М.П. Баранов
Барнаульский юридический институт МВД России

ЭКСТРЕМИЗМ В КИБЕРПРОСТРАНСТВЕ: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ И ПРОФИЛАКТИКА СРЕДИ ДЕТЕЙ И ПОДРОСТКОВ

Развитие и широкое распространение киберпространства поставило перед государством ряд проблем в сфере противодействия экстремизму. Во-первых, специалистами отмечается изменение структуры экстремистских организаций, переход от строгой иерархической организации к сетевой форме, в связи с чем снижается возможность государства по противодействию их деятельности [4].

Широкие возможности киберпространства изменили тактику действий экстремистских организаций, предоставив в руки экстремистов мощный инструмент вербовки.

Использование социальных сетей позволяет целенаправленно обращаться к конкретной аудитории, например к какой-нибудь возрастной группе, либо к последователям определенной религии, представителям групп повышенного протестного потенциала

(обманутых дольщиков, безработных и т.д.), либо к группам людей, знакомых с проблемами алкоголизма, наркомании, депрессии и т.д., выбирая максимально действенную стратегию.

Для вербовки используются не только сайты, социальные сети, форумы, но и игровые чаты [2]. Вовлечение в деятельность экстремистских организаций может осуществляться с помощью привычной для молодежи формы онлайн-игр, таких как «Большая Игра. Сломай систему».

Использование социальных сетей и мессенджеров позволяет осуществлять координацию действий, организовывать массовые акции и флешмобы, при этом организаторов флешмобов достаточно сложно выявить, а «мирный» флешмоб может в любой момент перерасти в насильственную акцию с помощью заранее спланированной манипуляции.

Киберпространство позволяет обращаться к широкой аудитории, не ограниченной территориями государств, передавая огромные объемы информации за короткое время, при этом оставаясь анонимным. Кроме того, организация распространения экстремистских идей в киберпространстве не требует высоких финансовых затрат. Появление виртуальных криптовалют позволило повысить скрытность проведения финансовых операций.

Объем информации, размещенной в интернете, и скорость её обновления затрудняют возможность оперативной оценки уполномоченными органами и снижают возможность к критическому осмыслению и объективной оценке пользователями, позволяя экстремистам манипулировать фактами. Информация может храниться в виде неограниченного количества копий на различных серверах, компьютерах пользователей либо других носителях.

В условиях невозможности определения государственных границ в киберпространстве единственным действенным способом контроля государства становится блокировка доступа к нежелательной информации.

Так, в целях ограничения оборота нежелательной информации в соответствии со ст. 15.1 Федерального закона № 149 «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации) [6] создан «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено». В реестр включаются доменные имена и (или) указатели страниц сайтов в сети Интернет; сетевые адреса, позволяющие идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено. Закон предписывает оператору связи ограничить доступ к такому сайту.

Однако ограничение доступа к нежелательной информации сталкивается с рядом проблем технического характера. Так, обойти ограничение доступа возможно с помощью прокси-серверов, сети Tor, используя технологию VPN.

В связи с этим с 1 ноября 2017 г. вступили в силу изменения в Закон об информации, в частности, запрещающие владельцам информационно-телекоммуникационных сетей, информационных ресурсов, посредством которых обеспечивается доступ к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации, предоставлять возможность использования на территории Российской Федерации принадлежащих им информационно-телекоммуникационных сетей и информационных ресурсов для получения доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации.

Проблема реализации данных положений Закона об информации заключается в том, что серверы, при подключении к которым пользователь может получить доступ к ресурсам, к которым ограничен доступ на территории Российской Федерации, физически располагаются за пределами Российской Федерации, и их количество может быть неограниченным, а адреса могут постоянно меняться. Так, в то время как ряд сервисов («Лаборатория Касперского», Opera VPN, анонимайзеры 2ip.ru) тестирует возможность взаимодействия с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций по возможности блокировки ресурсов, другие либо не определились (Hidemy.name, Cyberghost, Vemeo), либо заявили о том, что не собираются подчиняться требованиям российских законов и отказали в сотрудничестве (Tunnelbear, Zenmate, ExpressVPN) [1, 4].

Исходя из изложенного, для эффективного противодействия пропаганде экстремистских идей в сети Интернет необходимо создать эффективный механизм непрерывного мониторинга киберпространства и оперативного удаления либо блокирования нежелательной информации, что на современном этапе развития технически затруднено. Кроме того, для ограничения доступа к контенту необходима его правовая оценка, что сказывается на оперативности.

Таким образом, исходя из означенных проблем, вопрос профилактики и противодействия экстремизму в сети Интернет становится не только задачей государства, но и, возможно даже в большей степени, задачей гражданского общества. Опреде-

ляющим фактором становится профилактическая работа среди детей и подростков.

В первую очередь профилактика экстремизма среди детей и подростков включает в себя работу по разъяснению принципов информационной безопасности, предупреждению о возможности подвергнуться воздействию со стороны вербовщиков экстремистских организаций.

Кроме того, современные программные средства позволяют ограничивать распространение нежелательной информации среди детей и подростков.

Так, ограничения по доступу к информации можно настроить в операционной системе Windows с помощью настройки параметров учетных записей, настроить фильтрацию поиска, исключив из результатов нежелательный контент, в поисковых системы Google и Yandex, а также с помощью использования специальных программных комплексов «родительского контроля» (KinderGate, родительский контроль в Kaspersky Internet Security и др.).

Кроме того, все социальные сети, в т.ч. «Одноклассники», «ВКонтакте», Facebook, а также сервисы Youtube, Rutube позволяют пожаловаться администрации сайта на неприемлемый контент, который может быть заблокирован.

Об экстремистских материалах можно сообщить через сервис Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет (НЦПТИ) по адресу: http://нцпти.рф/ либо на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по адресу: http://eais.rkn.gov.ru/feedback/.

Перспективным направлением может стать поддержка государством стихийно складывающихся в сети Интернет добровольных объединений пользователей, стремящихся противостоять распространению экстремистских материалов, распространению профилактической информации в социальных сетях, а также создание в виртуальном пространстве площадок для реализации потенциала детей и подростков, в т.ч. в процессе принятия общественно значимых решений, привлечения «лидеров мнений» молодежи для пропаганды идей мультикультурализма и толерантности.

Литература

1. Диль В.А. Тенденции развития современного экстремизма: молодежный и информационный экстремизм // Известия ТПУ. 2009. № 6. С. 167-170.

2. ИГИЛ – угроза человечеству. Почему необходимо уничтожить терроризм / под общ. ред. С.А. Орджоникидзе. М.: Изд-во «Буки Веди», 2016. 40 с.

3. Лашин Р.Л., Чурилов С.А. Противодействие экстремизму и терроризму в сети Интернет и образовательной среде // Обзор.НЦПТИ. 2016. № 7. С. 34-39.

4. Мозговой В.Э. Особенности информационной экстремистской деятельности: социологический анализ // Вестник КГУ. 2014. № 7. С. 220-224.

5. Новые правила: как VPN-сервисы относятся к запрету на обход блокировок. URL: https://vc.ru/28288-novye-pravila-kak-vpn-servisy-otnosyatsya-k-zapretu-na-obhod-blokirovok (дата обращения: 05.11.2017).

6. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.

7. Чурилов С.А., Быкадорова А.С. О противодействии распространению и профилактике радикальных идеологий в молодежной среде и сети Интернет // Обзор.НЦПТИ. 2016. № 8. С. 39-43.