Научная статья
УДК 343
https://doi.org/10.36511/2078-5356-2024-4-113-119

«Битва за умы» — некоторые вопросы оперативно-розыскной профилактики преступлений, совершаемых с использованием информационно-коммуникационных технологий

Дягилев Андрей Аркадьевич
Нижегородская академия МВД России, Нижний Новгород, Россия, musasi2008@yandex.ru

Аннотация. Развитие информационно-коммуникационных технологий оказало существенное влияние на различные сферы жизни современного общества. Не стала исключением и противоправная деятельность, получившая мощный импульс к развитию и совершенствованию механизмов реализации преступлений, совершенных с использованием информационно-коммуникационных технологий. В настоящее время значительное число преступных посягательств направлено на завладение умами граждан для того, чтобы, манипулируя их поведением, преступники могли достичь своих целей. При этом прослеживается тенденция вовлечения потерпевших не только в общеуголовные преступления, но и в совершение уголовно наказуемых деяний экстремистской и террористической направленности. Таким образом, в статье предпринята попытка рассмотреть эффективность традиционных мер оперативно-розыскной профилактики совершения преступлений с учетом их меняющегося характера. Обозначены возможные направления совершенствования указанного вида деятельности.

Ключевые слова: оперативно-розыскная деятельность, информационные технологии, социальная инженерия, преступления экстремистского и террористического характера, оперативно-розыскная профилактика, ограничение прав и свобод человека в процессе оперативно-розыскной деятельности

Для цитирования: Дягилев А. А. «Битва за умы» — некоторые вопросы оперативно-розыскной профилактики преступлений, совершаемых с использованием информационно-коммуникационных технологий // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 4 (68). С. 113–119. https://doi.org/10.36511/2078-5356-2024-4-113-119.

Original article

“Battle for minds” — some issues of operational investigative prevention of crimes committed using information and communication technologies

Andrey A. Dyagilev
Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russian Federation, musasi2008@yandex.ru

Abstract. The rapid development of information and communication technologies has had a significant impact on various spheres of life in modern society. Illegal activities were no exception, receiving a powerful impetus for the development and improvement of implementation mechanisms. Currently, a significant number of criminal attacks are aimed at capturing the minds of victims, so that by manipulating their behavior, criminals can achieve their goals. At the same time, there is a tendency to involve victims of ordinary crimes in the commission of criminal acts of an extremist and terrorist nature. Accepting the relationship between the mechanisms of criminal activity and activities to combat it, within the framework of the presented article, an attempt is made to consider the effectiveness of traditional measures of operational-search prevention of crimes, taking into account their changing nature. Possible areas for improving this type of activity are also indicated.

Keywords: operational investigative activities, information technology, social engineering, crimes of an extremist and terrorist nature, operational investigative prevention, restriction of human rights and freedoms in the process of operational investigative activities

For citation: Dyagilev A. A. “Battle for minds” — some issues of operational investigative prevention of crimes committed using information and communication technologies. *Legal Science and Practice: Journal of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2024, no. 4 (68), pp. 113–119. (In Russ.) https://doi.org/10.36511/2078-5356-2024-4-113-119.

В последнее время отмечается рост различного рода преступных посягательств, объектом которых является сознание граждан. Фактически преступники пытаются «завладеть» умами людей, чтобы иметь возможность, манипулируя их поведением, решать свои противоправные задачи. Стоит отметить, что уровень преступного профессионализма в данной области растет с каждым годом. О чем свидетельствует, в частности, растущая длительность контроля над поведением жертвы, увеличивающийся набор действий, выполняемых ею в период нахождения под таким контролем.

В качестве примера приведем схему усложнения преступного механизма, реализуемого так называемыми мошенническими «колл-центрами». Если изначально преступники, используя методы психологических манипуляций, убеждали потерпевших сообщить им данные кредитных карт или код из СМС-сообщений, то со временем, апробируя и внедряя наиболее эффективные способы воздействия, им удалось существенно усилить степень контроля над поведением жертвы. Так, наряду с получением персональных данных потерпевших последних стали убеждать в необходимости совершения целого набора определенных действий. Например, снять деньги со своего счета либо оформить на свое имя кредит, после чего внести имеющиеся денежные средства через банкомат на счет, указанный преступниками. Кроме того, имеют место случаи, когда после перевода денег, жертву якобы для обеспечения ее безопасности убеждали в необходимости поменять номер мобильного телефона и уехать на квартиру, указанную преступниками, действующими под видом сотрудников правоохранительных органов или специальных служб. После чего родственникам жертвы выдвигали требования об уплате определенной суммы денег за возвращение якобы похищенного лица [1].

Более того, если изначально преступники были нацелены только на личные сбережения граждан, то с началом специальной военной операции (далее — СВО) телефонные атаки стали еще более изощренными и опасными. Апробированные в течение нескольких лет и доказавшие свою эффективность методы социальной инженерии, используемые при совершении преступлений в настоящее время, позволяют преступникам на определенный промежуток времени установить практически тотальный контроль над жертвой. В процессе нахождения под таким контролем, зачастую не отдавая в полной мере отчет своим действиям, жертва выполняет все поступившие ей указания, в результате чего не только отдает свои сбережения, но и совершает иные преступления. Так, по приказу «кукловодов» совершаются такие уголовно наказуемые деяния, как призывы к дискредитации действий Вооруженных Сил Российской Федерации в условиях СВО, осуществление взрыва или поджога, а также другие общественно опасные поступки.

В период проведения в марте 2024 года выборов Президента Российской Федерации лица, находившиеся под внешним воздействием, совершили целый ряд действий, направленных на воспрепятствование осуществлению избирательных прав или работе избирательных комиссий [2]. При этом, как отмечает председатель Центризбиркома России Э. Памфилова, «приказы о вливании красящих жидкостей в избирательные урны и поджогах на территории российских избирательных участков исполнители получили от кураторов с Украины и ряда стран Евросоюза» [3].

Вышесказанное достаточно наглядно иллюстрирует тот факт, что направленность преступного воздействия на умы граждан оказала существенное влияние на механизмы совершения как общеуголовных преступлений, так и уголовно наказуемых деяний экстремистского и террористического толка. При этом сложилась ранее не типичная ситуация, когда жертва общеуголовного преступления в очень короткий срок (от нескольких часов до нескольких дней) вовлекается в совершение преступления террористического или экстремистского характера.

Стоит отметить, что сложность противодействия ранее описанным криминальным посягательствам обусловлена тем, что в большинстве случаев лица, которые в результате внешнего воздействия были вовлечены в подобного рода преступления, до момента контакта с преступниками вели законопослушный образ жизни и не попадали в поле зрения правоохранительных органов.

Группа риска, куда специалисты относят лиц, которые смогут стать потенциальными жертвами телефонных мошенников и далее будут вовлечены в совершение иных преступлений, достаточна широка. В частности, исследования Центрального банка России показывают, что наиболее часто мошеннические действия совершаются в отношении лиц в возрасте от 25 до 64 лет (66,2 %), проживающих в городах (75,4 %), имеющих средний достаток (44,8 %). При этом доля мужчин (44,5 %) и женщин (55,5 %) среди потерпевших примерна одинакова, как и уровень их образования (общее — 32,8 %, среднее — 41,3 % и высшее — 25,9 %) [4]. Таким образом, выделить какую-либо конкретную социальную группу, требующую особого профилактического внимания, достаточно сложно.

В этой связи закономерно возникает вопрос о соответствии традиционных методов оперативно-розыскной профилактики в складывающейся ситуации. В настоящее время многие специалисты подчеркивают, что наиболее эффективным способом, как гражданину не стать жертвой телефонного мошенничества, является немедленное прекращение разговора. Информация об этом, а также о типичных способах и предлогах, используемых преступниками для установления контакта с жертвой и последующего склонения ее к выполнению своих требований, систематически доводится до граждан по различным каналам коммуникации (объявления в СМИ, сети «Интернет», в торговых центрах, в рамках осуществления просветительской работы с различными группами населения и т. д.). Эта работа дает определенные плоды. Так, по данным Всероссийского центра изучения общественного мнения: «В целом россияне скептически оценивают свои шансы быть обманутыми телефонными мошенниками: 46 % считают такое развитие событий маловероятным, 27 % — невозможным. Еще 23 % допускают («это вполне может случиться»), что могут лишиться денежных средств в результате действий телефонных мошенников, среди россиян постарше (45–59 лет) такой ответ звучит несколько чаще — 31 %» [5]. Таким образом, проводимая на различных уровнях работа по повышению цифровой и финансовой грамотности населения нашей страны приносит свои результаты. При этом указанное направление общепрофилактической деятельности должно быть скорректировано с учетом имеющихся фактов вовлечения жертв телефонных мошенничеств в противоправную деятельность. Кроме того, повышенное внимание следует уделять подрастающему поколению, у которого менее сформированы личностные и ценностные установки, что облегчает манипуляцию их поведением.

Однако, несмотря на принимаемые меры воспитательного и просветительского характера, не удается снизить количество рассматриваемого вида преступлений в существенных масштабах. Согласно данным МВД России, в 2023 году «каждое третье преступление совершено с использованием информационно-телекоммуникационных технологий. В этой сфере зарегистрировано на 29,7 % больше уголовно наказуемых деяний, чем в январе-декабре прошлого года. Подобных преступлений раскрыто на 21 % больше, чем в 2022 году. Их профилактика по-прежнему остается одной из важнейших задач органов внутренних дел» [6]. Более того, как уже отмечалось, происходит их трансформация в деяния, несущие угрозу не только собственности юридических и физических лиц, но и их жизни, здоровью и безопасности государства.

В этой связи представляется целесообразным рассмотреть вопрос о выработке новых мер профилактики данного вида преступлений. Как отмечает С. С. Галахов, «осуществление мер специального предупреждения допустимо с помощью как гласных, так и негласных сил,

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2024, no. 4 (68)

средств и методов» [7, с. 283]. Одним из таких методов представляется повышение уровня контроля в информационной среде, в том числе за содержанием телефонных переговоров граждан. В настоящее время операторы сотовой связи имеют возможность фиксировать содержание всех телефонных переговоров своих абонентов. Более того, в силу произошедших изменений законодательства, получивших укоренившееся название «пакета законов Яровой» они обязаны хранить записи данных телефонных переговоров, а также переписку и исходящий трафик всех своих пользователей [8–9]. Соответственно, субъекты оперативно-розыскной деятельности в рамках установленных законом процедур имеют возможность получить доступ к указанной информации.

Как известно, ограничение права человека на тайну телефонных переговоров в общем порядке осуществляется на основании соответствующего судебного решения. Тайна телефонных переговоров признается нарушенной, когда доступ к переговорам совершен без согласия лица, чью тайну они составляют, при отсутствии законных оснований для ограничения данного конституционного права [10]. Фактически речь идет о том, что третье лицо в нарушение установленных процедур ознакомится с содержанием данных телефонных переговоров либо получит сведения о «входящих и об исходящих сигналах соединения между абонентами или абонентскими устройствами пользователей связи (дате, времени, продолжительности соединений, номерах абонентов, других данных, позволяющих идентифицировать абонентов)» [11]. Вместе с тем операторами сотовой связи указанная информация обрабатывается и сохраняется в автоматическом режиме. Схожая ситуация имеет место в банковском секторе. Так, сведения об операциях, совершаемых по счетам физических лиц, выдаются субъектам оперативно-розыскной деятельности в рамках установленных процедур на основании соответствующего судебного решения [12]. При этом в рамках пресечения мошеннических действий многие банки активно используют различные алгоритмы, построенные на принципе анализа больших массивов данных, в том числе о финансовых операциях и поведенческих особенностях конкретного клиента, позволяющих выявлять и приостанавливать подозрительные операции, не характерные для него. Так называемые технологии антифрод мониторинга. Данная аналитическая деятельность осуществляется искусственным интеллектом без разглашения третьим лицам сведений, составляющих охраняемую законом банковскую тайну. Более того, в сентябре 2023 года Сбол получил патент на систему определения мошеннических звонков путем расшифровки диалогов искусственным интеллектом с лицами, звонящими в банк, посредством сопоставления цифровых «слепков» голоса. Схожая система предусмотрена также антифрод-ассистентом Т–банка [13].

Таким образом, в настоящее время с высокой степенью эффективности функционируют механизмы профилактики, при реализации которых искусственный интеллект анализирует значительный объем охраняемой законом информации, исключая доступ к ней третьих лиц.

Представляется, что подобного рода положительный опыт может быть масштабирован на все телефонные переговоры, осуществляемые на территории Российской Федерации. Например, путем разработки технических решений, которые позволяют, применяя искусственный интеллект, анализировать содержание телефонных разговоров, выявляя те из них, которые содержат признаки телефонного мошенничества либо последующего склонения лица, ставшего жертвой такого мошенничества, но еще не осознающего этого, к совершению террористического акта или иного преступления. При выявлении подобного рода разговоров возможно приостановление связи с направлением лицу соответствующего уведомления посредствам СМС–сообщения либо звонка. Кроме того, сведения о лице, в отношении которого, возможно, совершается противоправное действие или которое может быть вовлечено в подготовку либо совершение преступления, должны направляться сведения в правоохранительные органы для принятия превентивных мер, направленных на предотвращение либо пресечение преступления. К подобного рода мерам можно отнести установление места нахождения данного абонента, его идентификацию и обнаружение посредствам анализа данных с камер наружного видеонаблюдения. В случае нахождения данного лица в поле зрения камер сотрудники правоохранительных органов могут проанализировать его поведение в данный момент времени (например, выявить приготовление к совершению нападения на объекты инфраструктуры) и скорректировать комплекс необходимых профилактических мер.

Основываясь на диалектическом подходе, рассмотрим предложенный тезис о целесообразности контроля и обработки содержания телефонных переговоров при помощи искусственного интеллекта через возможные возражения. То есть проверим его через антитезисы, в качестве которых могут выступать следующие утверждения.

— Движение по предполагаемому пути повлечет за собой еще большее ограничение прав и свобод человека и приведет нас в «цифровой концлагерь». Вместе с тем законодательство должно отвечать реалиям времени и предоставлять правоприменителям действенные механизмы воздействия, адекватные возникающим угрозам. Похожие опасения высказывались и при установке видеокамер в общественных местах. При этом опыт использования систем видеонаблюдения, в том числе с применением биометрической идентификации личности, показал их высокую эффективность при решении задач борьбы с преступностью и не повлек за собой сколь либо значимое нарушение прав человека, похожие опасения высказывались и при установке видеокамер в общественных местах. При этом опыт использования систем видеонаблюдения, в том числе с применением биометрической идентификации личности, показал их высокую эффективность при решении задач борьбы с преступностью и не повлек за собой сколь либо значимое нарушение прав человека.

Кроме того, действующая редакция Федерального закона «Об оперативно-розыскной деятельности» от 12 августа 1995 года № 144-ФЗ, уже содержит в себе ряд нормативных положений, закрепляющих возможность проведения оперативно-розыскных мероприятий, ограничивающих конституционные права человека в уведомительном порядке с получением соответствующего судебного решения в течении 48 часов с момент начала их проведения. Схожие нормы закона касаются возможности ограничения конституционных прав при поиске лиц без вести пропавших. Соответственно, мы можем говорить о наличии общепризнанной нормативно закрепленной возможности ограничения в особых случаях конституционных прав широкого круга лиц без немедленного получения судебного решения. При этом стоит согласиться, что предлагаемые механизмы потребуют дополнительной правовой регламентации, в том числе в части взаимодействия между операторами связи и субъектами оперативно-розыскной деятельности при направлении информации, ее использовании и недопущения к ней неуполномоченных на то лиц.

— Внедрение подобных технологий потребует существенных материальных затрат как со стороны бизнеса (разработка, внедрение, поддержание работоспособности соответствующих информационных технологий на базе искусственного интеллекта), так и государства (выработка и обеспечение организационных, кадровых и технологических решений, необходимых для приема, обработки и проверки поступающей информации). Вместе с тем, как мы уже отмечали ранее на примере Сбола или Т-банка, бизнес самостоятельно движется в указанном направлении, стремясь обеспечить безопасность вкладов своих клиентов, повысив тем самым свою привлекательность и конкурентоспособность. Кроме того, общественная опасность и вероятный ущерб от рассматриваемой категории преступлений является достаточным основанием для осуществления подобных затрат, которые в будущем призваны обеспечить недопущение наступления тяжких последствий для граждан, организаций и безопасности государства.

— В случае внедрения подобного рода контроля за телефонными переговорами преступники перейдут на общение в мессенджерах или интернет телефонии. Безусловно, использование преступниками подобного рода технических решений влечет за собой новые риски, связанные с технологией подмены голоса либо изображения. Однако преступники используют данные технические решения и сейчас. Конечно, предлагаемый метод не искоренит все угрозы, но позволит купировать часть из них, поскольку все же именно телефонная связь в настоящее является более устойчивой и распространенной и вызывающей большее доверие среди группы риска.

Таким образом, обобщая доводы за и против, необходимо отметить, что предлагаемое решение требует дополнительного обсуждения как в научном сообществе, так и среди правоприменителей, специалистов в области связи и обеспечения информационной безопасности. Вместе с тем автору представляется, что наличие подобной дискуссии может принести свои плоды, подсказать новые решения существующей проблемы в области противодействия данному виду преступлений, в том числе предусматривающие использование возможностей искусственного интеллекта при обработке больших массивов данных.

Список источников

1. Игра в похищение: телефонные мошенники придумали опасную схему обмана россиян. URL: https://iz.ru/1503138/dmitrii-bulgakov/igra-v-pokhishchenie-telefonnye-moshenniki-pridumali-opasnuiu-skhemu-obmana-rossiian (дата обращения: 23.08.2024).

2. Зеленка, поджоги, спецслужбы: кто и как пытается сорвать выборы в России. URL: https://news.rambler.ru/politics/52441941/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 23.07.2024).

3. Раскрыты организаторы схемы по порче бюллетеней на выборах президента России. URL: https://360tv.ru/news/proisshestviya/raskryty-organizatory-shemy-po-porche-bjulletenej-na-vyborah-prezidenta-rossii/ (дата обращения: 29.07.2024).

4. Кибермошенничество: портрет пострадавшего Сайт Банка России. URL: https://cbr.ru/statistics/information_security/cyber_portrait/ (дата обращения: 21.03.2024).

5. Телефонное мошенничество: мониторинг. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (дата обращения: 23.03.2024).

6. Краткая характеристика состояния преступности в Российской Федерации за январь—декабрь 2023 года официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 25.07.2024).

7. Галахов С. С. Актуальные проблемы оперативно-розыскной деятельности в XXI веке в Российской Федерации: сборник научных трудов. Москва: Нома, 2024. 304 с.

8. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федеральный закон от 6 июля 2016 года № 374-ФЗ // Доступ из СПС «КонсультатнтПлюс» (дата обращения: 25.07.2024).

9. О связи: федеральный закон от 7 июля 2003 года № 126-ФЗ (ред. от 4 августа 2023 года) // Доступ из СПС «КонсультатнтПлюс» (дата обращения: 25.07.2024).

10. О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138, 139, 144, 145, 145 Уголовного кодекса Российской Федерации): пленум Верховного Суда Российской Федерации // Доступ из СПС «КонсультантПлюс» (дата обращения: 25.07.2024).

11. О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138, 139, 144, 145, 145 Уголовного кодекса Российской Федерации): пленум Верховного Суда Российской Федерации // Доступ из СПС «КонсультантПлюс» (дата обращения: 25.07.2024).

12. О банках и банковской деятельности: федеральный закон от 2 декабря 1990 года № 395-1 (ред. от 12 декабря 2023 года) // Доступ из СПС «КонсультантПлюс» (дата обращения: 25.07.2024).

13. Сбер получил патент на систему определения мошеннических звонков. URL: https://sber.pro/digital/publication/sber-poluchil-patent-na-sistemu-opredeleniya-moshennicheskikh-zvonkov/ (дата обращения: 23.08.2024).

References

1. Kidnapping game: telephone scammers have come up with a dangerous scheme to deceive Russians. URL: https://iz.ru/1503138/dmitrii-bulgakov/igra-v-pokhishchenie-telefonnye-moshenniki-pridumali-opasnuiu-skhemu-obmana-rossiian (accessed 23.08.2024). (In Russ.)

2. Green paint, arson, special services: who and how is trying to disrupt the elections in Russia. URL: https://news.rambler.ru/politics/52441941/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (accessed 23.07.2024). (In Russ.)

3. The organizers of the scheme to spoil ballots in the Russian presidential elections have been revealed. URL: https://360tv.ru/news/proisshestviya/raskryty-organizatory-shemy-po-porche-bjulletenej-na-vyborah-prezidenta-rossii/ (accessed 29.07.2024). (In Russ.)

4. Cyber fraud: portrait of the victim Website of the Bank of Russia. URL: https://cbr.ru/statistics/information_security/cyber_portrait/ (accessed 21.03.2024). (In Russ.)

5. Telephone fraud: monitoring. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (accessed 23.03.2024). (In Russ.)

6. Brief characteristics of the state of crime in the Russian Federation for January — December 2023 official website of the Ministry of Internal Affairs of Russia. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (accessed 25.07.2024). (In Russ.)

7. Galakhov S. S. Actual problems of operational-search activities in the 21st century in the Russian Federation: collection of scientific papers. Moscow: Noma Publ., 2024. 304 p. (In Russ.)

8. On Amendments to the Federal Law “On Counteracting Terrorism” and Certain Legislative Acts of the Russian Federation in Terms of Establishing Additional Measures to Counter Terrorism and Ensure Public Safety: federal law no. 374-FZ of July 6, 2016. Access from the reference legal system “ConsultantPlus”. (accessed 25.07.2024) (In Russ.)

9. On Communication: federal law no. 126-FZ of July 7, 2003 (as amended on August 4, 2023). Access from the reference legal system “ConsultantPlus”. (accessed 25.07.2024). (In Russ.)

10. On Certain Issues of Judicial Practice in Cases of Crimes against Constitutional Rights and Freedoms of Man and Citizen (art. 137, 138, 138, 139, 144, 145, 145 of the Criminal Code of the Russian Federation): plenum of the Supreme Court of the Russian Federation. Access from the reference legal system “ConsultantPlus”. (accessed 25.07.2024). (In Russ.)

11. On some issues of judicial practice in cases of crimes against the constitutional rights and freedoms of man and citizen (art. 137, 138, 138, 139, 144, 145, 145 of the Criminal Code of the Russian Federation): plenum of the Supreme Court of the Russian Federation. Access from the reference legal system“ConsultantPlus”. (accessed 25.07.2024). (In Russ.)

12. On banks and banking activities: federal law no. 395-1 of December 2, 1990 (as amended on December 12, 2023). Access from the reference legal system “ConsultantPlus”. (accessed 25.07.2024). (In Russ.)

13. Sber received a patent for a system for detecting fraudulent calls. URL: https://sber.pro/digital/publication/sber-poluchil-patent-na-sistemu-opredeleniya-moshennicheskikh-zvonkov/ (accessed 23.08.2024)

Информация об авторах

А. А. Дягилев — кандидат юридических наук, заместитель начальника кафедры оперативно–разыскной деятельности учебно-научного комплекса противодействия экономическим и налоговым преступлениям Нижегородской академии МВД России.

Information about the author

A. A. Diaghilev — Candidate of Sciences (Law), Deputy Head of the Department of Operational Investigative Activities of the educational and scientific complex of countering economic and tax crimes of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia.