Научная статья
УДК 343
https://doi.org/10.36511/2078-5356-2022-4-249-254

Способы и методы деанонимизации лиц, совершающих преступления в информационном пространстве

Фарахиев Динар Минзеферович
Казанский юридический институт МВД России, Казань, Россия, farah1evd1nar@gmail.com

Аннотация. В настоящем исследовании автором рассматриваются способы и методы деанонимизаци лиц, совершающих преступления в информационном пространстве, предлагается авторское определение данного понятия.

В настоящем исследовании авторами проанализированы вопросы формирования новой криминалистической теории информационного обеспечения деятельности оперативных подразделений полиции. Особое внимание в исследовании отводится способам и методам, которые могут быть использованы оперативными подразделениями полиции в процессе деанонимизации лиц, совершающих преступления в информационном пространстве.

На основе анализа пассивных и активных методов деанонимизации лиц, совершающих преступления в информационном пространстве, а также использования возможностей *Big Data* авторы приходят к выводу, что органы внутренних дел могут эффективно использовать данные технологии с учетом высоких требований к профессиональным навыкам и умениям.

Ключевые слова: борьба с преступностью, деятельность оперативных подразделений, анонимность, методы, деанонимизация, информационное пространство, *Tor*, *spoofing*-атаки, *Big Data*

Для цитирования: Фарахиев Д. М. Способы и методы деанонимизации лиц, совершающих преступления в информационном пространстве // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4. С. 249—254. https://doi.org/10.36511/2078-5356-2022-4-249-254.

Original article

Ways and methods of deanonymization of persons committing crimes in the information space

Dinar M. Farakhiev
Kazan Law Institute of the Ministry of Internal Affairs of Russia, Kazan, Russian Federation,
farah1evd1nar@gmail.com

Abstract. This study examines the ways and methods of deanonymization of persons who commit crimes in the information space, the author's definition is proposed.

In this study, the authors analyzed the formation of a new forensic theory of information support for the activities of operational police units. Particular attention in the study is given to the ways and methods that can be used by operational police units in the process of deanonymizing persons who commit crimes in the information space.

Based on the analysis of passive and active methods of deanonymization of persons committing crimes in the information space, as well as using the possibilities of Big Data, the authors come to the conclusion that the internal affairs bodies can effectively use these technologies, taking into account the high requirements for professional skills and abilities.

Keywords: fight against crime, activities of operational units, anonymity, methods, deanonymization, information space, Tor, spoofing attacks, Big Data

For citation: Farakhiev D. M. Ways and methods of deanonymization of persons committing crimes in the information space. *Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia,* 2022, no. 4, pp. 249—254. (In Russ.). https://doi.org/10.36511/2078-5356-2022-4-249-254.

В настоящее время общество активно развивается, совершенствуются информационные технологии, что в результате приводит к существенной трансформации жизнедеятельности общества и государства в целом. Совершенствование цифровых технологий привело к тому, что у органов внутренних дел (далее — ОВД), в частности у оперативных подразделений полиции, появились новые источники приобретения оперативно-значимых сведений и доказательств в виде виртуальных следов преступления. Сегодня возникает новый эволюционный процесс социальной и экономической сфер жизни общества. Современная информационная среда — главнейший фактор мирового экономического развития.

В связи с развитием инновационных технологий и информационного пространства возрастает количество преступлений, совершаемых посредством информационно-телекоммуникационных технологий, модифицируются способы, алгоритмы и механизмы совершения преступлений. Согласно статистическим данным МВД России за 2021 год было зарегистрировано 517,7 тыс. преступлений, совершенных с использованием информационно-коммуникационных технологий, что на 1,4 % больше, чем за аналогичный период 2020 года [1]. Как было отмечено на расширенном заседании коллегии Министерства внутренних дел Российской Федерации (далее — МВД России): «Количество преступлений в этой сфере ежегодно растет» [2].

В литературе авторы рассматривают информационную преступность по-разному, разделяя ее на отдельные виды преступлений. Так, А. Е. Шалагин в своих исследованиях приводит классификацию преступлений, совершаемых посредством информационного пространства. Выделим наиболее распространенные из них: 1) кибертерроризм; 2) мошенничество; 3) секстория; 4) *spoofing*-атаки; 5) *cyberbullying*; 6) *phishing* [3, с. 131]. Так, О. И. Алпеева, А. В. Бушуева к вышеуказанным преступлениям, совершаемым посредством информационного пространства относит также: 1) наркопреступления; 2) экономическую преступность; 3) незаконный оборот оружия; 4) преступления, связанные с нарушением прав интеллектуальной собственности [4, с. 55].

Вопросом деанонимизации лиц, совершающих преступления в интернет-пространстве занимались: С. В. Тимофеев [5], Г. П. Афонькин [6], Ю. В. Гаврилин [7], С. И. Земцова [8] и др.

Согласно результатам исследования следует, что в правоприменительной практике имеются проблемы организационно-управленческого, юридического, тактико-специального, материально-технического и кадрового характера. Основной проблемой является деанонимизация пользователей информационного пространства, а именно получения персональных данных преступников, совершающих преступления с использованием информационно-телекоммуникационных технологий. Так, большое внимание в процессе установления лиц, совершающих преступления в интернет-пространстве, отводится методам деанонимизации пользователей сети *"Tor"*. Актуальностью вышесказанного подтверждает тот факт, что уже в 2014 году МВД России объявило тендер на раскрытие данных пользователей [9].

В практике имеются определенные условия, при соблюдении которых возможна деанонимизация пользователей сети *"Tor"*. В свою очередь, А. В. Лазаренко предлагает разделение методов деанонимизации на пассивные и активные атаки [10, с. 258]. Первая категория методов, как правило, не модифицирует трафик, а только анализирует его; вторая категория — осуществляет все в совокупности. Рассмотрим подробнее методы деанонимизации пользователей сети *"Tor"* на примере пассивных и активных атак.

Пассивные методы деанонимизации информационных преступников.

Большой интерес в пассивных методах деанонимизации представляют *timing*-атаки, которые являются самыми ранними методами деанонимизации пользователей. *Timing*-атака представляет собой разновидность атаки по сторонним каналам, посредством которой атакующий предпринимает попытки скомпрометировать систему исходя из анализа временного промежутка, который тратится на осуществление операции. В случаях, когда атакующий имеет средства наблюдения «пользовательского трафика» и трафика конечной точки соединения, соответственно возникает возможность соединения между ними. В целях использования *timing*-атаки атакующий должен быть снабжен коррумпированным узлом, под которым следует понимать узел, трафик которого имеет возможность модифицировать и анализировать пользователя. Данный узел обладает возможностями соединения с иными узлами сети *"Tor"*; осуществляет мониторинг задержек данной сети; устанавливает шаблоны трафика и др.

Следующей интересной пассивной атакой является *circuit fingerprinting*, которая представляет из себя современную комбинированную атаку. Данная разновидность атаки направлена

на установление взаимосвязи пользователей сети *"Tor"* с ее «теневой службой». В тот момент, когда между пользователями сети *"Tor"* и ее «теневой службой» установлена активность, используется *WF*-атака, которая представляет собой атаку, позволяющую установить посещаемые пользователем площадки сети.

Механизм данного метода деанонимизации выглядит следующим образом:

1. Определение связи (цепи) между пользователями сети *"Tor"* и ее «теневой службой» (характеристиками соединения участников являются: длительная активность; количество сообщений; последовательность).

2. После определения цепи необходимо получить доступ к входному узлу пользователя сети *"Tor"*, которого необходимо деанонимизировать.

Активные методы деанонимизации информационных преступников

Raptor-атака так же, как и атака *circuit fingerprinting* является относительно новой технологией деанонимизациеи лиц, совершающих преступления в информационном пространстве. Данный метод атаки включает в себя ряд элементов:

1) асимметричный анализ трафика пользователей;

2) анализ натуральных перебоев;

3) атаки *BGP*-хищений и *BCP*-прослушивания.

Следующим активным методом деанонимизации является *DoS*-атаки, которые включают в себя следующую разновидность атак: *"packet spinning"*; атака перегрузки посредством длинных путей; *DoS*-атака *CellFlood*. Первая атака связана с принуждением пользователя сети *"Tor"* выбирать коррумпированные узлы посредством повреждения легитимных узлов. Атака будет считаться эффективной, если пользователь сети *"Tor"* выбирает только определенные атакующим коррумпированные узлы цепи. Вторая атака основывается на определенных характеристиках сети *"Tor"*, к которым следует относить: «а) маршрутизаторы *Tor* не вставляют искусственные задержки между запросами; б) *IP*-адреса всех узлов *Tor* публично известны и доступны» [11, с. 368]. Атакующий в данной ситуации контролирует выходной узел сети; фиксирует временные промежуточные интервалы периодических запросов, которые осуществляются в сети *"Tor"*. Третья атака применяет «тяжелые» запросы формирования связи (цепи) между пользователями и «теневыми службами», которые, в свою очередь, оперативно генерируются атакующим с наименьшими затратами.

Таким образом, можно сделать вывод, что атакующие в лице сотрудников оперативных подразделений полиции должны обладать высокотехнологическими средствами, ресурсами и достаточным уровнем профессионализма для эффективной деятельности по деанонимизации лиц, совершающих преступления в сети *"Tor"*. В правоприменительной практике сотрудники оперативных подразделений полиции, в том числе сотрудники подразделения «К» МВД России в перспективе смогут широко и эффективно применять совокупность активных и пассивных методов атак в целях деанонимизации пользователей сети *"Tor"*. Проанализированные нами методы можно использовать для отслеживания параметров пользователей информационного пространства.

Комплекс приобретаемых оперативными сотрудниками полиции сведений дает возможность организовать цифровой (виртуальный) след, представляющий собой 32-битное шестнадцатеричное число, полученное путем обработки всех данных от *cookie* браузера [12, с. 173]. Следует отметить, что сотрудники оперативных подразделений полиции могут собирать необходимую оперативно-значимую и аналитическую информацию о пользователях, совершающих преступления посредством сети «Интернет» с определенными цифровыми (виртуальными) следами, например, изучая историю их просмотра (через *cookie*) и авторизации на интернет-ресурсах. В дальнейшем сотрудниками оперативных подразделений полиции данная информация может быть использована в процессе определения круга общения деанонимизированных пользователей информационного пространства.

Комплексно проанализировав средства и методы деанонимизации пользователей сети *"Tor"*, предлагаем рассмотреть вопросы касательно деанонимизации лиц, совершающих мошенничество посредством *spoofing*-атак.

В контексте информационной безопасности *spoofing*-атака представляет собой ситуацию, в которой человек или программа удачно выдает себя за другого человека или программу, фальсифицируя сведения и приобретая незаконные преимущества [13, с. 109]. Наиболее распространенным способом совершения *spoofing*-атаки является использование электронной почты. Так, сведения об отправителе, отображаемые в электронном письме, могут быть легко подделаны путем подмены электронной почты (*E-mail spoofing*). Данная технология зачастую применяется «спамерами» в целях сокрытия источника электронной почты.

В *spoofing*-атаке мошенническое изменение адреса электронной почты реализуется посредством использования обычных электронных почт. Однако сообщение будет отправлено только в том случае, если набор символов будет соответствовать протоколу передачи почты (*SMTP*) путем применения почтового сервера *Telnet*.

Представим ситуацию, что интернет-мошенники направили письмо по электронной почте от имени организации, оказывающей услуги (управляющей компании), со следующим содержанием: «предлагаем Вам перейти на сайт организации, заполнить анкету и произвести оплату за услуги по *QR*-коду» (приложив к письму: *QR*-код, *online*-квитанцию, и самое главное ссылку на сайт организации). При этом итернет-мошенники направляют по электронной почте не официальный сайт организации, оказывающей услуги (управляющей компании), а сайт-двойник (мошеннический сайт), который был создан преступниками заранее. Здесь следует отметить, что, несмотря на попытки анонимизации преступников, сотрудники оперативных подразделений полиции имеют инструментарий для деанонимизации отправителей (адресантов), поскольку, помимо отправителя и получателя, в цепи электронных отправлений принимают участие несколько почтовых серверов.

В случае, когда известны *IP*-адреса подлинного отправителя электронных сообщений, правоохранители в лице сотрудников оперативных подразделений полиции могут воспользоваться сервисом *2ip.ru*, который предоставляет данные о хосте-пользователей. В последующем могут возникнуть разные варианты развития события:

1. *IP*-адрес принадлежит пользователю, который находится на территории Российской Федерации. В этой ситуации необходимо направить запрос провайдеру, который может предоставить сведения о пользователе, который использует данный *IP*-адрес.

2. *IP*-адрес принадлежит пользователю, который находится за пределами Российской Федерации. В этой ситуации следует оформить официальный запрос хостинг-провайдеру, присвоившему данный *IP*-адрес. Однако, в силу того, что пользователи информационного пространства в большинстве случаев используют *VPN*-программы, позволяющие шифровать *IP*-адрес, в правоприменительной практике возникают проблемы.

Необходимо подчеркнуть, что сотрудники оперативных подразделений полиции в целях деанонимизации лиц, использующих *VPN*-программы для совершения преступлений в интернет-пространстве могут использовать возможности технических средств для проведения оперативно-розыскных мероприятий (далее — ОРМ), которые «размещаются на узлах связи сети оператора» [14]. Из базы данных оператора связи обеспечивается возможность получения информации об абоненте: абонентский номер и (или) код идентификации которого указаны в запросе пункта управления ОРМ, а также об абонентском номере и (или) коде идентификации абонента, чьи персональные данные указаны в запросе пункта управления ОРМ.

Особое место в процессе деанонимизации лиц, совершающих преступления в информационном пространстве, уделяется использованию возможностей Больших данных *(Big Data)*. Невзирая на то, что данные о конкретном гражданине в массиве Больших данных *(Big Data)*, как правило, обезличены, специалисты из Университета Лувена и Имперского колледжа Лондона пришли к мнению, что практически любой поток данных можно деанонимизировать [15]. Пользователи информационного пространства при осуществлении поиска жертвы не оставляют сведений касательно их персональных данных, активность преступников сохраняется в *cookie* браузера и передается для дальнейшей ее обработки.

Когда агрегированные сведения соединяются с другими источниками, которые содержат сведения о конкретных лицах в информационном пространстве, становится возможным идентифицировать конкретное лицо. В данной ситуации то, что кажется обезличенным сбором информации, превращается в пул персональных данных многих пользователей. Итак, основываясь на Больших данных *(Big Data),* формируются подробные портреты лиц, совершающих преступления в информационном пространстве для дальнейшего их задержания и привлечения к ответственности.

Таким образом, сотрудники оперативных подразделений полиции, несмотря на использование преступниками инновационных методов противодействия расследованию, все же предпринимают эффективные попытки преодоления незаконных действий со стороны преступников, хотя и формируется определенная теория информационных технологий, являющаяся лишь опорой криминалистической деятельности. Следует принимать во внимание, что для эффективного использования средств

и методов деанонимизации лиц, совершающих преступления в информационном пространстве, требуется высокий уровень подготовленности сотрудников полиции, наличие у них профессиональных умений и навыков деятельности в сфере *IT*.

Подытоживая проведенное исследование, следует отметить, что деанонимизация лиц, совершающих преступления в информационном пространстве, — это специфические информационно-аналитические методы получения оперативно-значимой информации, которая не может быть отождествлена с классическими оперативно-розыскными мероприятиями. По этой причине целесообразно закрепить исследованные методы деанонимизации киберпреступников в виде отдельного оперативно-розыскного мероприятия, представляющего собой особый вид оперативно-поисковой деятельности, осуществляемый для решения задач в оперативно-розыскной деятельности. Способы, методику и алгоритмы действий, направленных на деанонимизацию лиц, совершающих преступления в информационном пространстве, необходимо отразить в Приказе МВД России с определенным грифом секретности.

Список источников

1. Состояние преступности в Российской Федерации за 2021 год. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 05.05.2022).

2. Расширенное заседание коллегии МВД России. URL: http://kremlin.ru/events/president/news/67795 (дата обращения: 05.05.2022).

3. Шалагин А. Е., Идиятуллов А. Д. Новые тенденции преступности в XXI веке: глобализация, цифровизация, социальный контроль // Modern Science. 2020. № 11-1. С. 131—134.

4. Алпеева О. И., Бушуева А. В. Применение цифровых технологий и искусственного разума при предупреждении преступности // Вестник Пензенского государственного университета. 2021. № 3. С. 54—62.

5. Тимофеев С. В. К вопросу добывания оперативно значимой информации в сети интернет: проблемы и пути их решения // Криминалистика: вчера, сегодня, завтра. 2021. № 2 (18). С. 111—117.

6. Афонькин Г. П., Смирнов Е. В., Чемерчев Д. В. Основы противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий // Полицейский вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2021. № 1 (4). С. 10—17.

7. Гаврилин Ю. В., Парадников А. Г. Совершенствование выявления, раскрытия и расследования хищений, совершенных и использованием информационных банковских технологий (по итогам Всероссийского онлайн-семинара) // Труды Академии управления МВД России. 2020. № 2 (54). С. 123—130.

8. Земцова С. И. Программные продукты, используемые для деанонимизации фактов совершения наркопреступлений с использованием цифровой валюты // Криминалистика — наука без границ: традиции и новации: материалы всероссийской научно-практической конференции, Санкт-Петербург, 26 ноября 2020 года / составители: А. В. Бачиева, Э. В. Лантух. СПб.: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2021. С. 112—115.

9. Закупка № 0373100088714000008. URL: https://zakupki.kontur.ru/0373100088714000008 (дата обращения: 05.05.2022).

10. Лазаренко А. В. Технологии деанонимизации пользователей Tor // Новые информационные технологии в автоматизированных системах. 2016. № 19. С. 257—262.

11. Авдошин С. М., Лазаренко А. В. Методы деанонимизации пользователей Tor // Информационные технологии. 2016. Т. 22. № 5. С. 362—372.

12. Тимофеев С. В. Деанонимизация пользователя сети интернет как метод оперативно-розыскного противодействия наркопреступности // Юристъ-Правоведъ. 2020. № 2 (93). С. 170—174.

13. Третьякова Е. И., Босхолов С. С., Щербина Р. П. Возможности деанонимизации лиц, совершающих мошенничество с применением спуффинг-атак // Криминалистика: вчера, сегодня, завтра. 2021. № 4. С. 106—118.

14. Требования к сетям электросвязи для проведения оперативно-разыскных мероприятий. Ч. I. Общие требования: утв. Приказом Мининформсвязи РФ от 16 января 2008 года № 6 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2008. № 9.

15. Опасность «Больших данных». Или как Big Data ведет к полной деанонимизации пользователя и составлению его профайла. URL: https://habr.com/ru/sandbox/161732/ (дата обращения: 05.05.2022).

References

1. The state of crime in the Russian Federation for 2021. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (accessed 05.05.2022). (In Russ.)

2. Extended meeting of the collegium of the Ministry of Internal Affairs of Russia. URL: http://kremlin.ru/events/president/news/67795 (accessed 05.05.2022). (In Russ.)

3. Shalagin A. E., Idiyatullov A. D. New crime trends in the 21st century: globalization, digitalization, social control. *Modern Science,* 2020, no. 11-1, pp. 131—134. (In Russ.)

4. Alpeeva O. I., Bushueva A. V. The use of digital technologies and artificial intelligence in crime preven-

tion. *Bulletin of the Penza State University,* 2021, no. 3, pp. 54—62. (In Russ.)

5. Timofeev S. V. On the issue of obtaining operationally significant information on the Internet: problems and ways to solve them. *Criminalistics: yesterday, today, tomorrow,* 2021, no. 2 (18), pp. 111—117. (In Russ.)

6. Afonkin G. P., Smirnov E. V., Chemerchev D. V. Fundamentals of combating crimes committed using information and telecommunication. *Police Bulletin of the All-Russian Institute for Advanced Training of Employees of the Ministry of Internal Affairs of the Russian Federation,* 2021, no. 1 (4), pp. 10—17. (In Russ.)

7. Gavrilin Yu. V., Paradnikov A. G. Improving the detection, disclosure and investigation of theft committed by using information banking technologies (based on the results of the All-Russian online seminar). *Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia,* 2020, no. 2 (54), pp. 123—130. (In Russ.)

8. Zemtsova S. I. Software products used to deanonymize the facts of drug crimes using digital currency. Criminalistics is a science without borders: traditions and innovations: Proceedings of the All-Russian Scientific and Practical Conference, St. Petersburg, November 26, 2020 / compiled by: A. V. Bachieva, E. V. Lantukh. St. Petersburg: St. Petersburg University of the Ministry of Internal Affairs of the Russian Federation, 2021. Pp. 112—115. (In Russ.)

9. Purchase № 0373100088714000008. URL: https://zakupki.kontur.ru/0373100088714000008 (accessed 05.05.2022). (In Russ.)

10. Lazarenko A. V. Tor user deanonymization technologies. *New information technologies in automated systems,* 2016, no. 19, pp. 257—262. (In Russ.)

11. Avdoshin S. M., Lazarenko A. V. Methods of deanonymization of Tor users. *Information technologies,* 2016, vol. 22, no. 5, pp. 362—372. (In Russ.)

12. Timofeev S. V. Deanonymization of the Internet user as a method of operational-search counteraction to drug crime. *Yurist-Pravoved,* 2020, no. 2 (93), pp. 170—174. (In Russ.)

13. Tretyakova E. I., Boskholov S. S., Shcherbina R. P. Possibilities of deanonymization of persons committing fraud using spoofing attacks. *Criminalistics: yesterday, today, tomorrow,* 2021, no. 4, pp. 106—118. (In Russ.)

14. Requirements for telecommunication networks for carrying out operational search activities. Part I. General requirements: approved. Order of the Ministry of Information and Communications of the Russian Federation no. 6 of January 16, 2008. *Bulletin of normative acts of federal executive authorities,* 2008, no. 9. (In Russ.)

15. The danger of Big Data. Or how Bid Data leads to the complete deanonymization of the user and the compilation of his profile. URL: https://habr.com/ru/sandbox/161732/ (accessed 05.05.2022). (In Russ.)

Статья поступила в редакцию 29.06.2022; одобрена после рецензирования 30.09.2022; принята к публикации 01.12.2022.

The article was submitted 29.06.2022; approved after reviewing 30.09.2022; accepted for publication 01.12.2022.