

Профилактика экстремизма и терроризма, осуществляемого с помощью сети Интернет*

В.В. Поляков

Алтайский государственный университет (Барнаул, Россия)

Prevention of Extremism and Terrorism Carried Out with the Help of the Internet

V.V. Polyakov

Altai State University (Barnaul, Russia)

Проанализированы причины тенденции совершения экстремизма и терроризма с помощью сети Интернет. Исследованы формы использования Интернета в экстремистских и террористических целях, в частности конспиративного общения участников таких сообществ, вербовки новых членов, дистанционного управления подобными криминальными сообществами и сбора денежных средств на преступные цели. Проанализирована проблема использования сети Интернет преступниками для исследования ими общественного мнения и психологии людей, отличающихся социальной нетерпимостью. Описаны тенденции развития исследуемой преступной деятельности, проанализированы формы совершенствования способов ее осуществления. Выдвинуто суждение о необходимости выработки системы криминалистических мер предупреждения таких преступлений, основанной на правовых, организационных, технических и методических мерах. Предложена специализированная программа профилактики таких преступлений. Описаны основные мероприятия, которые должны в нее входить, в частности по выявлению, фиксации и блокированию материалов экстремистского характера. С целью выяснения механизмов совершения таких преступлений, их следовой картины, данных о личности преступников, а также других криминалистически значимых вопросов предложено разработать и внедрить исследовательскую систему Honeypot.

Ключевые слова: экстремизм, терроризм, оперативно-разыскная деятельность, криминалистика, профилактика преступлений.

DOI 10.14258/izvasu(2016)3-26

Сеть Интернет в нашей стране становится мощным средством преступной деятельности. Эта тенденция в полной мере коснулась экстремизма

The article analyses the reasons for the trends of extremism and terrorism committed via the Internet. The research is made of the forms of the Internet use for terrorist and extremist purposes, in particular, conspiratorial communication between members of these communities, the recruitment of new members, remote control of such criminal communities and collection of funds for criminal purposes. Analysis is given of the problem of the Internet use by criminals to study the public opinion and the psychology of people with social intolerance. The description is given to the trends of criminal activity under study; analysis is made of improving the methods of its implementation. The author comes up with the judgment about the need for a system of forensic measures to prevent such crimes, based on the legal, organizational, technical and methodological measures. A specialized program of crime prevention is offered.

The article describes the main activities to be included in it, in particular, identification, fixing and blocking materials of extremist nature. To clarify the mechanisms of such offenses, their trace picture, the identity of these criminals, and other forensically relevant questions, the offer is made to develop and implement the Honeypot research system.

Key words: extremism, terrorism, operatively-search activity, criminalistics, crime prevention.

и терроризма [1, с. 178–185]. Использование телекоммуникационных сетей предоставляет преступникам ряд преимуществ. К их числу относятся:

* Публикация подготовлена в рамках поддержанного РГНФ научного проекта № 16-33-01160.

простой доступ к информационным ресурсам независимо от географического местонахождения преступников и их жертв; практически полное отсутствие ограничений потенциальной аудитории адресатов информации, что позволяет с высокой скоростью передавать большие информационные массивы; передача информации по таким каналам связи контролируется правоохранительными органами со значительными трудностями, в частности, в силу крайне низкой персонализации электронно-цифровых следов-последствий [2, с. 146–152].

Экстремисты и террористы используют сеть Интернет в своей организационной деятельности [3, с. 10–16]. Это позволяет им более безопасно общаться и передавать данные. Возможна ситуация, когда преступники почти не обладают реальной информацией о соучастниках своей группы или сообщества, что объясняется конспиративными целями.

Сеть Интернет позволяет преступным формированиям легко и масштабно вербовать новых членов или собирать денежные пожертвования от лиц, им симпатизирующих. В последнее время к экстремистским объединениям стали чаще присоединяться образованные молодые специалисты, имеющие незаурядные знания в области компьютерной техники и сетевых технологий [4, с. 113–114]. Во многом это объясняется тем, что неудовлетворенные какими-то жизненными ситуациями молодые люди желают вступить в кажущиеся им сильными экстремистские или террористические объединения, чтобы применить в них свои знания и способности. За счет этого в значительной мере совершенствуются способы и приемы преступной деятельности, что ставит ее на более высокий уровень. Для правоохранительных органов крайне сложно расследовать преступления, в которых используются такие современные технологии, как VPN, Tor, анонимные прокси-серверы, так как они крайне эффективно препятствуют получению доказательств личного участия преступников в содеянном [5, с. 162–166].

На различных сайтах, особенно в социальных сетях и на страницах тематических форумов, ведется фактическое управление криминальными сообществами экстремистской и террористической направленности. Там декларируются идеология и внутренние правила, выстраивается иерархия участников, собираются средства для достижения идеологических целей, описываются действительные или вымышленные достижения и возможности, вербуются новые участники, агитируется призыв к совершению «оправданных» преступлений, планируются и готовятся экстремистские и террористические акции, размещаются всевозможные запрещенные законом методические материалы, например об изготовлении средств совершения преступлений. Важной задачей, решаемой преступниками посредством сети

Интернет, является широкое освещение проведенных акций, что позволяет обрести известность среди большего числа людей, устрашить общество, заставить с собой считаться [6, с. 26].

Надо отметить, что сеть Интернет используется преступниками для проведения собственных исследований общественного мнения и психологии людей, отличающихся социальной нетерпимостью. Для этого применяется специально разработанное программное обеспечение, собирающее определенную информацию на автоматизированном уровне. Объектом подобного изучения, как правило, являются сведения, размещаемые на страницах социальных сетей. Итогом сбора и анализа становится выработка конкретных эффективных форм работы с людьми, склонными к экстремизму или терроризму.

Полагаем, что важно осуществлять борьбу с экстремизмом и терроризмом, использующими возможности сети Интернет, не только постфактум, но и в рамках криминалистического предупреждения. Для этого необходима выработка системы соответствующих правовых, организационных, технических и методических мер, носящих комплексный характер. Особую роль стоит отвести созданию специализированной программы профилактики таких преступлений. Ее основная функция должна быть сосредоточена на повышении уровня правовой культуры населения и противодействии распространению информации экстремистской или террористической направленности на популярных интернет-ресурсах. Простое закрытие сайтов, содержащих запрещенный контент, как это происходит в настоящее время, имеет низкую результативность. Полагаем, что применение специализированной программы профилактики таких преступлений будет более эффективным.

Перечислим основные мероприятия программы профилактики экстремизма и терроризма, осуществляемых в сети Интернет.

1. Выявление материалов экстремистского характера в социальных сетях, например «ВКонтакте», «Одноклассники», «Facebook» и других, а также на форумах сайтов, включая любую информацию, имеющую экстремистскую или террористическую направленность [7, с. 60].

2. Фиксация такой информации. Определение ее источников, средств размещения, адресатов и иных значимых сведений для оперативно-разыскной или доказательственной работы.

3. Блокирование в определенных ситуациях такого контента или сайтов.

4. Выработка принципов и механизмов взаимодействия различных государственных и общественных организаций, активных представителей социальных групп населения, которые могут выступить в качестве общественных помощников, возможно, в рамках конкретных объединений (например, выс-

ших учебных заведений) с органами, уполномоченными производить расследование и предупреждение экстремистской и террористической деятельности. Сообщение или предоставление выявленной в сети Интернет информации, полагаем, может быть осуществлено анонимно.

5. Проведение профилактической работы с владельцами интернет-ресурсов, подверженных использованию в преступных целях, их правовое просвещение, в частности, затрагивающее сообщение о наступлении ответственности за размещение незаконных материалов.

6. Активное информационное противодействие экстремизму и терроризму на различных сайтах в сети Интернет. Для этого требуется организация тематических групп, форумов, опросов общественного мнения и подобных мер. Просвещение о негативном влиянии экстремизма и терроризма на общество и государство должно исходить не только от лица государственных органов, но и от общественных и религиозных объединений. Граждан необходимо призывать к неравнодушию и социальной активности в желании устранить подобные настроения в своей среде общения.

7. Требуется разработка и широкое внедрение исследовательской системы *Noneurot*. Ее суть заключается в том, что эта компьютерная программа устанавливается на отдельный сервер или виртуальную систему (сайт, страницу пользователя социальной сети и пр.), к которой намеренно предоставляется относительно легкий доступ потенциальным преступникам посредством заранее подготовленных уязвимостей. Далее действия преступников исследуются.

Происходит это путем технической работы набора средств и команд по собиранию информации, включающей в себя следующие данные: время запуска/остановки процессов, идентификатор процессов, данные о взаимодействии с другими процессами, дампы используемой памяти, а также в ряде случаев полный снимок данных, расположенных в оперативной памяти компьютера, и пр. За счет использования *Noneurot* могут быть достигнуты следующие результаты: выяснены механизмы совершения таких преступлений, их следовая картина, данные о личности преступников, объекты преступных посягательств и многие другие криминалистически важные вопросы.

Применение такой программы позволит более гибко и эффективно в юридическом и техническом отношении адаптироваться к изменяющимся способам совершения экстремизма и терроризма, осуществляемого в сети Интернет.

Существующая динамика и качественные изменения экстремизма и терроризма в сети Интернет свидетельствуют о неэффективности борьбы с данными социально негативными явлениями имеющимися методами. Представляется недооцененной роль профилактики совершения таких преступлений. Необходима выработка системы правовых, организационных, технических и методических мер предупреждения подобных преступлений с акцентом на создание единой программы мероприятий в этой области. Результатом таких мероприятий должно стать уже на раннем этапе снижение показателей экстремистских настроений и числа террористических актов, совершаемых в нашей стране.

Библиографический список

1. Сунами А.Н. Молодежный экстремизм, ксенофобия, интолерантное поведение: конфликтный анализ российского Интернета // Конфликтология. — 2013. — № 1.
2. Гавло В.К. Следовая картина и ее значение для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации // Российский юридический журнал. — 2007. — № 5 (57).
3. Осипенко А.Л. Организованная преступность в сети Интернет // Вестник Воронежского института МВД России. — 2012. — № 3.
4. Поляков В.В. Использование сети Интернет при совершении преступлений против детей // Сборник материалов криминалистических чтений. — 2014. — № 10.
5. Поляков В.В. Средства совершения компьютерных преступлений // Доклады Томского государственного

университета систем управления и радиоэлектроники. — 2014. — № 2 (32).

6. Осипенко А.Л. Особенности раскрытия преступлений экстремистской направленности, совершаемых в сети Интернет // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. — 2015. — № 1.

7. Кудашкин Я.В. Правовые аспекты противодействия терроризму в сети Интернет // Реализация государственной политики по противодействию терроризму и экстремизму в Российской Федерации: основные направления, проблемы и перспективы : материалы Всерос. науч.-практ. конф. «X Державинские чтения в Республике Мордовия» (Саранск, 25 апреля 2014 г.). — Саранск, 2014.