendations for law enforcement agencies to identify illegal activities on the Internet and to suppress extremist and terrorist crimes committed via the Internet. These include monitoring the Internet space by using artificial intelligence to analyze a huge amount of information contained on Internet resources, social graphs to study the profiles of specific users of social networks in order to identify persons committing crimes of an extremist and terrorist nature.

The authors emphasize the need for professional training of law enforcement officers to increase the effectiveness of their work to identify and suppress extremist and terrorist activities in the Internet space.

Keywords: terrorist crime; extremist crime; monitoring; social graph; artificial intelligence; blockchain; website; IP-address; data analysis; investigation; detection.

DOI: 10.52425/25187252_2023_30_74

Введение. Появление Интернета дало человечеству большие возможности, как в развитии информационно-коммуникационных технологий, так и самого общества. Но вместе с тем, глобальная сеть принесла с собой и множество новых угроз. Одна из них распространение в сети Интернет террористической и экстремистской информации. Всемирная паутина стала для таких организаций площадкой для коммуникаций между собой и вовлечения в свои ряды все новых сторонников своих экстремистских и террористических идей.

В настоящее время современные технологии, интернет и специальное программное обеспечение позволяют не только экстремистам и террористам, но и другим преступным сообществам через расстояния совершать свои преступления, скрывать следы своих противоправных действий, тайно передавать информацию по всему миру, используя многочисленные шифрованные каналы связи.

Все это делает процесс выявления и пресечения преступных действий экстремистских и террористических организаций более сложным.

Задачи и цели. Основная цель публикации – исследование глобальной сети интернет с точки зрения площадки для совершения различных уголовных правонарушений. Основной задачей статьи является выделение ключевых проблем противодействия террористическим и экстремистским преступлениям.

Методы исследования. В работе использовались такие методы научного исследования, как логический анализ, индукция и синтез.

Результаты/обсуждение. Различные экстремистские и террористические организации используют Интернет, как площадку для осуществления своей незаконной деятельности, а именно в обеспечении коммуникации между своими членами и размещении на интернет-ресурсах противоправной информации.

На это обращает свое внимание и автор статьи «Реализация мер по противодействию экстремизму в сети Интернет» А.А. Куричев. Он говорит о том, что экстремистские и террористические организации для привлечения новых адептов в свою среду, вынуждены использовать современные технологии, такие как сеть «Интернет» [1,

127 стр.].

Главными угрозами, с которыми столкнулись правоохранительные и специальные органы всех государств стали:

- использование Интернета для распространения незаконного контента и новых адептов в свои преступные сообщества;

- координация и планирование террористических актов;

- использование возможностей различных криптовалют и систем платежей для финансирования экстремистской и террористической деятельностей;

- использование площадок распространенных социальных сетей для размещения видео, содержащих угрозы и заявления, а также для обмена информацией между членами террористической организации.

В этой связи видится необходимым усиление борьбы с экстремистскими и террористическими преступлениями в сети Интернет.

На сегодняшний день правоохранительные и специальные органы во всем мире выделяют несколько основных проблем противодействия данным преступлениям, требующих принятие решений.

Первая. Интернет или как его иногда называют всемирная паутина – это глобальная сеть соединенных между собой устройств (компьютеров), взаимодействующих между собой и предоставляющих через них доступ к различным интернет-ресурсам. Выявление преступлений, совершаемых посредством сети интернет всегда вызывало затруднение из-за сложности определения: места, откуда действует преступник или преступные сообщества, устройства, которым они пользуются и непосредственно самого лица, ответственного за такие деяния.

Если по обычным преступлениям правоохранительные и специальные органы имеют определенный опыт поиска и сбора доказательств, расследования и установления виновного лица, то по уголовным правонарушениям, совершенным с использованием сети Интернет и современных информационно-коммуникационных технологий им требуются специальные познания.

Такими познаниями являются технические особенности устройств, сетей, информационных систем, используемых преступниками, психология личности лиц, совершающих преступления данной категории.

Учитывая это правоохранительные и специальные органы привлекают к своим расследованиям специалистов в области IT-технологий, которые начинают свою работу в первую очередь с определения IP-адреса устройства, которое было задействовано:

- в распространении информации в интернете посредствам социальных сетей или самых распространенных мессенджеров;

- в размещении противоправного контента на определенном интернет-ресурсе.

IP-адрес – это уникальный номер или идентификатор устройства (компьютера, планшета, ноутбука, сотового телефона), подключенного к сети Интернет.

Он позволяет данным устройствам обмениваться между собой данными, определять путь, по которому эти данные должны идти в сети, идентифицировать друг друга.

IP-адрес может быть двух видов: формата IPv4, состоящий из 4-х байтов (192.168.0.1) и формата IPv6, состоящий из 8 групп по 4 символа (2001:0db5:0000:34a2:0000:7a3e:0730:7557).

Преступные сообщества в настоящее время научились не только скрывать реальный IP-адрес, но и не показывать устройство в сети интернет, использованного для совершения преступлений, что делает процесс идентификации преступника практически не возможным. К средствам анонимизации (сокрытия) IP-адреса относятся различные анонимайзеры или VPN-сервера, скрывающие реальный IP-адрес [2, 51 стр.].

Кроме того, преступники с помощью тех же технических специалистов, работающих на экстремистские и террористические организации, научились использовать

подпольные сайты и защищенные сервера, для того, чтобы правоохранительным органам было тяжело их отследить или заблокировать.

Некоторые такие преступные организации для распространения незаконного контента в Интернете используют еще и шифрование данных с помощью различных компьютерных программ и алгоритмов шифрования, что обеспечивает им дополнительную защиту своих сообщений от перехвата и мониторинга правоохранительными и специальными органами.

Вторая. Правоохранительные и специальные органы сталкиваются с проблемой прослушивания и просмотра информации, передаваемой посредством сети Интернет, в связи с использованием преступными сообществами зашифрованных каналов связи. Например, с целью исключения посторонних лиц на своих экстремистских и террористических интернет-ресурсах, преступники стали использовать так называемые «ключи активации».

Их суть заключается в том, что те интернет-пользователи, которые не имеют специальный шифр (пароль), не могут получить доступ к конкретным ресурсам сайта.

Третья. Правоохранительные и специальные органы несвоевременно выявляют и принимают меры к сайтам, распространяющим незаконный контент экстремистского и террористического характера. Это связано с тем, что некоторые свои преступления в Интернете экстремистские и террористические организации совершают в течение нескольких минут, после чего скрывают или удаляют свои следы в сети.

Более того, на каждый выявленный и заблокированный сайт, содержащий противоправный контент, экстремистские и террористические организации открывают два других сайта, распространяя в Интернете информацию о них, предоставляя ссылку для моментального перехода и скачивания незаконной информации экстремистского и террористического характера.

Все эти методы совершения преступлений препятствует своевременному выявлению и пресечению преступной деятельности таких организаций в сети Интернет, а также привлечения виновных лиц к установленной законом ответственности.

В этой связи, правоохранительные и специальные органы должны постоянно совершенствовать свои профессиональные навыки, развивая IT-компетенции такие как использование специального программного обеспечения для эффективной работы в данном направлении.

К их числу можно отнести программное обеспечение «IP Logger», которое позволяет формировать короткие ссылки для определения реального IP-адреса и соответственно географическое местоположение устройства, используемое преступником. Данная программа позволяет следователю получить информацию, необходимую для продолжения поиска *(розыска)* подозреваемого: время, дату, IP-адрес, страну, город, операционную систему и браузер.

Кроме того, в арсенале следователя должны быть такие инструменты поиска и определения геолокации преступника, как интернет-сервисы «2IP» или «Whois», позволяющие следователю узнать расширенную информацию по IP-адресу преступника и самое главное узнать название провайдера (поставщика услуг), через которого уже определить точные координаты местонахождения подозреваемого.

На сегодняшний день имеются следующие способы доступа к закрытым интернет-ресурсам, распространяющим экстремистскую и террористическую информацию в Интернете, которые могут использовать правоохранительные и специальные органы.

1) Использование специального программного обеспечения для подбора паролей (например, «Hashcat») и определения способов шифрования каналов передачи информации, экстремистскими и террористическими организациями (например, Picocrypt).

Это позволяет правоохранительным и специальным органам проникнуть в закрытые Интернет-ресурсы, проанализировать массив данных, провести соответствующую экспертизу на предмет содержания в них запрещенной экстремистской и террористической информации и своевременно блокировать к ним доступ.

Учитывая, что преступные сообщества научились пользоваться поддельными IP-адресами и виртуальными частными сетями, необходимо вовлекать в работу IT-специалистов, которые помогают сотрудникам правоохранительных и специальных органов решать данную проблему.

2) Использование возможностей интернет-провайдеров, а также владельцев интернет-ресурсов, на которых распространяется незаконный контент. Правоохранительные и специальные органы имеют право в рамках расследуемых уголовных дел по экстремистским и террористическим преступлениям запрашивать у таких организаций, предоставляющих услуги Интернета и владельцев интернет площадок, информацию об устройствах и их владельцах с целью выявления и привлечения виновных лиц к установленной законом ответственности.

3) Правоохранительные и специальные органы могут использовать различные уязвимости, как в программном обеспечении, используемом преступниками, так на сайтах, где размещена запрещенная и незаконная информация.

Для использования этого метода правоохранительным и специальным органам могут помочь IT-специалисты соответствующего профиля работы. Их иногда называют «пентестеры», т.е. специалисты по выявлению уязвимостей в информационной системе или программном обеспечении.

Данные специалисты находят возможность проникнуть незаметно на интернет-сайт и получить все необходимые сведения для правоохранительных и специальных органов.

Помимо этого, для выявления и идентификации экстремистов и террористов в сети Интернет, сотрудники правоохранительных и специальных органов должны постоянно проводить мониторинг и анализ данных в социальных сетях, поскольку они являются самыми распространенными площадками для обмена информацией. Путем данного мониторинга выявляются участники преступных групп и их связи.

Учитывая научно-технический прогресс, современное программное обеспечение и высокоскоростной интернет, с этой задачей успешно справляется искусственный интеллект. Именно методы машинного обучения, позволяют правоохранительным и специальным органам выявлять среди огромного количества информации в Интернете незаконный контент, правильно классифицировать сообщения, содержащие экстремистскую и террористическую информацию.

Установление связей между участниками преступных сообществ играет немаловажную роль в выявлении и расследовании преступлений данной категории. Одним из инструментов, позволяющих проводить такую работу, является анализ социальных графов.

Социа́ льный граф – это граф, узлы которого представлены социальными объектами, такими как пользовательские профили с различными атрибутами *(например: имя, день рождение, родной город)*, сообщества, медиа контента и так далее, а ребра – социальными связями между ними [3, 4 стр.].

Другими словами, социальные графы – это графические модели, взаимосвязанных между собой субъектов, таких как люди или организации.

На рисунке (Рис. 1) представлен пример социального графа, взаимосвязанных между собой людей, а также мест их пребывания.

Вышеуказанные графы используют не только интернет исследователи для сбора необходимой информации, анализа больших данных, но и сотрудники правоохранительных и специальных органов для выявления связей участников преступных сообществ, их структур, степени взаимодействия между собой.

Рис. 1

В качестве примера можно привести программное обеспечение «Maltego», которое позволяет анализировать различные данные, взятые из открытых источников (например, социальной сети «Вконтакте») и формировать группу социальных графов, связанных между собой, объединенных в кластеры.

Правоохранительные органы, исследуя данные кластеры, могут выявлять всех участников преступного сообщества.

Именно такие технологии правоохранительным и специальным органам позволяют сегодня собирать значительный объем важной информации для расследования преступлений экстремистского и террористического характера, понимания лиц их совершающих. Иногда такую работу проводят сотрудники силовых структур вручную, исследуя каждый заинтересованный интернет-ресурс, но в большинстве случаев используют специальное программное обеспечение, которое в автоматическом режиме выделяет, анализирует нужные сведения.

Для противодействия преступлениям данной категории предлагаются следующие меры, направленные на повышение эффективности работы правоохранительных и специальных органов:

1) Общественный контроль. Он позволяет гражданам непосредственно принимать участие в выявлении незаконного контента в сети Интернет, с последующим уведомлением правоохранительных и специальных органов о таких интернет-ресурсах;

2) Совершенствование правовой базы. Развитие правовых механизмов играет важную роль в эффективности выявления и расследования преступлений экстремистского и террористического характера, неотвратимости наказаний лиц их совершающих, формировании правосознания граждан и активизации гражданской активности. В частности, предусмотреть в уголовно-процессуальном кодексе понятие «электронные доказательства», «цифровые улики»;

3) Обеспечение прав и свобод граждан. Эффективные меры противодействия распространению незаконного контента в сети Интернет позволяют защищать граждан от информации, наносящей вред их психическому здоровью и нормальному развитию личности. К таким мерам можно отнести применение современных технологий, предполагающих использование различных фильтров при посещении сайтов интернет-

ресурсов, которые в автоматическом режиме блокируют запрещенную информацию;

4) Участие экспертов. Поскольку правоохранительные и специальные органы самостоятельно не могут определять и давать оценку распространяемой в сети Интернет информации, целесообразно привлекать к проводимой работе различных экспертов: теологов, религиоведов, психологов, судебных экспертов;

5) Профилактика. Интернет – это место пребывания молодежи. Молодое поколение, начиная от малых лет и до формирования личности, находятся в Интернете. Социальные сети стали местом коммуникации, обмена знаниями, опытом, иной информацией. Там же присутствуют и экстремистские и террористические организации, информация которых нацелена на молодежь, поскольку именно она наиболее подвержена обработке и зомбированию преступных сообществ. Поэтому правоохранительные и специальные органы должны во взаимодействии с уполномоченными государственными органами и неправительственными организациями привлекать молодежь к общественным мероприятиям, направленным на развитие духовной, нравственной, здоровой личности;

6) Развитие информационных технологий. Научные разработки в сфере интернет-технологий, такие, как блокчейн и искусственный интеллект сегодня позволяют эффективно противостоять распространению в Интернете экстремистской и террористической информации. Компьютерные программы с искусственным интеллектом без участия человека выявляют противоправный контент и блокируют к ним доступ, либо направляют ссылки на интернет-ресурсы в уполномоченные органы в автоматическом режиме [4, 57 стр.];

7) Использование IT-специалистов. Без специальных познаний, которые имеются у IT-специалистов правоохранительным и специальным органам было бы сложнее выявлять и пресекать противоправную деятельность экстремистских и террористических организаций;

8) Международное сотрудничество. Без взаимодействия между правоохранительными органами разных стран не возможна эффективная работа в сфере противодействия экстремизму и терроризму в сети Интернет. Это связано с тем, что Интернет сегодня позволяет совершать преступления, не зная границ и времени. Преступник может находиться в одной стране, а местом совершения преступления стать абсолютно другая страна;

9) Обучение. Эффективная работа по противодействию экстремистским и террористическим преступлениям в Интернете невозможна без обучения и повышения профессиональной квалификации сотрудников право-охранительных органов, которые должны обладать не только знаниями в сфере уголовного процесса и досудебного расследования, но и иметь такие же компетенции как у IT-специалистов.

Заключение/выводы. Противодействие экстремистским и террористическим преступлениям, которые совершаются в сети Интернет, является сложной задачей для правоохранительных органов, требующей совместных усилий органов расследования и специалистов в сфере IT-технологий. Данное сотрудничество включает в себя не только мониторинг и анализ данных, но и блокировка интернет-ресурсов, содержащих запрещенный контент, а для этого необходимо специальное программное обеспечение.

На сегодняшний день без поддержки технических специалистов, современных технологий и программных средств, позволяющих выявлять, анализировать и изымать электронные доказательства, сложно противостоять угрозам, исходящим из сети Интернет.

Только такое взаимодействие может привести к определенному результату.

Описанные проблемы и пути решения являются далеко не исчерпывающим списком, но, тем не менее, правоохранительным органам необходимо

учитывать их и использовать новые технологии для борьбы с экстремистскими и террористическими организациями.

Кроме того, для того чтобы расследование экстремистских и террористических преступлений в сети Интернет было более эффективным, необходимо продолжать совершенствовать законодательство и внедрять современные технологии в деятельность правоохранительных органов.

Список использованной литературы:

1. Куричев, А.А. Реализация мер по противодействию экстремизму в сети Интернет // Стратегии развития социальных общностей, институтов и территорий: материалы V Междунар. научно-практ. конф.; 22-23 апреля 2019 г.: в 2-х т. – Екатеринбург: Изд-во Урал. ун-та, 2019. – Т. 1. – С. 127-131.
2. Каримов, В.Х. Актуальные вопросы борьбы с преступлениями, совершаемыми с использованием систем анонимизации пользователей в сети Интернет / В.Х. Каримов // Российский следователь. – 2018. – №6. – С. 51-54.
3. Zillman, M.P. Online Social Networks / M.P. Zillman. – Virtual Private Library, 2022. – 30 s.
4. Бутенко, А.С. Экстремизм в сети Интернет: понятие и сущность / А.С. Бутенко // Юристъ-Правоведъ. – 2019. – №2(98). – С. 57-61.

References:

1. Kurichev, A.A. Realizacija mer po protivodejstviju jekstremizmu v seti Internet // Strategii razvitija social'nyh obshhnostej, institutov i territorij: materialy V Mezhdunar. nauchno-prakt. konf.; 22-23 aprelja 2019 g.: v 2-h t. – Ekaterinburg: Izd-vo Ural. un-ta, 2019. – T. 1. – S. 127-131.
2. Karimov, V.H. Aktual'nye voprosy bor'by s prestuplenijami, sovershaemymi s ispol'zovaniem sistem anonimizacii pol'zovatelej v seti Internet / V.H. Karimov // Rossijskij sledovatel'. – 2018. – №6. – S. 51-54.
3. Zillman, M.P. Online Social Networks / M.P. Zillman. – Virtual Private Library, 2022. – 30 s.
4. Butenko, A.S. Jekstremizm v seti Internet: ponjatie i sushhnost' / A.S. Butenko // Jurist#-Pravoved#. – 2019. – №2(98). – S. 57-61.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Дариға Болатқызы Қайназарова – Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының біліктілікті арттыру институтының қылмыстық құдалау және жедел-іздестіру қызметі кафедрасының доценті, заң ғылымдарының кандидаты, e-mail: dariga.76@list.ru.

Кайназарова Дарига Болатовна – доцент кафедры уголовного преследования и оперативно-розыскной деятельности Института профессионального обучения Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, кандидат юридических наук, e-mail: dariga.76@list.ru.

Kainazarova Dariga Bolatovna – Associate Professor of the Department of Criminal Prosecution and Operational Investigative Activities of the Institute of Professional Training of the Academy of Law Enforcement Agencies under the Prosecutor General's Office of the Republic of Kazakhstan, Candidate of Law, e-mail: dariga.76@list.ru.

Асқар Абужанұлы Қалиев – Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының кәсіптік оқыту институтының жаһандық қатерлерге қарсы іс-қимыл жөніндегі арнайы даярлық кафедрасының доценті, e-mail: askar909@mail.ru.

Калиев Аскар Абужанович – доцент кафедры специальной подготовки по противодействию глобальным угрозам Института профессионального обучения Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, e-mail: askar909@mail.ru.

Kaliyev Askar Abuzhanovich – Associate Professor of the Department of Special Training in Countering Global Threats of the Institute of Professional Training of the Academy of Law Enforcement Agencies under the Prosecutor General's Office of the Republic of Kazakhstan, e-mail: askar909 @mail.ru.