Зенкина Виктория Вадимовна
Преподаватель
Калининградский филиал АОЧУ ВО «Московский финансово-юридический университет МФЮА»
г. Калининград, Калининградская область

DOI 10.31483/r-149506

ОСОБЕННОСТИ ПРЕДВАРИТЕЛЬНОЙ ПРОВЕРКИ СООБЩЕНИЙ О СОВЕРШЕНИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация*: в статье освещены отдельные аспекты предварительной проверки сообщения о мошенничестве в сфере компьютерной информации. Особый интерес представляют особенности сбора оперативной информации в ходе установления факта совершения преступления. На примерах судебно-следственной практики рассмотрены некоторые особенности оперативно-розыскных мероприятий, применяемых для установления факта совершения преступления и способствующих повышению эффективности расследования и раскрытия данной категории уголовных дел.*

Ключевые слова*: компьютерное мошенничество, сообщение о преступлении, оперативно-розыскные мероприятия.*

Неминуемая компьютеризация и цифровизация всех сфер жизни общества помимо очевидных преимуществ порождает уязвимость от возможных преступных посягательств, смещает акценты противоправного поведения в сферу информационных технологий.

Одним из элементов реагирования уголовно-правового законодательства на изменения, происходящие в обществе, стало введение в 2012 году [4] в Уголовный кодекс Российской Федерации статьи 159.6 «Мошенничество в сфере компьютерной информации» [1].

Научное сообщество и правоприменители до сих пор неоднозначно воспринимают факт криминализации данного преступного деяния (по тексту –

компьютерное мошенничество), что, в свою очередь, не только порождает различные варианты толкования и квалификации преступления, но и формирует мнение о его нераспознаваемости и изъянах законодательства, позволяющих преступникам в большинстве случаев уходить от ответственности или получать мягкое наказание [6; 7].

Однако успешное завершение производства по ряду уголовных дел в отношении компьютерных мошенников позволяет говорить об обратном. А низкий уровень раскрываемости исследуемых преступных деяний свидетельствует не о феномене их нераспознаваемости, а об упрощенных, шаблонных представлениях о преступности или непреступности, доказуемости или недоказуемости тех или иных посягательств, недостаточном количестве квалифицированных кадров в правоохранительных органах, недостаточной отлаженности процедур взаимодействия между правоохранительными органами и экспертными организациями. Проанализированная судебная практика (всего было изучено и обобщено за период с 2019 по 2023 г. 89 судебных актов, вынесенных по результатам уголовных дел) стала ярким примером обнаружения и раскрытия деятельности компьютерных мошенников по результатам оперативно-розыскных мероприятий на этапе предварительной проверки сообщений потерпевших.

Активное использование возможностей оперативно-розыскной деятельности способствует установлению лиц, совершивших преступление и их задержанию. Особенно эффективно использование ОРМ в ситуации, когда преступники продолжают совершать мошенничество в отношении лица, обратившегося в правоохранительные органы. Разработка и реализация плана совместных действий следственных органов (органов дознания) и оперативных подразделений увеличивает шансы на задержание всех участников преступной деятельности с поличным, позволяет собрать наибольший объем доказательственной и ориентирующей информации и является основной особенностью предварительной проверки сообщения о совершенном компьютерном мошенничестве.

В одном из случаев (дело №1-01/2017 рассмотрено Замоскворецким районным судом города Москвы [9]) обвиняемые в похищении 59,9 млн рублей из

банкоматов ОАО АКБ «Авангард», по мнению ряда экспертов, были связаны со знаменитой группировкой Carbanak (по названию используемого ею одноименного вредоносного ПО для проникновения в защищенный периметр корпоративных сетей кредитных компаний).

В другом (дело №1-1/2022 рассмотрено в Кировском районном суде г. Екатеринбурга [8]) – жертвами злоумышленников – участников легендарного преступного сообщества под названием Lurk (от англ. «затаиться», «подстерегать», по наименованию вредоносного программного обеспечения), обвиненных в хищении почти 3 млрд рублей, стали ПАО АКБ «Металлинвестбанк» и еще ряд коммерческих организаций. Группировка, в состав которой входило примерно 15 человек (на последнем этапе ее деятельности число «постоянных» соучастников возросло до 40, по рассматриваемому делу проходил 21 обвиняемый) обеспечивала, что называется, «полный цикл» разработки, доставки и монетизации вредоносных программ – этакая небольшая компания по разработке программного обеспечения.

Своевременное обращение потерпевших в правоохранительные органы, исследование атакованных вредоносным программным обеспечением (ВПО) компьютеров, изучение доступных в открытых источниках данных, своевременное привлечение к оперативно-розыскным мероприятиям экспертов в области цифровой криминалистики – только эти меры уже позволяют составить примерное представление о лицах, которые предположительно имеют отношение к преступлению.

Участники выше описанных преступных групп имели хорошее представление о средствах анонимизации своей активности в сети Интернет, активно использовали шифрование в повседневных коммуникациях, фальшивые данные для регистрации доменов или сервисы анонимной регистрации и т. д. И всё же и они совершали ошибки, пусть незначительные и редкие на первый взгляд. Но уверенность преступников в своей неуязвимости, невозможности раскрыть подобное преступление рано или поздно приводит к накоплению таких ошибок и, соответственно, формированию следовой картины преступлений.

Так, например, поиск разработчиков ВПО, специалистов, отвечающих за работоспособность серверов управления, их защиту от обнаружения и перехвата управления ими мошенники осуществляют на обычных сайтах по подбору персонала для удаленной работы. Не исчезают данные об аккаунтах электронной почты, социальных сетей, мессенджерах (для описанных группировок средством общения был «jabber»). Всю эту информацию следствие получило по результатам оперативно-розыскных мероприятий «снятие информации с технических каналов связи» (ОРМ «СИТКС»), проведенных в ходе предварительной проверки сообщений о преступлении. В рамках названного вида ОРМ с участием специалиста в области информационной безопасности производилось удаленное копирование данных, содержащихся на серверах злоумышленников, что позволило не только выявить ВПО и следы несанкционированного доступа злоумышленников к компьютерам и сетевым устройствам юридических лиц и их клиентов, но и обнаружить переписку злоумышленников о создании, распространении и использовании ими вредоносных программ. Таким образом, была собрана информация, прямо указывающая на лиц, которые оказывали незаконное воздействие на программное обеспечение серверов, компьютеров и сами информационно-телекоммуникационные сети с целью хищения денежных средств.

В ходе прослушивания телефонных переговоров удалось установить лиц, причастных к обналичиванию похищенных денежных средств, тех, кто непосредственно снимал их в банкоматах, осуществлял действия по регистрации фиктивных юридических лиц, на счета которых с помощью ВПО выводились денежные средства потерпевших кредитных организаций и физических лиц, управлению такими счетами. Были также запрошены видеозаписи банкоматов из кредитных и близлежащих организаций. Комплекс мероприятий и анализ данных помогли установить внешние признаки причастных лиц. Согласно свидетельским показаниям оперативного сотрудника в ходе судебного разбирательства люди, которые снимали деньги, не использовали средства маскирования. Подсудимые в ходе судебного разбирательства подтверждали, что для об-

щения по «работе» все пользовались своими телефонами и абонентскими номерами, для перевода вознаграждения за выполнение действий согласно оговоренным в группе ролям (они его называли зарплатой) использовали личные банковские карты, мер конспирирования не предпринимали.

Оформленные справками об исследовании специалистом и актами ОРМ перечисленные данные стали основой доказательственной базы по описанным делам и не дали преступникам уйти от наказания.

Как следует из приведенных примеров, составляющих лишь незначительную часть эпизодов проверки, все используемые сообщниками по преступлениям способы оперативной связи друг с другом те же, которыми пользуются все преступники на протяжении последних десятилетий. Скорость связи компьютерного мошенника с сообщниками не отличается от скорости связи для обычного мошенника или взяточника. Помимо прочего, материалы ОРД свидетельствуют о том, что преступники, используя технологии цифровой анонимизации (шифрование данных с помощью специальных программ для маскировки IP-адресов, выходы в сеть Интернет через публичные точки доступа и т. п.), одновременно позволяют себе оставлять следы в социальных сетях, электронной почте, на видеокамерах, линиях телефонной связи. Результат проверки при таких обстоятельствах зависит не столько от быстроты действий оперативных работников, сколько от их своевременных действий по привлечению для проведения предварительных исследований специалистов в области информационной безопасности, постоянному обмену информацией между ними и сотрудниками правоохранительных органов с соблюдением ограничений, которые законодательство накладывает на определенные виды информации, составлению соответствующих справок, их нормативно предусмотренному оформлению, что, в свою очередь, позволяет легализовать данные, полученные оперативным путем.

Именно вопрос о легализации результатов ОРМ в рамках уголовного процесса на практике вызывает самые большие затруднения у сотрудников оперативно-розыскных подразделений. В своем первоначальном виде, до придания

им процессуальной формы, результаты оперативно-розыскных мероприятий доказательствами считаться не могут, а сами мероприятия, не соответствуя познавательной и процессуальной характеристике следственных действий, не являются таковыми. Следователь признает собранную информацию доказательством, если она соответствует требованиям относимости и допустимости. В этой связи особое значение имеет знание оперативными работниками Инструкции о порядке предоставления результатов ОРД органу дознания, следователю или в суд [5]. При соблюдении её положений, а также требований статьи 89 УПК РФ [2], статьи 8 Федерального закона от 12.08.1995 N 144-ФЗ «Об оперативно-розыскной деятельности» [3] легализация результатов ОРМ возможна и на стадии досудебного производства. Во всяком случае, только при условии, что известны происхождение и способы получения доказательственной информации, такая информация может стать доказательством уже в уголовно-процессуальном смысле.

Таким образом, анализ отечественных источников, обобщение судебной практики и процессуальные нормы доказывают, что производство ОРМ с применением средств технического контроля жизни граждан (прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации), являясь неотъемлемой частью проверки сообщения о компьютерном мошенничестве, служит не только установлению основания возбуждения уголовного дела. Результаты ОРМ, полученные на этапе рассмотрения сообщения о противоправном деянии, оказывают влияние на формирование следственных ситуаций первоначального этапа расследования исследуемых преступлений и механизма их разрешения, могут быть впоследствии использованы как ориентирующие при планировании проведения различных следственных действий либо приобщены к материалам дела в качестве доказательства. Выдвижение версий, определение подлежащих выяснению вопросов, а также комплекс подлежащих проведению действий выстраивается вокруг ситуации, складывающейся на момент получения оперативной информации о событии.

Список литературы

1. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 №63-ФЗ (ред. от 23.03.2024), принят Государственной Думой 24 мая 1996 года, одобрен Советом Федерации 5 июня 1996 года // СПС «КонсультантПлюс».

2. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 №174-ФЗ (ред. от 23.03.2024), принят Государственной Думой 22 ноября 2001 года, одобрен Советом Федерации 5 декабря 2001 года // СПС «КонсультантПлюс».

3. Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 №144-ФЗ (ред. от 29.12.2022), принят Государственной Думой 5 июля 1995 года // СПС «КонсультантПлюс».

4. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 29.11.2012 №207-ФЗ (ред. от 03.07.2016), принят Государственной Думой 23 ноября 2012 года, одобрен Советом Федерации 28 ноября 2012 года // СПС «КонсультантПлюс».

5. Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: утверждена от 27.09.2013 Приказом МВД России №776, Минобороны России №703, ФСБ России №509, ФСО России №507, ФТС России №1820, СВР России №42, ФСИН России №535, ФСКН России №398, СК России №68 // СПС «КонсультантПлюс».

6. Григорян Г.Р. Об объекте мошенничества в сфере компьютерной информации /Г.Р. Григорян // Российская юстиция. – 2018. – №5. – С. 29–31; СПС «КонсультантПлюс». EDN XNSLIT

7. Лопашенко Н.А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? / Н.А. Лопашенко; под ред. О.А. Кузнецовой, В.Г. Голубцова, Г.Я. Борисевич [и др.] // Пермский юридиче-

ский альманах. Ежегодный научный журнал. – 2019. – №1. – С. 598–609; СПС «КонсультантПлюс». – EDN CIQENR

8. Архив Кировского районного суда г. Екатеринбурга Свердловской области: приговор по делу №1-1/2022 (1-1/2021, 1-3/2020, 1-52/2019, 1-650/2018) от 08.02.2022 [Электронный ресурс]. – Режим доступа: https://kirovsky--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=2&name_op=case&case_id=271884867&case_uid=0067e968-0ed8–4ce2-b547-205c6e5e80a5&delo_id=1540006 (дата обращения: 05.02.2024).

9. Архив Замоскворецкого районного суда города Москвы: приговор по делу №1-01/2017 [Электронный ресурс]. – Режим доступа: https://mos-gorsud.ru/rs/zamoskvoreckij/services/cases/criminal/details/edbd924a-6d7d-4903-9a84-1f6b7cbf50ce?participant=%D0%A2%D0%B0%D0%BC%D0%B1%D0%BE%D0%B2%D1%86%D0%B5%D0%B2 (дата обращения: 10.03.2024).