Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2021, 4: 7–11

АКТУАЛЬНАЯ ТЕМА

DOI 10.26163/GIEF.2021.70.94.001
УДК 343.985:343.2:004.738.5

A.G. Akhmedov, T.O. Boziev

OPERATIONAL SEARCH COUNTERACTION TO INTERNET CRIMES: ISSUES AND PROBLEMS

Akhmed Akhmedov – professor, the Department of Operational-Investigative Activity in Internal Affairs Agencies, St. Petersburg University of the Ministry of Internal Affairs of the Russian Federation, PhD in Law, associate professor, St. Petersburg; **e-mail: Osnaz82@yandex.ru**.
Taulan Boziev – Head of the Department of Criminal Law, State Institute of Economics, Finance, Law and Technology, PhD in Law, associate professor, Gatchina; **e-mail: boziev1975@yandex.ru**.

In recent years, our state and society have faced a grave problem of rise in crime resulting from the sanctions introduced by the USA and other countries, restrictions and prohibitions due to the pandemic of COVID-19, political and socio-economic transformations taking place in the country. The biggest growth is seen in the amount of crimes relying on technological progress and advancements, which makes the crime powerful and largely professional. New types of Internet crime have appeared, ways of committing and concealing crimes have become more sophisticated. We look at problems concerning operational search counteraction to the crimes in question.

***Keywords**: crimes relying on technological progress and advancements; Internet crime; operational search activities in the Internet; operational surveillance; operational search; operational search control; operational search monitoring; deep Web; darknet.*

А.Г. Ахмедов, Т.О. Бозиев

ОПЕРАТИВНО-РОЗЫСКНОЕ ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ: ВОПРОСЫ И ПРОБЛЕМЫ

Ахмед Гусейнович Ахмедов – профессор кафедры ОРД в ОВД, Санкт-Петербургский университет МВД России, кандидат юридических наук, доцент, г. Санкт-Петербург; **e-mail: Osnaz82@yandex.ru**.
Таулан Османович Бозиев – зав. кафедрой уголовно-правовых дисциплин, Государственный институт экономики, финансов, права и технологий, кандидат юридических наук, доцент, г. Гатчина; **e-mail: boziev1975@yandex.ru**.

Последние годы в условиях санкций, введенных США и другими странами, а также в условиях ограничений и запретов, связанных с COVID-19, общественно-политических и социально-экономических преобразований, которые происходят в нашей стране, государство и общество столкнулось с серьезной проблемой роста преступности. Прежде всего, это рост преступлений, совершаемых с использованием достижений науки и техники, что превращает преступность в организованную и в значительной степени профессиональную силу. Появились ранее не встречавшиеся преступления с использованием сети Интернет, стали более изощренными способы совершения и сокрытия преступлений. В статье рассмотрены проблемы, связанные с оперативно-розыскным противодействием таким преступлениям.

***Ключевые слова**: преступления, совершаемые с использованием достижений науки и техники; преступления с использованием сети Интернет; оперативно-розыскные мероприятия в сети Интернет; оперативное наблюдение; оперативный поиск; оперативно-*

розыскной контроль; оперативно-розыскной мониторинг; глубокий Интернет (deep web); теневой Интернет (darknet).

Глобальные компьютерные сети до последнего времени не попадали в поле зрения правоохранительных органов и, соответственно, не рассматривались в качестве объектов оперативно-розыскного воздействия. Если и проводилась оперативно-розыскная работа в сети Интернет, то она была направлена на противодействие преступлениям экстремистской направленности. За последние 2 года существенно выросло количество зарегистрированных преступлений, совершаемых с использованием достижений науки и техники [6]. В связи с этим назрела необходимость глубокого и всестороннего изучения, исследования и разработки оперативно-розыскной политики и проявления воли государства по отношению к преступности в целом и преступлениям, совершаемым с использованием высоких технологий в частности.

Статистические данные зарегистрированных преступлений в сфере высоких технологий показывают значительный рост. По сравнению с прошлым годом в г. Санкт-Петербурге число зарегистрированных случаев мошенничества выросло вдвое, в Москве – на 76%, в Свердловской области – на 60% [8].

Приходится констатировать, что в настоящее время для данного направления деятельности органов внутренних дел характерно использование стереотипных методов и приемов, не учитывающих особенности новых видов преступлений, слабое методическое обеспечение оперативно-розыскной деятельности в глобальных компьютерных сетях, недостаточный уровень профессиональной подготовки сотрудников оперативных подразделений, занимающихся противодействием преступлениям, совершаемым с использованием сети Интернет.

В то же время в условиях интенсификации потоков информации, передаваемых по открытым линиям связи, и переводе многих сфер жизнедеятельности в электронную сферу, использование глобальных компьютерных сетей оказывает значительное влияние на изменение сущности, характера и содержания оперативно-розыскных мероприятий.

В последнее время в связи с распространением COVID-19 возрастает роль дистанционного управления с использованием сети Интернет во многих сферах жизнедеятельности, будь то организация удаленный рабочих мест, образование с применением электронного обучения и дистанционных образовательных технологий, удаленная медицинская диагностика и консультация, удаленное управление финансами и т.д. При этом отсутствие отлаженных правовых механизмов регулирования перечисленных выше областей позволяет совершать преступления в сетевом пространстве. Поэтому с оперативно-розыскной точки зрения сетевое пространство должно быть отнесено к специфическим криминогенным объектам и в качестве такового требует повышенного внимания со стороны оперативных подразделений.

Обстоятельствами и факторами, влияющими на организацию и тактику осуществления оперативно-розыскных мероприятий в сети Интернет, являются нарастающая сложность инфраструктуры современных сетей и сетевых процессов; возможность анонимной деятельности в сети Интернет; влияние глобальных компьютерных сетей на состояние национальной безопасности; отсутствие единой организации, координирующей деятельность сети Интернет; надгосударственный характер данной сети.

Развитие преступности с использованием Интернета и высоких технологий как организованной профессиональной деятельности требует совершенствования всех направлений борьбы с ней. Данные о преступлениях, совершаемых с использованием современных технологий, показывают, что в настоящее время раскрытие преступлений, особенно совершаемых организованными преступными группами с использованием сети Интернет, невозможно без широкого, продуманного ис-

пользования возможностей оперативно-розыскной деятельности (далее – ОРД). Такие преступления не только не могут быть раскрыты, но также становится невозможным их выявление и предупреждение. Это подтверждают статистические данные, показывающие значительный рост преступлений, совершаемых с использованием сети Интернет, и высокая латентность таких преступлений [10].

Для оперативно-розыскной практики преступления в глобальных компьютерных сетях представляют собой достаточно новое явление.

Решение задач по выявлению в глобальных сетях криминогенного контингента и признаков преступной деятельности требует специфических знаний оборота информации в сети Интернет и постоянного творческого подхода. Оперативно-розыскное наблюдение за обстановкой предполагает постоянный мониторинг и непрерывный сбор информации, поступающей из различных источников. Как свидетельствует практика, интенсивность поступающей информации зависит от профессионализма сотрудников, правильного осуществления ряда мер, касающихся определения информационного поиска, обеспечения этого участка работы необходимыми силами и средствами. Значительный рост совершенных преступлений с использованием сетевого пространства показал отсутствие своевременной реакции правоохранительных органов на происходящие криминальные процессы. Поэтому уже на начальных этапах оперативного поиска важно провести изучение структуры обслуживаемых сетей, определить перечень существующих в них информационных источников. К таким источникам могут быть отнесены:

- сообщения операторов связи, служб безопасности и администрации обслуживаемых объектов;

- заявления и сообщения граждан на специально организованных сайтах;

- места сетевого общения в реальном времени;

- сообщения от других субъектов оперативно-розыскной деятельности;

- сообщения от других субъектов оперативно-розыскного обслуживания глобальных сетей, зарубежных правоохранительных органов;

- публикации в сетевых средствах массовой информации, в сетевых конференциях и др.

Получение оперативно значимой информации непосредственно на сетевых объектах будет наиболее эффективным при применении таких приемов, как установление личного контакта с сотрудниками; проведение на объектах целевых мероприятий по выявлению признаков противоправной деятельности, изучение документов, направление запросов.

Информация, поступающая из перечисленных источников, способствует выявлению в глобальных сетях криминогенного контингента. Чтобы сузить круг изучаемых субъектов, важно учитывать поведенческие признаки лиц, склонных к совершению сетевых преступлений. При этом среди них основное внимание следует уделять гражданам:

- попадавшим в поле зрения полиции в связи с совершенными сетевыми преступлениями;

- подозреваемым в причастности к сетевым преступлениям;

- имеющим связи с представителями организованных преступных сообществ;

- высказывающим намерение совершить сетевое преступление или склоняющим к этому других;

- связанным с вышеназванными категориями граждан.

Представляет интерес изучение специфических приемов практического применения изучения криминогенного контингента, успешно применяемых ФБР в местах сетевого общения. Так, легендированная переписка в Интернете в рамках программы «Innocent Images» позволила сотрудникам ФБР, работавшим под видом детей, произвести задержание в период с 2014 по 2019 гг. более 50 педофилов [4].

Анализ материалов дел оперативного учета, а также интервьюирование специалистов позволяют определить несколько способов выявления подготавливаемых и совершаемых преступлений на сетевых пространствах. К ним могут быть отнесе-

ны уже упоминавшиеся: получение информации от администрации и службы безопасности объекта, мониторинг содержимого сайтов, контент-анализ сетевых конференций. Дальнейшего совершенствования требует тактика осуществления автоматизированного учета оперативно значимой информации.

Эффективным тактическим способом обнаружения признаков преступной деятельности является проведение целевых комплексных мероприятий на сетевых объектах. В ходе таких мероприятий обследуется системы безопасности, изучаются файлы регистрации событий (log-файлы[1]). При этом могут быть обнаружены признаки, указывающие на попытки сетевых вторжений: ошибки авторизации при входе в систему; регистрация пользователя в необычное время (например, когда он точно отсутствовал) или с необычного места; одновременная регистрация двух пользователей под одним именем или с одного места; появление новых учетных записей в регистрационных журналах; наличие скрытых файлов с вредоносными программами-«закладками» и поврежденных файлов; сравнение программ и устройств обнаружения сетевых вторжений.

Для реализации сигнальной функции важен сбор осведомительной информации о деятельности объектов, лиц и группировок, который должен начинаться еще до появления конкретных фактов или признаков преступления. С этой целью целесообразно осуществлять оперативно-розыскной контроль по двум направлениям: непосредственно в криминогенной сетевой среде и по объектовому признаку.

Наибольшим объемом информации обладают хакеры, владельцы сайтов криминальной направленности и т.п. Находясь в среде лиц, склонных к совершению сетевых преступлений, и пользуясь их доверием и своим авторитетом, такой конфидент[2] способен непосредственно выявить преступные намерения определенных ее участников. Иным путем это сделать трудно, поскольку такие субъекты, как правило, обеспечены необходимыми силами и средствами.

На обслуживаемых участках сетей обычно складывается определенный круг подобных лиц. Среди специфических тактических приемов их выявления можно выделить оперативно-розыскной мониторинг местных сетевых конференций. Такой прием связан с анализом всех сообщений, публикуемых в соответствующих конференциях, причем в отдельных случаях может осуществляться отбор сообщений по ключевым словам. Мониторинг позволяет получать сведения о намерениях участников, устанавливать их связи между собой, выявлять признанных лидеров, вести подбор. Рассматривая вопросы противодействия преступлениям, совершаемым с использованием сети Интернет, вне исследования правоохранительных органов остается так называемый «глубокий Интернет»[3].

Глубокий Интернет раскинулся под общедоступным пространством сети и включает около 90% всех веб-сайтов [11]. Эта невидимая часть айсберга находится «под водой» и намного превосходит по размерам общедоступный Интернет. По сути, эта скрытая часть настолько велика, что невозможно точно установить, какое количество веб-страниц или сайтов в ней активно в тот или иной момент времени.

Крупные поисковые системы можно сравнить с рыбаками на лодках, которые

[1] log-файлы – это текстовые файлы, в которых хранится информация о посещениях, параметрах посещений сайта и ошибках, которые возникали на нем.

[2] Конфидент – обобщенное название категории физических лиц, участников ОРД, которые на основании оперативно-розыскного законодательства были привлечены оперативно-розыскным органом для оказания ему конфиденциального содействия в достижении целей и решении задач ОРД и тем самым вступили с ним в правовые отношения.

[3] Глубокий интернет (deepweb) – сегмент Интернета, страницы и порталы которого не индексируются поисковыми системами (т.е. не определяются). Большинство deepweb-ресурсов – это информация, не предназначенная для широкого использования, такая как архивы компаний и государственных органов, каталоги, сервисы доступа к базам данных, библиотеки и тому подобное. Зайти на страницы deepweb возможно, используя стандартный браузер, но для этого нужно иметь прямую ссылку на ресурс.

могут поймать только веб-сайты, близкие к поверхности. Все остальное – от научных журналов до закрытых баз данных и нелегального контента – нашим «рыболовам» недоступно. Глубокий Интернет включает и так называемый теневой Интернет[4].

В связи с этим нами поддерживается предложение о необходимости реализации законодательной инициативы Министерства Внутренних Дел России о внесении в часть первую статьи 6 Федерального закона «Об оперативно-розыскной деятельности» изменения с целью дополнения перечня оперативно-розыскных мероприятий новым оперативно-розыскным мероприятием, предусматривающим проведение исследования компьютерной информации [9].

ЛИТЕРАТУРА

1. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (ред. 01.07.2021 г.) // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru/ (дата обращения: 12.11.2021).

2. Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи» (ред. 02.07.2021 г.) // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru/ (дата обращения: 12.11.2021).

3. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. 02.07.2021 г.) // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru/ (дата обращения: 12.11.2021).

4. Аморальные соцсети: ФБР ловит педофилов на живца // Forbes. 11.03.2019: [сайт]. URL: https://www.forbes.ru/tehnologii/373141-amoralnye-socseti-fbr-lovit-pedofilov-na-zhivca (дата обращения: 12.11.2021).

5. *Ахмедов А.Г., Бозиев Т.О.* Информационное обеспечение оперативно-розыскной деятельности в вопросах противодействия преступлениям, совершаемым юридическими лицами // Журнал правовых и экономических исследований. Journal of Legal and Economic Studies. 2017. № 1. С. 34–38.

6. В России за два года в полтора раза выросло число IT-преступлений // ТАСС. 11.10.2021: [сайт]. URL: https://tass.ru/proisshestviya/12628881 (дата обращения: 12.11.2021).

7. Криминология / под ред. А.И. Долговой. М.: ИНФРА-М-НОРМА, 1997. 784 с.

8. *Линделл Д. [и др.]*. Число дел о мошенничестве рекордно выросло на фоне пандемии. Каким преступлениям поспособствовала самоизоляция // РБК. 31.08.2020: [сайт]. URL: https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d (дата обращения: 12.11.2021).

9. МВД России предлагает дополнить перечень оперативно-розыскных мероприятий «исследованием компьютерной информации» // Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Glavnie_upravlenija/Glavnoe_upravlenie_jekonomicheskoj_bezop/Publikacii_i_vistuplenija/item/24427520/ (дата обращения: 12.11.2021).

10. МВД России публикует данные о состоянии преступности по итогам пяти месяцев 2021 года // Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/news/item/24738876 (дата обращения: 12.11.2021).

11. Что такое глубокий и теневой Интернет // Лаборатория Касперского: [сайт]. URL: https://www.kaspersky.ru/resource-center/threats/deep-web (дата обращения: 12.11.2021).

12. *Boziev T.O., Korotkov A.V., Sipyagina M.N., Intykbaev M.K.* IT crime: a virtual threat with real consequences // SHS Web of Conferences. IX Baltic Legal Forum «Law and Order in the Third Millennium». 2021. P. 03011.

[4] Теневой интернет (darknet) – часть deepweb, сегмент Интернета, который скрыт из общего доступа. Соединение в нем устанавливается между доверенными пирами (участниками) в зашифрованном виде, с использованием нестандартных портов и протоколов. В отличии от deepweb страницы darknet недоступны без применения специального программного обеспечения.