УДК 343.98.067

Кульпин Александр Евгеньевич
Санкт-Петербургский государственный университет
Юридический факультет
Россия, Санкт-Петербург
culpinsash@yandex.ru
Kulpin Alexander
St. Petersburg State University
Faculty of Law
Russia, St. Petersburg

КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ «БОТОФЕРМ» В ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация: автор рассматривает использование «ботоферм» и «фабрик троллей» в качестве особого способа совершения медиапреступлений. Особое внимание в работе уделено рассмотрению отличительных признаков ботов, используемых с целью совершения преступления в медиасреде. В статье анализируются особенности выявления и расследования преступлений, совершенных ботами, а также выдвигаются ряд предложений по повышению эффективности борьбы с ними, в качестве примера рассматривается организация под названием «Легион эльфов». В заключении выдвигается тезис о необходимости создания методики выявления, пресечения и расследования преступлений, совершенных ботами.

Ключевые слова: ботофермы, фабрики троллей, цифровые следы, сеть Интернет, оперативное внедрение, IP-адрес, Легион эльфов.

FORENSIC ASPECTS OF THE USE OF «BOTOFARMS» IN CRIMINAL ACTIVITY

Annotation: the author considers the use of "bot farms" and "troll factories" as a special way of committing media crimes. Particular attention is paid to the consideration of the distinctive features of bots used for the purpose of committing a crime in the media environment. The article analyzes the peculiarities of detection and investigation of crimes committed by bots, and also puts forward a number of proposals to improve the effectiveness of the fight against them, as an example, an organization called «Legion of elves» is considered. In conclusion, the thesis is put forward about the need to create a methodology for the detection, suppression and investigation of crimes committed by bots.

Key words: bot farms, troll factories, digital footprints, Internet, operational implementation, IP address, Legion of elves.

Возрастание роли виртуального пространства в повседневной жизни человека непосредственно отражается на большинстве сфер жизни, к которым относится и преступная деятельность. Особое значение в последние годы приобретают противоправные действия, совершаемые в медийном пространстве, так называемые медиапреступления. Под этим следует понимать преступления, в которых способом их совершения является информационное воздействие на сознание человека с помощью информационно-телекоммуникационных технологий с целью причинения ущерба законным интересами личности или общества. Под подобную характеристику попадает целый ряд составов, предусмотренных Уголовным Кодексом Российской Федерации, а именно п. д) ч.2 ст.110 УК РФ; п. д) ч. 3 ст. 110.1 УК РФ; ч.2 ст.128.1 УК РФ; п. в) ч.2 ст.151.2 УК РФ; ч.2 ст.205.2 УК РФ; ст. 207.3 УК РФ и иные.

В качестве одной из разновидностей подобных преступлений можно выделить те, которые совершены с использованием «ботоферм» или по-другому «фабрик троллей». Приблизительным временем появления данного явления можно назвать начало 2000-х годов, где оно зародилось именно в

политическом пространстве в сети Интернет, в свою очередь существование «ботоферм» вполне можно назвать интернациональным явлением, что отмечает ряд исследователей, указывая на использование подобных структур в Китае, Израиле, Великобритании, России и многих других странах [6, с. 76-78]. Весьма точно на сущность и опасность этого феномена указывает Т.Е. Новицкая, по мнению которой, в тех случаях, когда были использованы «ботофермы», происходит непосредственная манипуляция общественным сознанием, что приводит к угасанию демократических институтов [7, с. 185].

В качестве наиболее показательного примера в данной работе стоит рассмотреть недавний скандал, связанный с так называемым «Легионом эльфов», являющимся проектом, который создан и финансируется Free Russia Foundation (признан Минюстом РФ нежелательной организацией), а также вероятно имеет отношение к Anti-Corruption Foundation International*, Inc (Фонд борьбы с коррупцией, признанный в России экстремистской организации и перенесший свою деятельность в США), признанному в России нежелательной организацией [14]. Исходя из информации о работе этого учреждения, которая попала в открытый доступ благодаря его бывшему сотруднику, предоставившему СМИ внутреннею переписку и документацию, данный проект попадает под признаки «ботофермы». Собственно, как верно подмечает А.В. Соколов: «Использование троллинговых ферм, в современной реальности является инструментом ведения информационной войны. Ботофермы программируются на определенное задание, чаще всего связанное с формированием определенных мнений, дискредитаций оппонентов и трансляцию дезинформации различной формы» [12, с. 62]. Данная организации полностью соответствует этой концепции, так как её деятельность заключается в основном в написании комментариев, носящих преимущественно антиправительственный и антироссийский характер, на различных информационных платформах. Если проанализировать комментарии, которые оставляли «эльфы», имеющиеся в выложенном архиве, то вполне можно

квалифицировать их действия по таким составам как публичное распространение заведомо ложной информации об использовании Вооруженных Сил РФ; публичные призывы к осуществлению террористической деятельности; публичные призывы к осуществлению экстремистской деятельности; публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации и другие.

По большому счету, «ботоферму» в ряде случае можно рассматривать как преступное сообществу в виду наличия большого количества ключевых признаков для данной квалификации. Если говорить о «Легионе эльфов», то в этом случае имеется высокая степень организованности, четкое распределение ролей, многоуровневость (разделение на комментаторов, кураторов и т.д.), масштабность деятельности (наличие офисов в нескольких странах, в том числе Грузии и Литве), общая материально-финансовая база (спонсирование от Free Russia Foundation), согласованность действий участников (у всех комментаторов имеется общая «методичка» с необходимыми тезисами).

Если говорить о расследовании преступлений, совершенных с использованием ботов, то в самом начале перед нами встаёт проблема именно выявления ботов в общей массе пользователей соцсетей и иных информационных платформ. К.С. Князев выделяет следующие признаки, которые могут определить платного комментатора: числовое соотношение репостов к оригинальным постам, дата создания аккаунта, случайность имени пользователя и другие. Однако, куда надежнее будет получение внутренних инструкций, списков троллей или же сентиментальный анализ [1, с. 49].

После распознавания в комментаторе сотрудника «фабрики троллей» перед следствием встает необходимость выяснения не только его личности, но и местонахождения его рабочего места. Связано это с тем, что слово «фабрика» применяется к данному феномену по причине частого сходства с производством, разбитым на большее количество подразделений, имеющим

специальные службы контроля и работающим безостановочно, поэтому работники для выполнения своих обязанностей должны находиться на рабочем месте и строго соблюдать дисциплину [6, с. 79]. Собственно, в качестве особенности можно указать то, что, как правило, «тролль» имеет стационарное рабочее место, где также ведут свою деятельность и другие сотрудники «фабрики троллей», что определенно представляет интерес для следствия, поэтому установление местонахождения «ботофермы» имеет первостепенное значение.

Учитывая тот факт, что преступления совершаются ботами именно в виртуальном пространстве, то особое значение для следственных органов имеет обнаружение и фиксация цифровых (виртуальных) следов. Под ними понимают «криминалистически значимую компьютерную информацию о событиях и действия, отраженных в материальной среде, в процессе возникновения данной информации, ее обработки, хранения и передачи» [9, с. 179]. Однако, ряд исследователей выделяют эти следы отдельную группу, разграничивая их с материальными и идеальными, поскольку само отображение происходило теперь не в памяти человека или в материальном мире (рядом учёных данное обстоятельство активно оспаривается), но в исключительно новой среде, именуемой как киберпространство, виртуальное пространство, информационная среда [8, с. 174].

Основной проблемой расследования подобных преступлений можно назвать то, что для обнаружения и фиксации цифровых следов следствию приходится полагаться на такие «традиционные» действия как обыск, осмотр места происшествия, осмотр предметов, выемка, а если говорить об оперативно-розыскных мероприятиях: исследование, снятие информации с технических каналов связи, получение компьютерной информации, сбор образцов для исследования, оперативный эксперимент [9, с. 180]. Собственно, можно отметить, что на данный момент при проведении расследования преступлений в медиапространстве основной упор делается на работу с

электронным устройством, которое было орудием преступления, что отмечается исследователями, указывающими на то, что изъятие носителя чаще всего является одним из условий выявления и исследования компьютерной информации [3, с. 150].

Пожалуй, отдельно стоит остановиться на таком оперативно-розыскном мероприятии как получение компьютерной информации, предусмотренном п.15 ст.6 Федеральный закон от 12.08.1995 N 144-ФЗ «Об оперативно-розыскной деятельности». На сегодняшний день получение подобной информации возможно с помощью удаленного подключения к компьютеру подозреваемого в процессе его работы, но только по поручению следователя и с разрешения суда, что определенно отражается на скорости и эффективности расследования. Следовательно, в изменении данной ситуации заинтересованы и правоохранительный органы, особенно Министерство внутренних дел, которое разработало поправки к Федеральному закону «Об оперативно-розыскной деятельности», позволяющие получить удаленный доступ к электронным устройствам до разрешения суда в связи с нехваткой инструментов, которые позволяли бы оперативно и в режиме реального времени исследовать текстовые, аудио- и видеоданные, а также техническую информацию о месте и времени удаленного подключения, оборудовании, включая его модель, сетевой и физический адрес, серийный номер, а также сведения о взаимодействии пользователя с информационными системами и их реакции на запросы пользователя [13]. В действительности, подобные предложения не лишены основания, поскольку даже в документах «Легиона эльфов» можно найти сведения, указывающие на использование различных средств с целью сохранения анонимности в сети «Интернет», в том числе речь идёт об активном использование VPN-сервисов, что является обязательным требованием в работе каждого «эльфа», что затрудняет работу следственных органов, а следовательно необходимо получать криминалистически важную информацию в кратчайшие срок.

Отдельно следует рассмотреть установление IP-адреса в ходе расследования преступлений с использованием ботов. Исследователь К.С. Сидорова предлагает рассматривать IP-адрес, под которым понимается уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP, в качестве одного из специфических идентификаторов человека в виртуальной среде [10, с. 84]. Однако формальный подход к расследованию и поспешное обвинение человека, на чьей устройство указывает IP-адрес, будет являться ошибочным. В заблуждение следственные органы может ввести так называемый IP-спуфинг, который представляет из себя использовании чужого IP-адреса источника с целью обмана системы безопасности. Помимо этого, в определенных случаях может совпадать динамический IP-адрес, который назначается провайдером автоматически каждый раз при подключении к сети и вполне возможно, что под одним и тем же адресом в разное время суток в сети «Интернет» находились разные пользователи, поэтому необходимо учитывать время совершения преступления, так как в практике известны случаи, когда в совершении преступления пытались обвинить людей к нему непричастных как раз из-за неучета данного фактора [2, с. 77]. Также совпадения IP-адреса возможно при использовании точки доступа к Wi-Fi, к которой может подключиться несколько устройств, и не стоит исключать вероятность того, что злоумышленник использует чужое электронное устройства. В любом случае, для расследования подобных преступлений оптимальной будет следующий алгоритм: установление IP-адреса; установление устройства, на которое указывает IP-адрес; выявление виновного лица.

Собственно, в качестве возможных способов установления IP-адресов исследователями указывается следующее: 1) направление запроса в адрес компании-провайдера, осуществляющей услуги доступа к сети «Интернет» по определенному физическому адресу; 2) направление запроса администрации сайта, на котором зарегистрирован интересующий следователя пользователь в

рамках расследования уголовного дела; 3) проведение следственных действий с целью установления IP-адреса; 4) направление поручения органу дознания об установлении IP-адреса конкретного соединения (й) по обстоятельствам совершенного преступления [11, с. 88-89]. Стоит понимать, что злоумышленники, в том числе сотрудники «ботоферм», активно противодействует тому, чтобы их вычислили подобным образом, что требует привлечения специалистов с соответствующей компетенцией и разработки дополнительных способов установления IP-адресов.

Несмотря на всё вышесказанное, ключевой проблемой, связанной с расследование преступной деятельности «ботоферм», можно назвать их расположение на территории недружественных государств, если говорить о «Легионе эльфов», то речь идёт о Грузии и Литве, что практически лишает российские правоохранительные органы возможности провести подавляющую часть необходимых действий, в том числе изъятие электронных устройств и получение компьютерной информации удаленным путем, что связано с особой ролью «ботоферм» и «фабрик троллей», которые, как правило, являются инструментами информационной войны, поэтому не стоит ожидать, что правоохранители данных государств будут активно сотрудничать с российскими коллегами в данных случая. Собственно, именно это и берут в расчет организаторы подобных проектов, располагая свои структуры за пределами Российской Федерации.

В качестве возможного решения данной проблемы стоит предложить более активное применение оперативного внедрения, предусмотренного в статье 6 ФЗ «Об оперативно-розыскной деятельности». В качестве особенностей данного оперативно-розыскного мероприятия исследователи отмечают, что «сущность данного мероприятия состоит не только в проникновении в криминальную среду (подразумевается внедрение в преступные группы, организации, сообщества, на объекты оперативной заинтересованности), осуществление разведывательной по сути работы, но и

закрепление в ней лица, обладающего определенными социально значимыми свойствами, что позволяет не только своевременно получать достоверную оперативную информацию, но и оказывать воздействие на происходящие в данной среде процессы» [4, с. 156].

В практике выделяются два вида данного мероприятия на основании способа внедрения: «1) Внедрение в преступное сообщество сотрудников оперативных подразделений органов дел или лиц, оказывающих им содействие на конфиденциальной основе; 2) приобретение оперативно-розыскным органом конфиденциального источника информации из числа лиц, уже находящихся в криминальной среде» [4, с. 156-157].

Если же говорить о разделение в зависимости от субъекта оперативного внедрения, то можно указать следующие виды: «1) оперативное внедрение «негласно» штатных засекреченных сотрудников правоохранительных структур; 2) проведение операций против преступников штатных представителей служб МВД и ФСБ, не засекреченных по своей работе; 3) оперативная деятельность лиц, не являющихся сотрудниками силовых структур, но тесно с ними взаимодействующими» [5, с. 208].

Как уже было указано ранее, по своей структуре «ботоферма» подпадает под признаки преступного сообщества, поэтому достаточно закономерно можно предположить, что использование оперативного внедрения будет крайне эффективно не только из-за возможности выяснить цели и методы работы конкретной организации, но также вероятности установить личности ряда сотрудников «ботофермы», поскольку работа бота, в большинстве случаев, предполагает нахождение в определенном месте с другими ботами во время осуществления деятельности, что позволяет внедренному установить контакт с «коллегами» и выяснить их личные данные. Помимо этого, внедренный информатор может являться способом установления личности кураторов «ботофермы» благодаря непосредственному контакту с ними во время работы, их выявление представляет из себя более приоритетную задачу для

правоохранительных органов, чем установление данных постоянно меняющихся рядовых сотрудников, так как кураторы занимают более высокое место в преступной иерархии и через них в свою очередь можно выйти на заказчиков преступлений, что в свою очередь дает возможность нейтрализовать всю организацию. Если учитывать тот факт, что многие «ботофермы», действующие против Российской Федерации, располагаются на постсоветском пространстве и рекрутируют туда преимущественно выходцев из России, то потенциал для использования оперативного внедрения достаточно высок.

Подводя итоги, активное использование «ботоферм» и «фабрик троллей» в современном медиапространстве представляет из себя особый способ осуществления преступной деятельности, поэтому перед криминалистами стоит задача по разработке и усовершенствованию методики выявления, пресечения и расследования преступлений, совершаемых с применением ботов. Основную роль в данном случае будет играть стремительно развивающаяся цифровая криминалистика, связанная с обнаружением и фиксацией цифровых следов. Однако, большое значение продолжают иметь и более традиционные следственные действия и оперативные мероприятия, от обыска до оперативного внедрения.

Список литературы:

1. Князев К.С. Астротурфинг и призывы в сети Интернет к участию в общенациональных уличных протестах в Российской Федерации // Гуманитарные, социально-экономические и общественные науки. – 2021. – №7(1). – С.48-50.

2. Кувычков С. И. К вопросу об использовании электронной информации в уголовно-процессуальном доказывании: теоретико-прикладной аспект // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2015. – №2(30). – С.76-81.

3. Ланцова А.В. Проблема виртуального следа в цифровой криминалистике //Международный журнал гуманитарных и естественных наук. – 2020. – №12-3(51). – С.149-151.

4. Лузько Д.Н. Некоторые правовые и тактические аспекты проведения оперативного внедрения // Вестник Сибирского юридического института МВД России. – 2021. – №4(45). – С.155-160.

5. Макарова Д.А., Дрыгина Т.А. Проведение оперативно-розыскного мероприятия «оперативное внедрение» // E-Scio. – 2022. – №6(69). – С.205-209.

6. Мартьянов Д.С. Политический бот как профессия // ПОЛИТЭКС. – 2016. – Том 12. – №1. – С.74-89.

7. Новицкая Т. Е. Агентность и отчуждение в условиях цифрового капитализма // Труды БГТУ. Сер. 6, История, философия. – 2023. – № 1 (269). – С. 181–186.

8. Переверзева Е. С., Комов А. В. Виртуальные и цифровые следы: новый подход в понимании // Вестник Санкт-Петербургского университета МВД России. – 2021. – № 1 (89). – С. 172–178.

9. Семикаленова А.И., Рядовский И.А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. – 2019. – №6(103). – С.178-185.

10. Сидорова К.С. IP-адрес как один из идентификаторов личности в расследовании преступлений // Психопедагогика в правоохранительных органах. – 2018. – № 3(74). – С. 84–87.

11. Сидорова К.С. Способы установления IP-адреса и сведений о нем при расследовании уголовных дел // Вестник Сибирского института бизнеса и информационных технологий. – 2018. – №2(26). – С.88-92.

12. Соколов А.В. Генезис и эволюция категории «фейковые новости» // Социально-гуманитарные знания. – 2022. – №7. – С.61-64.

13. Добрунов М. МВД попросило доступ к устройствам до разрешения суда [Электронный ресурс] // ежедневная аналитическая газета РБК. 2023. 16 августа. URL: https://www.rbc.ru/society/16/08/2023/64dc0fb49a794714d5e55314/ (дата обращения 05.02.2024)

14. Казаков И. «Фабрика эльфов»: что это такое, кому принадлежит, чем отличается от «фабрики троллей» [Электронный ресурс] // интернет-газета Фонтанка.ру. 2023. 16 ноября. URL: https://www.fontanka.ru/2023/11/16/72920387/ (дата обращения: 05.02.2024).