Вестник Восточно-Сибирского института МВД России. 2024. № 4 (111). С. 262–277.
Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2024. No. 4 (111). P. 262–277.

5.1.4. Уголовно-правовые науки (юридические науки)

Научная статья
УДК 343.98
DOI: 10.55001/2312-3184.2024.45.56.024

ПЕРСПЕКТИВЫ СОВЕРШЕНСТВОВАНИЯ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ СЛЕДОВ ПРЕСТУПЛЕНИЯ

Тимофеев Сергей Владимирович[1], Кочесоков Рустам Хажмударович[2]
[1]Восточно-Сибирский институт МВД России, г. Иркутск, Российская Федерация
[2]Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России, г. Нальчик, Российская Федерация
[1]tsv.1981@mail.ru
[2] r-kochesokov@mail.ru

Введение. В статье рассматриваются проблемы и перспективы использования цифровых следов в деятельности оперативных подразделений. В условиях стремительного развития информационных технологий и широкого распространения мобильных устройств вопросы обработки и анализа данных становятся особенно актуальными для правоохранительных органов. Цифровые следы представляют важный инструмент борьбы с динамично развивающейся киберпреступностью. Авторы акцентируют внимание на различных аспектах цифровых следов, таких как их природа, форма и источники, а также на методах их сбора и анализа. Обсуждаются основные проблемы, с которыми сталкиваются оперативные подразделения, включая отсутствие стандартизированных подходов к обработке данных, вопросы конфиденциальности и правовые ограничения. В своем исследовании авторы выделяют перспективы интеграции современных технологий, таких как машинное обучение и искусственный интеллект, в процессы анализа цифровых следов, что может значительно повысить эффективность работы оперативных подразделений и улучшить их взаимодействие с другими органами власти. Таким образом, статья представляет собой комплексный анализ актуальных вопросов и предоставляет полезные рекомендации для дальнейшего развития практики применения цифровых следов в оперативной деятельности.

Материалы и методы. Нормативную базу исследования составили Конституция Российской Федерации и иные федеральные законы и подзаконные нормативные акты. Кроме того, методологической основой исследования послужил всеобщий диалектический метод научного познания, общенаучные и некоторые частнонаучные методы, среди которых анализ, сравнение, обобщение оперативно-следственной и экспертной практики, литературных и интернет-источников.

Результаты исследования. Обоснована необходимость дальнейшего совершенствования уголовного и уголовно-процессуального законодательства, касающегося процедуры хранения электронных носителей информации и содержащихся на них цифровых следов. Предложены дополнения в статью 272 УК РФ и статью 164.1 УПК РФ, а также изменения в статью 273 УК РФ, предусматривающие ответственность за размещение в сети Интернет программного обеспечения, посредством которого обеспечивается возможность использования информационных ресурсов, доступ к которым ограничен на территории Российской Федерации.

Выводы и заключения. Сделан вывод о том, что неурегулированным и дискуссионным остается ряд вопросов, касающихся процессуальных процедур работы с электронными носителями информации, но бесспорным представляется факт того, что институты работы с ними продолжат развиваться в ближайшие годы.

Ключевые слова: цифровые следы, расследование и раскрытие преступлений, следы преступления, киберпреступность, цифровая преступность, компьютерные преступления

Для цитирования: Тимофеев С. В., Кочесоков Р. Х. Перспективы совершенствования российского законодательства в области использования цифровых следов преступления // Вестник Восточно-Сибирского института МВД России : науч.-практ. журн. Иркутск : Восточно-Сибирский институт МВД России. 2024. № 4 (111). С. 262–277.
DOI: 10.55001/2312-3184.2024.45.56.024

5.1.4. Criminal law sciences
(legal sciences)

Original article

PROSPECTS FOR IMPROVING RUSSIAN LEGISLATION IN THE FIELD OF USING DIGITAL TRACES OF CRIME

Sergey V. Timofeev[1], Rustam K. Kochesokov[2]
[1]East Siberian Institute of the Ministry of Internal Affairs of Russia, Irkutsk, Russian Federation
[2] North Caucasian Institute for Advanced Studies (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia, Nalchik, Russian Federation,
[1]tsv.1981@mail.ru
[2] r-kochesokov@mail.ru

Introduction. The article considers the problems and prospects of using digital traces in the activities of operational units. In the context of the rapid development of information technology and the widespread use of mobile devices, the issues of data processing and analysis are becoming especially relevant for law enforcement agencies. Digital traces are an important tool in the fight against dynamically developing cybercrime. The authors focus on various aspects of digital traces, such as their nature, form and sources, as well as methods of their collection and analysis. The main problems faced by operational units are discussed, including the lack of standardized approaches to data processing, privacy issues and legal restrictions. Summarizing the research, the authors highlight the prospects for integrating

modern technologies, such as machine learning and artificial intelligence, into the processes of digital trace analysis, which can significantly increase the efficiency of operational units and improve their interaction with other authorities. Thus, the article is a comprehensive analysis of current issues and provides useful recommendations for the further development of the practice of using digital traces in operational activities.

Materials and Methods. In the process of preparing this study, Federal In addition, the methodological basis of the study was the general dialectical method of scientific knowledge, general scientific and some specific scientific methods, including analysis, comparison, generalization of operational-investigative and expert practice, literary and Internet sources.

The Results of the Study. The necessity of further improvement of criminal and criminal-procedural legislation concerning the procedure of storage of electronic information carriers and digital traces contained on them is substantiated. Supplements to Articles 272 of the Criminal Code of the Russian Federation and 164.1 of the Criminal Procedure Code of the Russian Federation are proposed. Also, amendments are proposed to Article 273.1 of the Criminal Code of the Russian Federation providing for liability for posting on the Internet software by means of which access to information resources and information and telecommunication networks is provided, access to which is restricted on the territory of the Russian Federation.

Findings and Conclusions. It was concluded that a number of issues concerning procedural procedures for working with electronic information carriers remain unresolved and debatable, but it is an indisputable fact that institutions for working with them will continue to develop in the coming years.

Keywords: digital traces, investigation and disclosure of crimes, traces of crime, cybercrime, digital crime, computer crimes

For citation: Timofeev S. V., Kochesokov R. Kh. Perspektivy sovershenstvovanija rossijskogo zakonodatel'stva v oblasti ispol'zovanija cifrovyh sledov prestuplenija [Prospects for improving Russian legislation in the field of using digital traces of crime]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii - Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. Irkutsk, 2024, no. 4 (111), pp. 262–277.
DOI: 10.55001/2312-3184.2024.45.56.024

Информационные технологии, получившие широкое распространение в XXI веке, в корне изменили быт современного человека. Данные изменения коснулись различных сфер общественной жизни. Новейшие достижения научной и технической мысли активно используются в медицине, образовании, строительстве, сельском хозяйстве и во многих других областях жизнедеятельности человека.

Развитие цифровых технологий детерминировало ежегодный рост количества угроз и вызовов для безопасности людей и их собственности. Наглядно это иллюстрируют данные статистики, ежегодно обобщаемой Главным информационно-аналитическим центром Министерства внутренних дел Российской Федерации (далее – ГИАЦ МВД России). В 2003 году ГИАЦ МВД России впервые начал фиксировать статистические данные о преступлениях, совершенных в Российской Федерации с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (далее – ИТТ). Так, в 2003 году из 2 756 398 преступлений

лишь 7 540 совершались с использованием цифровых технологий, что составляло 0,27 % от общего числа зарегистрированных преступлений[1].

В таблице 1 обобщена статистика по зарегистрированным преступлениям в сфере ИТТ за 21 год, взятая на сайте ГИАЦ МВД России. Отметим, что процент преступлений данной категории в общем количестве зарегистрированных преступлений начал значительно повышаться еще в 2017 году, и в настоящее время существуют объективные условия для его роста.

Таблица 1

Данные официальной статистики ГИАЦ МВД России за 2003–2023 гг.

Год	Количество зарегистрированных преступлений	Количество преступлений в сфере ИТТ	Удельный вес преступлений в сфере ИТТ (%)	Раскрыто преступлений в сфере ИТТ	Раскрываемость преступлений в сфере ИТТ(%)
2003	2 756 398	7 540	0,27 %	7 186	95,31 %
2004	2 893 810	8 739	0,30 %	8 406	96,19 %
2005	3 554 738	10 214	0,29 %	9 759	95,55 %
2006	3 855 373	8 889	0,23 %	8 654	97,36 %
2007	3 582 541	7 236	0,20 %	6 614	91,40 %
2008	3 209 862	9 010	0,28 %	8 419	93,44 %
2009	2 994 820	11 636	0,39 %	11 296	97,08 %
2010	2 628 799	7 398	0,28 %	6 804	91,97 %
2011	2 404 807	2 698	0,11 %	2 687	99,59 %
2012	2 302 168	2 820	0,12 %	2 425	85,99 %
2013	2 206 249	2 563	0,12 %	2 301	89,78 %
2014	2 190 578	1 739	0,08 %	1 321	75,96 %
2015	2 388 476	2 382	0,1 %	1 213	50,92 %
2016	2 160 063	1 748	0,08 %	903	51,66 %
2017	2 058 476	90 587	4,4 %	20 424	22,55 %
2018	1 991 532	174 674	8,77 %	43 362	24,82 %
2019	2 024 337	294 409	14,54 %	65 238	22,16 %
2020	2 044 221	510 396	24,97 %	94 942	18,6 %
2021	2 004 404	517 722	25,8 %	118 920	22,96 %
2022	1 966 795	522 065	26,5 %	142 384	27,27 %
2023	1 947 161	676 951	34,7 %	172 290	25,4 %
Всего за 21 год	53 165 608	2 871 416	5,4 %	735 548	25,61 %

[1] Состояние преступности – январь – декабрь 2003 года // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/reports/item/209710/ (дата обращения: 30.09.2024).

Как отметил 25 сентября 2024 года Министр внутренних дел Российской Федерации В. А. Колокольцев на заседании общественного совета при МВД России, «за последние пять лет число противоправных деяний в киберпространстве увеличилось более чем вдвое. Сегодня их доля в общем массиве остается значительной и составляет около 40 %. То есть почти каждое второе преступление, совершаемое в нашей стране, – это преступление в сфере высоких технологий. А по тяжким, особо тяжким составам этот показатель приблизился к 60 %»[1].

Ущерб, наносимый подобными деяниями, по оценочным показателям превысил 116 млрд рублей менее чем за 10 месяцев 2024 года. Пострадавшими становятся не только граждане и крупные организации, но также государственные структуры. Сложность в раскрытии и расследовании этих преступлений обусловливается не только спецификой и неочевидностью киберпреступлений, но и присущим им межрегиональным и международным характером.

Ученые уже указывали на то, что на данном этапе развития информационного общества нет предельно четких и эффективных способов и механизмов действий, направленных на противодействие киберпреступности [1, с. 85]. За последние семь лет средний процент раскрываемости компьютерных преступлений составил менее 25 % (23,39 %).

Это показывает, что нашему государству требуется создание новых и развитие уже существующих инструментов борьбы с киберпреступностью. Фиксация цифровых следов и их последующее использование в доказывании по уголовным делам – важная процедура. Она напрямую влияет на качество собранной следовой информации, которая в последующем, согласно уголовно-процессуальному законодательству, может быть использована в качестве доказательств по уголовному делу.

Работа с цифровыми следами – это составная часть всей борьбы с киберпреступностью. По мнению О. П. Грибунова, «цифровые следы имеют большое значение для раскрытия преступления. Цифровой след, как и любой другой вид информации, состоит из двух элементов: материального носителя сведений, которым в данном случае выступает электромагнитное поле, и информации, то есть сведений о каком-либо явлении объективной реальности, которая может оставаться в компьютерных и иных цифровых устройствах» [2, с. 39].

Такие разделы криминалистики, как криминалистическая тактика и техника, выстраивают направления развития в зависимости от криминологических характеристик преступности в конкретном обществе. Важно учитывать «переменный характер преступности, а также обновления общественных отношений», чтобы всегда быть готовыми «дать практическим работникам правоохранительных органов новые тактические приемы и рекомендации по их использованию для расследования новых способов совершения преступлений» [3, с. 140].

[1] На заседании Общественного совета при МВД обсудили борьбу с киберпреступлениями // Новости на РЕН ТВ : сайт. URL: https://ren.tv/news/v-rossii/1264500-o-chem-govorili-na-zasedanii-obshchestvennogo-soveta-pri-mvd-rossii-v-moskve (дата обращения: 27.09.2024).

Важным, по нашему мнению, представляется комплексный подход к вопросу борьбы с киберпреступностью. Поэтому следует обозначить актуальную проблему фиксации и использования цифровых следов по уголовным делам.

Проведенное нами исследование позволило выявить определенные тенденции, а также вскрыть и (по возможности) развить некоторые аспекты этой проблемы, касающиеся идентификации источника цифровой информации. Это связано с тем, что в большинстве случаев правоохранителям сложно идентифицировать автора или владельца цифровой информации.

Большое количество предлагаемых на рынке цифровых услуг средств анонимизации обеспечивает возможность обращения широкого круга лиц к запрещенным сайтам и сервисам. Для скачивания какого-либо цифрового контента или приложений пользователи сети Интернет, как правило, пользуются программой uTorrent или ее аналогами.

Несмотря на то, что с 1 ноября 2017 года вступил в силу Федеральный закон от 29 июля 2017 г. № 276-ФЗ[1], прямо запрещающий специальные программы, которые могут скрывать пользователя в сети Интернет, существует немало сервисов и средств, обеспечивающих пользователю анонимность в информационном пространстве. Самыми популярными из них являются VPN-сервисы, прокси-серверы различного вида и SSH-туннели, I2P, dedicated-серверы. Это создает условия для того, чтобы каждый желающий мог ими воспользоваться, в том числе и в противоправных целях.

Согласно результатам исследования компании Platforma, в 2023 году число пользователей VPN в России выросло на 37 % по сравнению с предыдущим годом, и в 2,5 раза – по сравнению с 2021 годом[2].

Следует учесть, что 31 июля 2023 года Президент Российской Федерации В. В. Путин подписал Закон[3], запрещающий распространять сведения о методах и способах доступа к запрещенной информации. К этому относится и популяризация VPN-сервисов, позволяющих обходить блокировки.

После этого Правительством Российской Федерации было принято Постановление, наделяющее Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор)

[1] О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» : Федер. закон № 276-ФЗ : принят Гос. Думой 21 июля 2017 года : одобрен Советом Федерации 25 июля 2017 года // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_221230/ (дата обращения: 30.09.2024).

[2] Количество пользователей VPN в России в 2023 выросло почти на 40 % // Platforma : сайт. URL: https://platforma.id/kolichestvo-polzovatelej-vpn-v-rossii-v-2023-vyroslo-pochti-na-40-procentov (дата обращения: 09.09.2024).

[3] О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» : Федер. закон № 408-ФЗ : принят Гос. Думой 26 июля 2023 года : одобрен Советом Федерации 28 июля 2023 года // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_453264/ (дата обращения: 30.09.2024).

правом ограничивать рекламу VPN-сервисов, а Роскомнадзор подготовил приказ[1], содержащий критерии оценки для ограничения доступа в России к соответствующим материалам. Данный приказ вступил в силу 1 марта 2024 года и будет действителен до 1 сентября 2029 года.

В приказе Роскомнадзора, помимо прочего, перечислены новые причины, по которым регулятор сможет блокировать сайты. В реестр будут вносить страницы, которые:

– рассказывают о способах и методах обхода блокировок;

– побуждают применять эти способы, например перечисляют их преимущества;

– поясняют, как зайти на запрещенные ресурсы;

– предлагают купить или скачать VPN-сервисы;

– исключением может быть только «научная и статистическая информация».

Роскомнадзор уточнил, что требование о запрете распространения такого контента относится ко всем материалам, независимо от того, когда они были опубликованы и на каких ресурсах.

Важным представляется и тот факт, что Роскомнадзор выступил разработчиком проекта (ID 02/08/09-23/00141911), направленного в том числе на борьбу с VPN-сервисами. Всего Роскомнадзором за период с 2021 г. по 2023 г. был ограничен доступ к 167 VPN-сервисам и 84 приложениям.

Отметим, что на сегодняшний день VPN запрещены в Северной Корее, Беларуси, Омане, Египте, Китае, Иране, Уганде, а также в Индии. Граждане других государств имеют свободный доступ к сервисам.

Компаративный анализ законодательства в сфере связи и передачи компьютерных данных по сетям стран Содружества Независимых Государств показал, что Закон Республики Казахстан от 5 июля 2004 года № 567-II «О связи»[2] запрещает работу сетей и (или) средств связи, оказание услуг связи, доступ к интернет-ресурсам

---

[1] О внесении изменений в Критерии оценки материалов и (или) информации, необходимых для принятия Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено", утвержденные приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 февраля 2023 г. № 25 : приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 8 ноября 2023 г. № 168 // Гарант : сайт. URL: https://base.garant.ru/408110657/ (дата обращения: 30.09.2024).

[2] О связи : Закон Республики Казахстан от 5 июля 2004 года № 567-II : послед. ред. // ЮРИСТ: Законы, Постановление, Приказы, Кодексы в РК : сайт. URL: https://online.zakon.kz/Document/?doc_id=1049207 (дата обращения: 30.09.2024).

и (или) размещенной на них информации в целях доступа к информации, запрещенной вступившим в законную силу решением суда или законами Республики Казахстан.

По нашему мнению, меры, направленные на противодействие использованию на территории Российской Федерации информационно-телекоммуникационных сетей и информационных ресурсов, доступ к которым ограничен, не являются в достаточной мере эффективными ввиду отсутствия в уголовном законодательстве соответствующей ответственности за их нарушение.

Здесь, по нашему мнению, уместно закрепить в части 1 статьи 273 УК РФ ответственность за размещение в сети Интернет программного обеспечения, позволяющего использовать информационные ресурсы, доступ к которым ограничен на территории Российской Федерации, и изложить ее в следующей редакции:

«Создание и распространение компьютерных программ, обеспечивающих использование информационных ресурсов, доступ к которым ограничен.

1. Создание и распространение компьютерных программ, обеспечивающих использование информационных ресурсов, доступ к которым ограничен, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.».

В настоящее время, по данным сайта Countrymeters[1], население Земли составляет более 8,1 млрд человек, а четвертая версия интернет-протокола IP-IPv4, которую до сих пор использует большинство интернет-провайдеров в России, может создать лишь 4 млрд IP-адресов. Так как последний блок IP-адресов данного протокола в России распределили еще в 2019 году, интернет-компаниям придется сделать новые версии сайтов, поддерживающие стандарт IPv6, а операторам связи – модернизировать сети.

По состоянию на начало июня 2023 года доля интернет-трафика IPv6 в России составила 8,16 % от общего объема передаваемых данных[2]. Данное обстоятельство создает проблемы правоохранительным органам в установлении конкретного лица, пользующегося IP-адресом. Это связано с тем, что нескольким пользователям сети Интернет может присваиваться один и тот же цифровой идентификатор.

Отдельно следует отметить программы, позволяющие шифровать информацию, хранящуюся на электронных носителях информации. Нередко злоумышленники, которые профессионально занимаются преступной деятельностью, знают и используют специализированное программное обеспечение (далее – ПО). позволяющее осуществить несанкционированное использование компьютерной информации, хранящейся на электронном носителе. В таких случаях дешифровка пакета цифровых данных невозможна. Примером программного обеспечения, находящегося в открытом доступе, может служить приложение TrueCrypt, используя

[1] Население Земли // Countrymeters : сайт URL: https://countrymeters.info/ru/World (дата обращения: 09.09.2024).

[2] IPv6 // TADVISER : сайт. URL: https://www.tadviser.ru/index.php/Статья:IPv6 (дата обращения: 09.09.2024).

которое, можно полностью зашифровать какой-либо электронный носитель информации или его раздел.

Существует также программное обеспечение, позволяющее дистанционно перепрограммировать электронное устройство до заводских настроек либо полностью удалить информацию. Например, на сайте Лайфхакер [1] доступны 10 подобных программ и инструкции по их применению.

В связи с изложенным нам представляется уместным рекомендовать отключение электронных устройств от сетей питания при проведении следственных действий и оперативно-розыскных мероприятий в целях предотвращения дистанционного доступа к файлам и воздействия на них.

Также отдельно следует выделить время как один из ключевых «врагов» правоохранительных органов. Расследование по горячим следам – один из наиболее эффективных способов борьбы с преступностью, которым всегда пользовались полицейские структуры. Однако сейчас существуют технические сложности отслеживания передаваемой информации через интернет-мессенджеры, т. к. данные сервисы заботятся о клиентах и шифруют переписки при помощи электронных ключей, которые создаются и хранятся на устройствах пользователей, исключая внешние сервисы. Такой способ защиты персональной информации, с одной стороны, представляется эффективным для пользователя, но с другой – затрудняет работу ряда правоохранительных органов, занимающихся противодействием IT-преступности, для которых важно оперативное получение информации о преступлении.

Злоумышленники, как и правоохранительные структуры, находятся в постоянном поиске новых подходов к ведению своей деятельности. Так, изменился способ незаконного сбыта наркотиков: от схемы «из рук в руки» – к дистанционному посредством информационных ресурсов. Если организатор не оставляет цифрового следа в киберпространстве, то тем самым усложняет для оперативных подразделений процесс своего поиска, о чем писали многие ученые, например профессор Ю. В. Гаврилин [4, с. 126].

В настоящее время, несмотря на широкие возможности использования электронных устройств, существуют ограничения. В качестве примера можно привести камеры видеонаблюдения, которые имеют определенный запас памяти для хранения файлов и определенное качество съемки. В среднем объема их памяти хватает на 30 суток, а дальше происходит процесс перезаписи [5, с. 101]. Соответственно, если возникнет необходимость получить запись о событии, произошедшем за этими временными рамками, сделать это будет невозможно.

Большая часть работы подразделений по борьбе с киберпреступностью строится на отправлении запросов по материалам проверки сообщений о преступлениях и уголовным делам с последующим получением ответов. Множество компаний расположено в странах, которые официально прекратили сотрудничество с Российской Федерацией по политическим мотивам. Например, серверы популярного на

[1] Козориз А. 10 бесплатных программ для удаленного доступа к компьютеру // ЛАЙФХАКЕР : сайт. URL: https://lifehacker.ru/udalyonnyj-dostup-k-kompyuteru/ (дата обращения: 09.09.2024).

территории Российской Федерации мессенджера Telegram расположены в Объединенных Арабских Эмиратах, а соответственно, получить информацию о переписках пользователя и других цифровых следах его аккаунта без физического доступа к носителю информации, с которого осуществлялось использование приложения, не получится.

Отечественные же компании могут не отвечать на запросы длительный промежуток времени, что приводит к осложнению процедуры предварительного следствия. Кроме того, как мы уже отмечали, применение таких оперативно-розыскных мероприятий, как наведение справок, снятие информации с технических каналов связи и получение компьютерной информации, неэффективно как ввиду специфики, практически полной анонимности резидентов сети, так и принципов функционирования сети DarkNet (отсутствие правового регулирования данного сегмента сети Интернет) [6, с. 171]. В настоящее время в законодательстве не определен срок ответа частных компаний на запросы правоохранительных органов.

Согласно ряду федеральных законов (от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», от 07.02.2011 № 3-ФЗ «О полиции», от 28.12.2010 № 403-ФЗ «О Следственном комитете Российской Федерации» и др.), у правоохранительных органов и судов есть полномочия обращаться в технологические компании за сведениями о пользователях.

Однако в настоящее время существуют сложности в получении персональных данных пользователя, хранящихся на серверах частных компаний. Поскольку российская социальная сеть «ВКонтакте» предоставляет переписку пользователя, содержащую информацию о преступлении, на основании судебного решения, оперативным сотрудникам из разных регионов необходимо добраться до одного из десяти офисов компании, представленных в шести городах[1].

Абсолютное большинство исследуемых преступлений являются латентными, а лица, совершившие киберпреступления, продолжают оставаться безнаказанными. В Интернете ежедневно публикуется информация о том, что неизвестные продавцы «слили» в Darknet базу данных какого-либо приложения. В зависимости от приложения такая база данных может содержать различную персональную информацию пользователя. Например, сервисы доставки, как правило, собирают данные о месте доставки (жительства), фамилии, имени и отчестве лица, оставившего заказ, номере мобильного телефона и другую информацию.

В судебной практике существуют случаи, когда злоумышленники сами выдавали преступный характер своей деятельности. Например, при осуществлении денежного перевода за покупку какого-либо запрещенного товара прямо указывали, за что переводят деньги.

Сегодня организованные преступные группы в основном осуществляют свою деятельность в виртуальном пространстве. В целом, как отмечали исследователи еще в 2015 году, структура киберпреступной группы ненамного отличается от структуры традиционной преступной группы [7, с. 127]. При систематическом совершении IT-

[1] VK объединяет // vk.company : сайт. URL: https://vk.company/ru/company/contacts/ (дата обращения: 09.09.2024).

преступлений данные преступные группы используют специальное программное обеспечение, применяют методы анонимизации в сети Интернет, а соответственно, оставляют меньше цифровых следов, пригодных для их идентификации.

Телефонное мошенничество – один из самых быстрорастущих сегментов криминального рынка. Миллионы звонков от мошенников поступают россиянам ежедневно, а основным субъектом, осуществляющим подобные действия, выступают кол-центры, расположенные на территории других государств. Данные преступления являются дистанционными и носят транснациональный характер, что затрудняет, а в ряде случаев делает невозможным их расследование по причине сложности в установлении лица, их совершившего, и доказывании его виновности. Даже если звонок был совершен с IP-адреса, принадлежащего одному лицу, это не означает, что в интересующий правоохранительные органы момент времени именно оно пользовалось данным IP-адресом.

В наши дни популярность набирают SIM-Box – сервисы, которые также называются SIM-банками, или SIM-фермами (рис. 1). Данные сервисы предоставляют пользователям удаленный доступ к одноразовым SIM-картам. Один SIM-Box может содержать до 300–400 SIM-карт [8, с. 94]. При этом для оператора связи точкой регистрации SIM-карты будет расположение того шлюза, с которым она сейчас работает, а не действительное ее месторасположение[1].

Вред при помощи таких сервисов наносится не только самим пользователям, которых мошенникам удается обмануть, но и операторам связи, в обход которых мошенники осуществляют свою деятельность. В ряде случаев, если правоохранительным органам удается установить номер телефона, с которого были совершены мошеннические действия, – это лишь начало цепочки, которая приводит к подобным SIM-фермам, а не к лицу, непосредственно совершившему преступное посягательство.

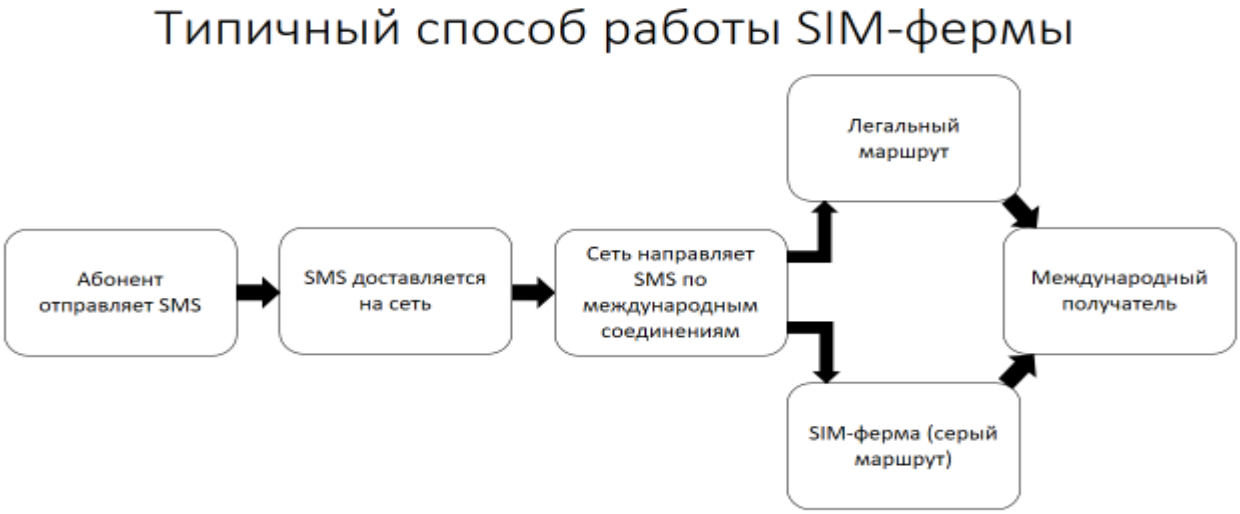

Рис. 1. Принцип работы SIM-фермы

[1] Что такое SIM-банк и как он работает // Хабр : веб-сайт. URL: https://habr.com/ru/companies/arttel/articles/369963/ (дата обращения: 09.09.2024).

Также в Российской Федерации не предусмотрена ответственность за передачу или продажу банковских карт, которые могут служить средствами платежа для преступников. Как правило, при таких обстоятельствах лицо целенаправленно не блокирует банковскую карту, в отличие от случаев краж или утери. Соответственно, чужие банковские карты являются одним из средств анонимизации производимых преступных транзакций. Как и SIM-карты, банковские карты могут оформляться на лиц, ведущих люмпенизированный образ жизни.

Проблемы продажи банковских карт и возможности дальнейшего регулирования данных процессов в настоящее время не получили широкого отражения в научной литературе.

Важным в таких ситуациях представляется установление цифровых следов, которые злоумышленники могут оставить при использовании данных средств.

Говоря о несовершенстве законодательства, отметим, что Уголовный закон и уголовно-процессуальное право, их материальная составляющая недостаточно динамично совершенствуются. Например, статьей 272 УК РФ за неправомерный доступ к компьютерной информации (ее уничтожение, модификацию, копирование и блокирование) предусмотрена уголовная ответственность. Однако законодательно не предусмотрена ответственность за ознакомление с подобной информацией. Адвокат Павел Домкин [1] полагает, что если лицо визуально ознакомилось с информацией, хранящейся на устройстве, то данное деяние не может расцениваться как копирование. Хоть лицо и фиксирует в своей памяти изученную информацию, оно не может ей воспользоваться. По смыслу состава преступления, квалифицируемого по ст. 272 УК РФ, для лица, совершившего подобное деяние, не наступит никаких последствий.

В то же время в статье 8 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2] понятие «доступ» толкуется как поиск и получение любой информации в любых формах и из любых источников. Сложность предполагается в соотнесении понятий «получение» и «ознакомление».

Если сравнить нормы статьи 272 УК РФ и статьи 283 УК РФ, то мы видим, что в ст. 283 разглашение сведений, составляющих государственною тайну, имеет форму активных действий, например в демонстрировании документов или устной беседе, что по своей сути предполагает ознакомление другого лица с какими-либо сведениями.

По нашему мнению, несанкционированное ознакомление тоже можно расценивать как активное действие, а соответственно, преступное деяние, вне зависимости от того, с какой информацией ознакомился пользователь, в случаях, если она охраняется законом.

---

[1] Адвокатское бюро «Домкины и партнеры» : сайт. URL: https://www.advodom.ru/ (дата обращения: 12.02.2024).

[2] Об информации, информационных технологиях и о защите информации : Федер. закон № 149-ФЗ : принят Гос. Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 21.09.2024).

Полагаем, что назрела объективная необходимость дополнения части 1 статьи 272 УК РФ путем изложения ее в следующей редакции: «Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию, копирование информации либо ознакомление с ней».

Ключевой проблемой доказывания факта ознакомления с информацией является сложность в установлении субъективной стороны состава преступления. Предполагается, что доказательствами в данном случае могли бы являться задокументированные факты воспроизведения подобной информации на каких-либо носителях, а также задержание лица с поличным в процессе ознакомления с охраняемой законом компьютерной информацией.

В наши дни граждане Российской Федерации не всегда понимают, что в отношении них было совершено киберпреступление, а соответственно, не сообщают о нем в правоохранительные органы. Существующие уголовное и уголовно-процессуальное законодательства продолжают адаптироваться к новой угрозе развития цифрового общества, и не всегда положения федеральных законов позволяют эффективно квалифицировать совершенное деяние.

Деятельность преступников обуславливает постоянное совершенствование и деятельности по противодействию киберпреступности. Новые подразделения, созданные в экспертно-криминалистических центрах МВД России, занимающиеся проведением компьютерных экспертиз, нуждаются в специалистах, а ведомственные институты как единицы комплектования для данных подразделений – в преподавателях, имеющих практический опыт борьбы с современной угрозой цифрового общества.

Неурегулированным и дискуссионным остается ряд вопросов, касающихся процессуальных процедур работы с электронными носителями информации, но бесспорным представляется тот факт, что институты работы с ними продолжат развиваться в ближайшие годы.

В проведенном исследовании нами выявлены основные проблемы, возникающие при использовании цифровых следов в уголовном судопроизводстве, и предложены варианты решения проблемы.

Обычному пользователю цифровых устройств, как правило, не по силам удалить свой цифровой след из сети Интернет, однако он может скрыть его от посторонних глаз. Так, идентификацию пользователя правоохранительные органы осуществляют путем направления запросов в частные компании. Принятые поправки в ряд законодательных актов, получившие в дальнейшем название «Пакет Яровой», которые обязали отечественные компании хранить переписки, телефонные звонки и иной входящий и исходящий трафик пользователей, в 2023 году набрали «предельные обороты». Это дало положительный эффект: в настоящее время существует возможность получить информацию даже в случае удаления ее с электронных устройств.

На примере некоторых электронных носителей информации мы также продемонстрировали возможность изменения и сокрытия содержащейся на них

информации. Так, Постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37[1] помогло разрешить ряд вопросов, касающихся квалификации преступлений в сфере компьютерной информации, предусмотренных статьями 272, 273, 274 и 274.1 УК РФ, а также иных преступлений, совершенных с использованием электронных технологий. Указанное Постановление разъясняет квалификацию преступлений, предусмотренных Главой 28 УК РФ, но не затрагивает другие составы преступлений, совершенных с использованием ИТТ.

По нашему мнению, в ближайшее время Верховным Судом Российской Федерации будут даны разъяснения, касающиеся работы по остальным составам преступлений, отнесенным к компетенции нового оперативного подразделения органов внутренних дел Российской Федерации – Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК). Министр внутренних дел Российской Федерации В. А. Колокольцев приказом от 31 марта 2023 года № 199[2] внес изменения в организационно-штатную структуру МВД России. В соответствии с этим подзаконным нормативным правовым актом подразделения УБК стали полноправными субъектами оперативно-розыскной деятельности.

В заключение следует сказать, что изменения, происходящие в российском обществе в части развития и повсеместного использования цифровых технологий, уже сейчас положительно влияют на эффективность расследования и раскрытия преступлений. Выделение цифровых следов в отдельный предмет криминалистических знаний и их использование в доказывании по уголовным делам – лишь часть глобальных изменений. Однако это направление исследований в области криминалистики и теории оперативно-розыскной деятельности требует выработки на практике специальных методов и средств результативной работы с цифровыми следами преступлений, а также внесения изменений в отечественное уголовное законодательство.

Исследования в области цифровых следов преступления, их классификация и постепенное устранение проблем, возникающих в работе с ними, способствуют не только повышению эффективности борьбы с преступностью, но и формированию доверия общества к правоохранительным органам, что является залогом успешного функционирования правового государства.

---

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 30.09.2024).

[2] Об утверждении Перечня оперативных подразделений органов внутренних дел Российской Федерации, правомочных осуществлять оперативно-розыскную деятельность : приказом МВД России от 31 марта 2023 года № 199 // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_455075/ (дата обращения: 30.09.2024). Режим доступа: для зарегистрир. пользователей.

СПИСОК ИСТОЧНИКОВ

1. Пороховой, Э. Ю., Быков, В. Д. О некоторых проблемах взаимодействия между государствами в расследовании транснациональных киберпреступлений // Научный дайджест Восточно-Сибирского института МВД России : электрон. науч. журн. 2022. № 2 (16). С. 82–91. URL: https://elibrary.ru/item.asp?id=49159141 (дата обращения: 12.02.2024). Режим доступа: для зарегистрир. пользователей.

2. Цифровая валюта и цифровые финансовые права как предмет и средство совершения преступлений : монография / О. П. Грибунов, П. В. Никонов, С. В. Пархоменко и др. Иркутск : Иркутский юридический институт (филиал) федерального государственного казенного образовательного учреждения высшего образования «Университет прокуратуры Российской Федерации», 2023. 170 с.

3. Денисов, И. М. Лещинский, М. И. Криминалистическое исследование цифровой информации // Международный журнал гуманитарных и естественных наук. 2023. № 1–1 (76). С. 139–141.

4. Гаврилин, Ю. В. Противодействие цифровой трансформации наркопреступности (по итогам Всероссийского онлайн-семинара) // Труды Академии управления МВД России. 2020. № 4 (56). С. 122–129.

5. Льянов, М. М. Процесс обнаружения виртуальных следов при расследовании преступлений // Юридическая наука и правоохранительная практика. 2021. № 4 (58). С. 97–106.

6. Тимофеев, С. В. Деанонимизация пользователя сети Интернет как метод оперативно-розыскного противодействия наркопреступности // Юристъ-Правоведъ. 2020. № 2 (93). С. 170–174.

7. Решняк, М. Г., Павлова, Д. А. О некоторых особенностях раскрытия преступлений в сфере высоких информационных технологий // Бизнес в законе. Экономико-юридический журнал. 2015. № 5. С. 125–129.

8. Молчанова, Т. В., Аксенов, В. А. Факторы, обуславливающие мошенничество, совершенное с использованием информационно-телекоммуникационных технологий // Вестник экономической безопасности. 2020. № 2. С. 93–98.

REFERENSES

1. Porokhovoy E. Yu., Bykov V. D. O nekotoryh problemah vzaimodejstvija mezhdu gosudarstvami v rassledovanii transnacional'nyh kiberprestuplenij [On some problems of interaction between states in the investigation of transnational cybercrimes]. Nauchnyj dajdzhest Vostochno-Sibirskogo instituta MVD Rossii - Scientific digest of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2022, no. 2 (16), pp. 82-91.

2. Gribunov O. P., Nikonov P. V., Parkhomenko S. V. Cifrovaja valjuta i cifrovye finansovye prava kak predmet i sredstvo sovershenija prestuplenij [Digital currency and digital financial rights as a subject and means of committing crimes]. Irkutsk, 2023, 170 p.

3. Denisov I. M. Leshchinsky M. I. Kriminalisticheskoe issledovanie cifrovoj informacii [Forensic study of digital information]. Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk - International journal of humanitarian and natural sciences. 2023, no. 1–1 (76), pp. 139–141.

4. Gavrilin Yu. V. Protivodejstvie cifrovoj transformacii narkoprestupnosti (po itogam Vserossijskogo onlajn-seminara) [Counteracting the digital transformation of drug-related crime (based on the results of the All-Russian online seminar)]. Trudy Akademii upravlenija MVD Rossii - Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2020, no. 4 (56), pp. 122–129.

5. Lyanov M. M. Process obnaruzhenija virtual'nyh sledov pri rassledovanii prestuplenij [The process of detecting virtual traces during crime investigation]. Juridicheskaja nauka i pravoohranitel'naja praktika - Legal Science and Law Enforcement Practice. 2021, no. 4 (58), pp. 97–106.

6. Timofeev S. V. Deanonimizacija pol'zovatelja seti Internet kak metod operativno-rozysknogo protivodejstvija narkoprestupnosti [Deanonymization of an Internet user as a method of operational-search counteraction to drug-related crime]. Jurist#-Pravoved# - Jurist-Lawyer. 2020, no. 2 (93), pp. 170–174.

7. Reshnyak M. G., Pavlova, D. A. O nekotoryh osobennostjah raskrytija prestuplenij v sfere vysokih informacionnyh tehnologij [On Some Features of Solving Crimes in the Sphere of High Information Technologies]. Biznes v zakone. Jekonomiko-juridicheskij zhurnal -Business in Law. Economic and Legal Journal. 2015, no. 5, pp. 125-129.

8. Molchanova T. V., Aksenov V. A. Faktory, obuslavlivajushhie moshennichestvo, sovershennoe s ispol'zovaniem informacionno-telekommunikacionnyh tehnologij [Factors Determining Fraud Committed Using Information and Telecommunication Technologies]. Vestnik jekonomicheskoj bezopasnosti - Vestnik of Economic Security. 2020, no. 2, pp. 93-98.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Тимофеев Сергей Владимирович, кандидат юридических наук, доцент кафедры оперативно-розыскной деятельности и специальной техники в ОВД. Восточно-Сибирский институт МВД России. 664074, г. Иркутск, ул. Лермонтова, 110.
ORCID: 0000-0002-4172-1571.

Кочесоков Рустам Хажмударович, преподаватель кафедры огневой подготовки. Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России. 360016, г. Нальчик, ул. Мальбахова, 123.
ORCID 0009-0009-4653-9312.

INFORMATION ABOUT THE AUTHORS

Timofeev Sergey Vladimirovich, Candidate of Law, Associate Professor of the Department of Operational Investigative Activities and Special Equipment. East Siberian Institute of the Ministry of Internal Affairs of Russia. 664074, Irkutsk, 110 Lermontov str..

Kochesokov Rustam Khazhmudarovich, teacher of the Department of Fire Training, North Caucasus Institute for Advanced Studies, branch of the Krasnodar University of the Ministry of Internal Affairs of Russia. 360016, Nalchik, 123 Malbakhova str.

Статья поступила в редакцию 14.09.2024; одобрена после рецензирования 15.10.2024; принята к публикации 19.12.2024.

The article was submitted 14.09.2024; approved after reviewing 15.10.2024; accepted for publication 19.12.2024.