МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ВОЛГОГРАДСКАЯ АКАДЕМИЯ

С. М. Голятина

Криминалистическая теория и практика расследования хищений электронных денежных средств

Монография

под научной редакцией А. П. Алексеевой

Волгоград
ВА МВД России
2021

УДК 343.985.7:343.7
ББК 67.523.12
Г 60

Одобрено
редакционно-издательским советом
Волгоградской академии МВД России

Голятина, С. М.

Г 60 Криминалистическая теория и практика расследования хищений электронных денежных средств : монография / С. М. Голятина ; под научной редакцией А. П. Алексеевой. – Волгоград : ВА МВД России, 2021. – 184 с.

ISBN 978-5-7899-1308-6

В монографии рассмотрены особенности оборота электронных денежных средств, дана криминалистическая характеристика хищений электронных денег, проанализирована специфика первоначального, последующего и завершающего этапов расследования указанных преступлений, уделено внимание тактике производства отдельных следственных действий. Выводы, полученные автором в процессе исследования, помогут устранить недостатки криминалистического обеспечения расследования анализируемых уголовно наказуемых деяний и усовершенствовать типовую методику расследования хищений электронных денежных средств.

Монография предназначена для курсантов и слушателей образовательных организаций системы МВД России, сотрудников следственных подразделений органов внутренних дел.

УДК 343.985.7:343.7
ББК 67.523.12

Рецензенты: заместитель начальника – начальник следственного отдела ОМВД России по Урванскому району *А. С. Закаев*; начальник кафедры криминалистики Калининградского филиала Санкт-Петербургского университета МВД России кандидат юридических наук, доцент *Е. А. Клоков.*

ISBN 978-5-7899-1308-6

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

XXI век с уверенностью можно назвать веком информации, Интернета и новейших технологий. Сегодня цифровизация охватила практически все сферы жизнедеятельности человека. Компьютеры, смартфоны, планшеты и прочие девайсы стали неотъемлемой частью нашего существования, а глобальная сеть – привычной средой. В Интернете люди не только общаются, но и работают, совершают покупки, строят бизнес, смотрят кино, бронируют билеты и гостиницы и т. д. Согласно отчету о состоянии цифровой отрасли Digital 2020 на начало минувшего года более 4,5 млрд жителей нашей планеты пользовались Интернетом, а аудитория социальных сетей перешагнула отметку в 3,8 млрд человек. К январю 2021 г. эти цифры составили 4,66 млрд и 4,2 млрд соответственно. В России на начало этого года насчитывалось 124 млн интернет-пользователей, 99 млн россиян имели страницы в различных социальных сетях[1].

Не последнюю роль в увеличении количества интернет-пользователей сыграла пандемия коронавирусной инфекции COVID-19: в то время как «офлайн-жизнь была поставлена на паузу», те, кто хотел бороться, начали «активно переводить продажи в онлайн, туда же последовали и рекламные бюджеты»[2]. По оценкам экспертов основными трендами Рунета в 2020 г. стали «пандемические» технологии, телемедицина, удаленная работа, игровая индустрия и стриминги[3]. Здесь же стоит назвать и онлайн-торговлю: в России число покупок в интернет-магазинах в минувшем году выросло на 78 %[4]. Все это наряду с «цифровым невежеством»[5] обусловило значительное увеличение количества киберпреступлений.

---

[1] См.: Вся статистика Интернета и соцсетей на 2021 год – цифры и тренды в мире и в России. URL: https://www.web-canape.ru/business/vsya-statistika-interneta-i-socsetei-na-2021-god-cifry-i-trendy-v-mire-i-v-rossii/ (дата обращения: 26.03.2021).

[2] «Этот год стал серьезным тестом для всех отраслей, и интернет-отрасль этот тест прошла»: эксперты подвели итоги года Рунета. URL: https://raec.ru/live/branch/12132 (дата обращения: 20.06.2021).

[3] Там же.

[4] См.: Интернет-торговля в России 2020. URL: https://datainsight.ru/DI-eCommerce-2020 (дата обращения: 20.06.2021).

[5] См.: Пандемия и цифровое невежество: эксперты назвали причины роста киберпреступности в России. URL: https://online47-ru.turbopages.org/ (дата обращения: 20.06.2021).

Приведенный тезис подтверждается статистическими данными о состоянии киберпреступности, полученными из ряда субъектов Российской Федерации. Так, в Волгоградской области в 2020 г. правоохранительными органами было зарегистрировано 8 563 преступления, совершенных с использованием информационно-телекоммуникационных технологий (аналогичный период прошлого года (далее – АППГ) – 5 719, +2 844), практически каждое второе из них было совершено на территории административного центра региона – 4 624 (АППГ – 2 993, +1 631)[1]. При этом наблюдается увеличение остатка нераскрытых преступлений – 7 282 (АППГ – 4 242, +3 045). В Ростовской области в минувшем году было зарегистрировано 13 403 IT-преступления (АППГ – 7 383, +6 020), не раскрыто 11 401 преступление (АППГ – 5 977, +5 424)[2]. Согласно данным информационного центра МВД России по Карачаево-Черкесской Республике, в 2020 г. число зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, составило 1 063 (АППГ – 848, +215), не раскрыто 123 преступления (АППГ – 27, +96)[3]. Сотрудниками УМВД России по городскому округу Нальчик в 2020 г. было зарегистрировано 779 IT-преступлений (АППГ – 410, +369), не раскрыто – 687 преступлений (АППГ – 250, +437)[4].

На расширенном заседании коллегии МВД России, прошедшем 3 марта 2021 г., Министр внутренних дел Российской Федерации В. А. Колокольцев отметил: «…криминальные деяния, совершенные с использованием IT-технологий, составляют все большую долю в общей структуре преступности. Сегодня она достигла

[1] Справка ГУ МВД России по Волгоградской области «О состоянии работы правоохранительных органов по выявлению, пресечению и расследованию преступлений против собственности, совершенных с использованием информационно-телекоммуникационных технологий».

[2] Сведения ГУ МВД России по Ростовской области о преступлениях, совершенных с использованием информационно-коммуникационных технологий.

[3] Данные ИЦ МВД России по Карачаево-Черкесской Республике о количестве преступлений, совершенных с использованием информационно-коммуникационных технологий.

[4] Справка о состоянии служебной деятельности по мошенничествам и кражам с банковских карт, совершенных с использованием информационно-коммуникационных технологий, УМВД России по г. о. Нальчик.

двадцати пяти процентов. Динамика ежегодного прироста фиксируется последние несколько лет. Данные изменения являются отражением глобальных тенденций. Своеобразным „катализатором“ здесь стала пандемия, которая повлекла масштабный „уход в онлайн“ многих сфер жизнедеятельности общества»[1].

Построение информационно-телекоммуникационной инфраструктуры закономерно вызвало появление новых форм общественно опасных посягательств на традиционно охраняемые законом общественные отношения. Так, согласно данным Генеральной прокуратуры Российской Федерации, в 2020 г. в России было совершено 510 400 киберпреступлений, каждое второе из которых было мошенничеством. Общая сумма ущерба, причиненного злоумышленниками, составила 150 млрд руб.[2] Самыми популярными схемами совершения интернет-мошенничества стали бинарные опционы, мгновенные игры и казино, фейковые объявления на популярных сайтах, реклама ставок на спорт, попрошайничество, лотереи и розыгрыши, взлом страниц в социальных сетях, «выгодные» предложения от «банков», «компенсации» от различных фондов и др. Центробанк России утверждает, что в минувшем году «самый большой объем мошеннических транзакций пришелся на интернет-платежи – 1,2 млрд рублей <…> Доля операций с использованием социальной инженерии составила 64 %, вырос средний чек похищенных средств с 7,6 тысячи рублей до 8,6 тысячи рублей. На 27 % вырос объем мошеннических переводов с помощью банковских услуг, а сумма транзакций увеличилась с 17,5 тысячи рублей до 30,3 тысячи рублей год к году за счет ряда разовых крупных хищений. В 2020 году выросло количество всех видов атак»[3].

---

[1] Выступление Министра внутренних дел Российской Федерации генерала полиции Российской Федерации Владимира Колокольцева на расширенном заседании коллегии Министерства внутренних дел Российской Федерации. URL: мвд.рф (дата обращения: 10.03.2021).

[2] См.: Состояние преступности в России за январь–декабрь 2020 г. URL: genproc.gov.ru›upload/iblock/aab…декабрь2020.pdf (дата обращения: 08.05.2021).

[3] Евсеева Е. ЦБ: объем мошеннических операций в 2020 году в России вырос на 32 % – до 2,5 млрд рублей. URL: https://vc.ru/finance/192576-cb-obem-moshennicheskih-operaciy-v-2020-godu-v-rossii-vyros-na-32-do-2-5-mlrd-rubley (дата обращения: 07.04.2021).

В настоящем исследовании фокус нашего внимание будет сосредоточен на электронных деньгах, которые сегодня входят в тройку самых популярных средств платежа у россиян[1]. Это обусловлено возможностью использовать их в любое время в любом месте, низкими комиссиями за транзакции, высокой скоростью перевода, бесперебойной работой платежных систем, отсутствием необходимости заполнять документы, снижением издержек обращения и. т. д. Кроме того, сделать акцент на электронных деньгах нас заставляет высокий темп роста прекаризации: с 14 млн человек в 2020 г. до 71 млн человек в 2021 г.[2] Последнее замечание особенно важно, поскольку все чаще фрилансеры отдают свое предпочтение именно электронным деньгам.

В монографии дана авторская дефиниция понятия электронных денежных средств, указаны их отличия от наличных и безналичных денег, криптовалюты, электронных средств платежа, что приобретает свою актуальность в связи с тем, что в последнее время суды нередко исключают из обвинения квалифицирующий признак «а равно хищение электронных денежных средств» по причине их неверного определения; проанализированы основные модели механизмов хищений электронных денежных средств; уточнен перечень элементов криминалистической характеристики данных преступлений; рассмотрены особенности первоначального, последующего и завершающего этапов их расследования.

[1] См.: Как и за что россияне платят онлайн в 2020 году: исследование Mediascope. URL: https://www.shopolog.ru/metodichka/payments/kak-i-za-chto-rossiyane-platyat-onlayn-v-2020-godu-issledovanie-mediascope/ (дата обращения: 02.02.2021).

[2] См.: Сапожникова М. Свобода по выбору: настоящее и будущее фриланса в России. URL: https://trends-rbc-ru.turbopages.org/turbo/trends.rbc.ru/s/trends/social/-60c8e3139a79472ba64fde35 (дата обращения: 07.04.2021).

ГЛАВА 1 ОСОБЕННОСТИ СОВЕРШЕНИЯ ХИЩЕНИЙ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

1.1. Характеристика электронных денежных средств и средств платежа, программно-технических и организационных средств их обеспечения

Электронные денежные средства прочно вошли в жизнь современного человека, поскольку «в условиях роста потребностей людей, изменения экономики и научно-технического прогресса» возникла «необходимость в быстрой и эффективной платежной системе, способной удовлетворять запросы как покупателей, так и продавцов»[1]. Однако, несмотря на популярность, термин «электронные денежные средства» по-прежнему интерпретируется по-разному и применяется к широкому спектру платежных инструментов, в основе которых лежат инновационные технические решения в сфере реализации розничных платежей. Это обусловило отсутствие единой, признанной во всем мире дефиниции, которая бы однозначно объясняла их экономическую и правовую природу[2].

Термин «электронные денежные средства» возник в 1970-х гг., однако феномен таких денег появился значительно раньше. В 1824 г. в Соединенных Штатах Америки была запушена система безналичных расчетов, что ознаменовало начало эры виртуальной валюты. Следующим важным событием стало изобретение телеграфа в 1837 г.: с этой даты ведется отсчет электронной коммерции. В 1858 г. телеграфная компания Mississippi Valley Printing Telegraph Company была переименована в Western Union, если ранее она занималась преимущественно отправкой почтовых телеграмм, то теперь сосредоточилась на денежных переводах, первый из которых был осуществлен в 1871 г. Со временем данная услуга приобрела популярность, и уже к 1876 г. Western Union совершила 37 190 денежных переводов. Схема работы была такой же, что и с пересылкой корреспонденции: в почтовом отделении отправитель отдавал сотруднику сумму, подлежащую переводу, последний записывал ее на бланке в специальной книге учета, который затем уходил в почтовое отделение, где по нему полу-

[1] Казимагомедова З. А., Атемова А. З. Электронные деньги в современном мире // Экономические исследования и разработки. 2020. № 4. С. 37.

[2] См.: Про электронные деньги: история появления. URL: http://niceforex.ru/2016/03/pro-electronnye-dengi-istoriya-poyavleniya/ (дата обращения: 18.03.2021).

чателю выдавались деньги. С появлением телеграфа необходимость пересылать бланк отпала, соответственно, процесс ускорился[1]. Уже к началу XX в. с помощью данного изобретения осуществлялось восемь переводов из десяти.

В середине минувшего столетия мир начал завоевывать пластик. В 1946 г. Дж. С. Биггинс организовал работу по кредитной схеме Charge-it: магазины принимали расписки за мелкие покупки, затем передавали их в банк, который вносил плату со счетов клиентов. В 1950 г. была выпущена первая многоцелевая платежная карта Diners Club Card. Считается, что она появилась благодаря бизнесмену Ф. Макнамаре, забывшему дома кошелек и не сумевшему оплатить ужин в ресторане. Чтобы впредь избегать подобных конфузов, он создал карту, действовавшую в заведениях общественного питания. Ее держателями были около 200 человек, однако уже к 1953 г. Diners Club Card получила признание в Великобритании, Канаде, Мексике и на Кубе. В 1952 г. свет увидел полноценную карту, которой можно было оплатить не только обед или ужин, но и авиа- и круизные билеты. Через несколько лет начали работу платежные системы VISA и MasterCard.

В 1971 г. компания IBM совместно с банками и авиационной промышленностью разработала международный стандарт для кредитных карт с магнитной полосой, что позволило пользоваться ими по всему миру. Кроме того, в пластик начали внедрять электронные системы авторизации.

Рост числа банковских карт обусловил увеличение количества мошенничеств с ними. В целях противодействия злоумышленникам в середине 1990-х гг. в сфере электронных платежей были разработаны регламенты и стандарты, в частности требования к технологии изготовления микропроцессорных карт EMV (Europay + MasterCard + VISA) для повышения уровня безопасности финансовых операций и специальный протокол SET (Secure Electronic Transaction) – набор цифровых сертификатов и криптографических технологий, предназначенный для аутентификации транзакций при проведении операций по карте через небезопасные сети (например, Интернет)[2].

---

[1] См.: Краткая история электронных платежных технологий. URL: https://smart-lab.ru/mobile/topic/557567/ (дата обращения: 18.03.2021).

[2] См.: Полная история кредитных карт от древности до наших дней. URL: https://kartaexpert.ru/eto-interesno/istoria-kreditnih-kart (дата обращения: 12.07.2021).

В начале 2000-х гг. платежные системы VISA и American Express стали выпускать предоплаченные карты. Сначала они пользовались особой популярностью среди родителей, поскольку позволяли им перечислять определенную сумму на счет детей и контролировать их расходы, но со временем получили распространение и у других категорий граждан[1].

Толчок развитию электронных денег дало появление сети Интернет и торговли в ней. Именно последняя требовала подходящей электронной системы платежей, которая бы позволяла оплачивать товар как внутри страны, так и за ее пределами[2]. В 1993 г. глава криптографического отдела CWI (Centrum Wiskunde & Informatica) Д. Чаум основал компанию DigiCash и предпринял попытку создания независимой системы электронных денег – eCash. Идея заключалась в том, что депозиты хранились на жестком диске компьютера пользователя, но были подписаны банком. Для управления ими и совершения операций требовались специальное программное обеспечение и подключение к сети Интернет. В основе eCash лежали слепые подписи – двухключевые криптосистемы, позволявшие осуществлять подписание электронного документа так, чтобы подписывающая сторона не имела доступа к информации, содержащейся в нем[3]. Особое внимание Д. Чаум уделял анонимности. По его словам, «в киберпространстве нет физических ограничений, нет никаких стен. Это совершенно другое, жуткое и странное место, и вопрос идентификации здесь – чистый кошмар <…> Все, что вы делаете, может видеть другой человек, все может быть записано навсегда. Это резко противоречит основному принципу демократии»[4], «…Даже при незначительных платежах регистрация того,

[1] См.: Мелкова А. Предоплаченная карта – отличия от других платежных карт. URL: https://loando.ru/statya/predoplachennye-karty-chem-otlichayutsya-ot-drugih-bankovskih-kart (дата обращения: 12.07.2021).

[2] См.: Интересные факты об электронных деньгах. Чем так любопытна цифровая валюта. URL: https://yandex.ru/turbo/finansy.name/s/upravlenie/fakty-ob-jelektronnyh-dengah.html (дата обращения: 19.05.2021).

[3] См.: Информационная безопасность: лекции (контент по дисциплине). URL: eos.ibi.spb.ru (дата обращения: 18.03.2021).

[4] Генезис-архивы: ecash Дэвида Чаума и рождение мечты шифропанков. URL: https://forklog.com/genesis-arhivy-ecash-devida-chauma-rozhdenie-mechty-shifropankov/ (дата обращения: 18.03.2021.)

кто, когда и за что заплатил деньги, является нарушением права на конфиденциальность»[1]. По задумке Д. Чаума, у пользователя была возможность тратить eCash в магазинах, не раскрывая личных данных, информации о своем счете или кредитной карте[2].

В 1994 г. в США была совершена первая покупка через Интернет, приобретаемым товаром стала пицца от Pizza Hut – большая Pepperoni с грибами и дополнительной порцией сыра. Однако существует и иная версия, согласно которой первой покупкой был диск с песнями Стинга «The Summoner's Tales», приобретенный в магазине Net Market Company в Нью-Гэмпшире. Тогда же в России презентовали первую отечественную межбанковскую платежную систему «Золотая корона».

С 1995 по 1998 гг. пользователями eCash стали около 5 000 клиентов банка Mark Twain – единственного в США, кто работал с электронными деньгами, в Европе eCash обрела популярность в Швейцарии, Германии, Австрии, Швеции и Дании[3]. В 1998 г. основанная Д. Чаумом компания обанкротилась: его стартап потерпел неудачу, не выдержав конкуренции с кредитными картами. Но этому событию предшествовало еще несколько, не менее важных: в 1995 г. платежная система Mondex создала электронный кошелек – своеобразный аналог обычного кошелька или банковского счета, представляющий собой «уникальный идентификатор, а также один или несколько интерфейсов взаимодействия с системой, позволяющих контролировать средства и осуществлять платежи»[4], а в Европе начала функционировать система PhonePaid, благодаря которой стала возможной оплата товаров и услуг с помощью мобильного телефона.

В 1997 г. появилась первая российская электронная платежная система CyberPlat, а 12 августа 1998 г. с ее помощью был проведен онлайн-платеж в пользу оператора сотовой связи «Билайн». В это же время свою первую транзакцию осуществил крупнейший в Рос-

---

[1] Ecash. URL: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:ECash (дата обращения: 18.03.2021).

[2] См.: Praxxis: как устроен анонимный цифровой «кэш» от Дэвида Чаума. URL: https://decenter.org/ru/praxxis-david-chaum (дата обращения: 22.03.2021).

[3] Там же.

[4] Электронные деньги. URL: https://www.tadviser.ru/index.php (дата обращения: 18.03.2021).

сии и странах Содружества Независимых Государств оператор электронных платежей WebMoney[1]. Вместе с тем программист М. Левчин и финансист П. Тиль, а также Л. Носек и К. Хоури основали компанию «Confinity», которая в 1999 г. запустила службу денежных переводов PayPal. В 2002 г. на суд пользователей представил свой продукт еще один российский гигант в сфере электронных денег – Яндекс.Деньги.

В начале XXI в. в мире насчитывалось уже несколько сотен электронных платежных систем, в их число входили Neteller, StormPay, PayAce, E-gold, MoneyBookers и др., в России – Яндекс.Деньги, ChronoPay, CyberPlat, WebMoney и т. д. К 2004 г. электронные деньги функционировали в 37 странах.

Отметим, что в разработке электронных платежных систем преуспели и некоторые государства Азии, в частности Китай. В 2003 г. здесь была запущена площадка для c2c-торговли – Taobao, вместе с этим начала формироваться компания Alibaba Group. В 2004 г. она создала собственную платежную систему Alipay, главное преимущество которой состояло в условном депонировании: продавец не имел доступа к средствам до тех пор, пока покупатель не подтверждал получение заказа. В 2009 г. число пользователей Alipay превысило 200 млн человек, к концу 2010 г. сервис стал ключевой частью операций Taobao и обрабатывал около 8,5 млн транзакций в день, а в 2013 г. Alipay представляла собой крупнейшую в мире платформу электронных платежей[2]. Тогда же появился мобильный кошелек Alipay Wallet. Его отличительная черта – использование технологии Sound Wave Payment, которая посредством создаваемого телефоном белого шума позволяла двум находившимся рядом устройствам с установленным Alipay Wallet обмениваться информацией. Кроме основных функций кошелек давал своему владельцу возможность оплачивать коммунальные услуги, а также совершать офлайн-платежи в POS-терминалах. Однако скажем, что за пределами

[1] См.: Виртуальные деньги: что это такое, плюсы и минусы электронной валюты. URL: https://elgreloo.com/business-and-finances/internet-money (дата обращения: 16.03.2021).

[2] См.: Финансовая империя Alibaba Group: от одного платежного сервиса до гиганта китайского рынка. URL: https://vc.ru/story/24990-ant-financial-story (дата обращения: 22.03.2021).

Китая Alipay не имеет широкого распространения, несмотря на то что поддерживает транзакции в 18 иностранных валютах[1].

За несколько десятилетий своего существования рынок электронных денег претерпел значительные изменения. По мнению аналитиков консалтинговой компании Bain&Company, метаморфозы ждут его и в ближайшем будущем. «Платежи, – на их взгляд, – перестают быть отдельной специализацией и встраиваются в многофункциональные приложения, а электронные кошельки получают все большее распространение <…> платежи и переводы дешевеют, а в какой-то момент могут стать бесплатными. Это требует от платежных компаний искать новые пути развития»[2]. С точки зрения сооснователя Bitlish[3] С. Есипова, «сейчас главный фокус – это синтез всех платежных решений в одном. Пользователи не хотят выбирать между PayPal и биткоином, они хотят иметь возможность пользоваться всем и желательно из одного интерфейса»[4]. Сказанное подтверждает и практика. Так, в Китае еще в 2013 г. был создан мессенджер WeChat, впоследствии объединивший множество сервисов. В рамках WeChat функционирует приложение Wallet, которое позволяет оперировать любыми платежными картами, эмитированными в Китае. В 2018 г. известный американский инвестор Ч. Мангер назвал WeChat главным соперником электронных платежных систем и отметил его большое будущее: «Есть только одно маленькое облачко на горизонте платежных систем, и это WeChat в Китае»[5]. В Юго-Восточной Азии также были разработаны приложения, сначала запущенные как сервисы такси, а затем вобравшие в себя функции покупки билетов, заказа доставки еды, бронирования гостиниц и т. д. Ими стали малазийский Grab и индонезийский Go-Jek.

Компания Worldpay прогнозирует, что «платежи с помощью электронных кошельков продолжат распространяться: так, при по-

[1] См.: Краткая история электронных платежных технологий. URL: https://smart-lab.ru/mobile/topic/557567/ (дата обращения: 18.03.2021).

[2] Кошельки уходят в Интернет. Bain подготовила доклад о настоящем и будущем рынка платежей. URL: https://yandex.ru/turbo/kommersant.ru/s/doc/4096264 (дата обращения: 25.03.2021).

[3] Платформа для торговли цифровыми активами.

[4] Краткая история электронных платежных технологий. URL: https://smart-lab.ru/mobile/topic/557567/ (дата обращения: 18.03.2021).

[5] Там же.

купке товаров в физических магазинах их доля к 2022 году вырастет на 18 процентных пунктов, а в случае с онлайн-торговлей – на 11 процентных пунктов. На такой способ оплаты в 2022 году будет приходиться почти половина всех платежей онлайн и более четверти платежей в обычных магазинах»[1]. Полагаем, прогноз Worldpay обоснован, поскольку сегодня электронные деньги прочно входят в тройку самых популярных средств платежа в Интернете. Например, согласно опросу Mediascope[2], только в России в 2020 г. с их помощью наряду с банковскими картами и интернет-банкингом оплата покупок производилась чаще всего. При этом активными пользователями интернет-платежей стали люди 25–34 и 35–44 лет. Банковские карты использовали 93 % жителей нашей страны 25–34 лет и 93,7 % – 35–44 лет, интернет-банкинги – 93,2 % россиян 25–34 лет и 92,8 % – 35–44 лет, электронные деньги – 81,7 % респондентов 25–34 лет и 82,2 % – 35–44 лет[3].

Таким образом, постепенно не только в России, но и в других странах оплата с помощью электронных денежных средств если не вытесняет иные формы оплаты, то составляет им достойную конкуренцию. Е. Ю. Кругова отмечает: «Электронные деньги продолжают формировать универсальные связи между людьми и предметным миром, сами не обладая никакой качественной определенностью. Мир, связи в котором опосредованы деньгами, гораздо обширнее и разнообразнее мира, основанного на естественных межличностных или идеологических связях. Развитие телекоммуникационных технологий позволяет еще более расширить пространственные и временные рамки»[4].

Ранее мы уже говорили о том, что сегодня отсутствует единое определение электронных денег. Юристы называют данным термином бессрочные денежные обязательства финансово-кредитного

---

[1] Кошельки уходят в Интернет. Bain подготовила доклад о настоящем и будущем рынка платежей. URL: https://yandex.ru/turbo/kommersant.ru/s/doc/4096264 (дата обращения: 25.03.2021).

[2] Исследовательская компания.

[3] См.: Как и за что россияне платят онлайн в 2020 году: исследование Mediascope. URL: https://www.shopolog.ru/metodichka/payments/kak-i-za-chto-rossiyane-platyat-onlayn-v-2020-godu-issledovanie-mediascope/ (дата обращения: 02.02.2021).

[4] Кругова Е. Ю. Понятие электронных денег: функциональные особенности // Социально-экономические явления и процессы. 2012. № 7-8 (041-042). С. 92.

института, выраженные в электронном виде, удостоверенные электронной цифровой подписью и погашаемые в момент предъявления обычными деньгами. Экономисты – платежный инструмент, обладающий в зависимости от схемы реализации свойствами традиционных наличных денег (возможность проведения расчетов минуя банковскую систему) и традиционных платежных инструментов (банковских карт, чеков и т. д.: возможность проведения расчетов в безналичном порядке через счета, открытые в кредитных организациях[1]).

По мнению экспертов Европейского центрального банка, электронными деньгами надлежит именовать электронный запас денежной стоимости на техническом устройстве, действующий как предоплаченный инструмент, который может быть широко использован для осуществления платежей иным, нежели эмитент, компаниям, без обязательного использования при транзакции банковских счетов[2].

Банк международных расчетов (г. Базель) применяет термин «электронные денежные средства» к денежной стоимости, измеренной в фидуциарных единицах и хранимой на устройстве, принадлежащем потребителю или доступном ему[3]. Эксперты отмечают, что приведенная дефиниция соотносится главным образом с двоичной формой скриптуальных денег, которые хранятся на неком портативном устройстве, например смарт-карте[4].

Директива Европейского Парламента и Европейского Союза 2000/46/ЕС об учреждении и деятельности организаций, эмитирующих электронные деньги, и о пруденциальном надзоре за их деятельностью понимала под электронными денежными средствами «денежную стоимость, представляющую требование к эмитенту, которая хранится на электронном устройстве, эмитируется при получении денежных средств в стоимостном размере не меньшем, чем

[1] См.: Электронные деньги: виды, характеристика и платежные системы. URL: https://mir-fin.ru/elektronnye_dengi.html (дата обращения: 21.03.2021).

[2] См.: Report of Electronic Money. European Central Bank. Frankfurt am Main. August, 1998. 47 p.

[3] См.: Survey of Electronic Money Developments. Bank for International Settlements. Committee on Payment and Settlement Systems. Basel. Switzerland. May, 2000. 104 p.

[4] См.: Типы дематериализованных денег (Dematerialized Money). URL: https://bstudy.net/660752/informatika/tipy_dematerializovannyh_deneg_dematerialized_money (дата обращения: 25.03.2021).

эмитированная денежная стоимость, принимается как средство платежа предприятиями, иными, чем эмитент»[1]. Данное определение было внедрено в денежное и банковское законодательство всех 25 стран – участниц Евросоюза. Аналогичная дефиниция содержится в тексте Директивы 2009/110/ЕС Европейского Парламента и Совета Европейского Союза об организации, деятельности и пруденциальном надзоре за деятельностью учреждений электронных денег, вносящей изменения в директивы 2005/60/ЕС и 2006/48/ЕС и отменяющей Директиву 2000/46/ЕС (распространяется на Европейскую экономическую зону): «Хранимая в электронном виде, в том числе на магнитном носителе, представленная в виде требований к эмитенту стоимость в денежном выражении, эмитируемая при получении денежных средств для проведения платежных трансакций <…> и принимаемая физическими или юридическими лицами, отличными от эмитента электронных денег»[2].

В Соединенных Штатах Америки электронные денежные средства часто «уподобляют другим предоплаченным финансовым продуктам, таким как дорожные чеки. В связи с этим, по мнению Федеральной резервной системы и Казначейства США, деятельность в сфере электронных денег, включающая: эмиссию, обращение, погашение электронных денег, – должна подпадать под действие традиционного банковского законодательства»[3].

В странах Азии электронные денежные средства определяются по-разному. Нередко их рассматривают либо как новую форму депозита, либо в качестве его близкого заменителя. Так, Банк Японии понимает под электронными деньгами электронное средство пла-

[1] Директива 2000/46/ЕС Европейского Парламента и Совета Европейского Союза от 18 сентября 2000 г. об учреждении и деятельности организаций, эмитирующих электронные деньги, и о пруденциальном надзоре за их деятельностью (отменена). URL: https://base.garant.ru/2569190 (дата обращения: 02.02.2021).

[2] Директива 2009/110/ЕС Европейского Парламента и Совета Европейского Союза от 16 сентября 2009 г. об организации, деятельности и пруденциальном надзоре за деятельностью учреждений электронных денег, вносящая изменения в директивы 2005/60/ЕС и 2006/48/ЕС и отменяющая Директиву 2000/46/ЕС (распространяется на Европейскую экономическую зону). URL: https://base.garant.ru/71312234 (дата обращения: 02.02.2021).

[3] Аллаханов С. Ю. Электронные деньги: эпоха к совершенству // Экономика, статистика и информатика. 2013. № 3. С. 7.

тежа, хранящее денежную стоимость в электронной форме (или право ее требования).

В России основы правового статуса и правил использования электронных денежных средств закреплены в Федеральном законе «О национальной платежной системе» от 27 июня 2011 г. № 161-ФЗ. Здесь ими называются «денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. При этом не являются электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность, деятельность по организации привлечения инвестиций и (или) деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами и осуществляющими учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций»[1].

В памятке Банка России «Об электронных денежных средствах» они определяются как «безналичные денежные средства в рублях или иностранной валюте, учитываемые кредитными организациями без открытия банковского счета и переводимые с использованием электронных средств платежа в соответствии с Федеральным законом № 161-ФЗ»[2].

Таким образом, в документах, регулирующих банковскую деятельность, внимание сосредоточено на следующих характеристиках электронных денег:

1) хранятся на технических устройствах в виде записи;

---

[1] О национальной платежной системе: федер закон от 27 июня 2011 г. № 161-ФЗ. URL: www.consultant.ru. (дата обращения: 02.02.2021).

[2] Об электронных денежных средствах: памятка Банка России. URL: https://base.garant.ru/70576142/53f89421bbdaf741eb2d1ecc4ddb4c33 (дата обращения: 03.04.2020).

2) для распоряжения ими необходимо собственно устройство и Интернет;

3) используются для осуществления платежей иным, нежели эмитент, компаниям;

4) не требуют доступа к депозитным счетам.

В отечественной экономической науке под электронными деньгами сначала понимали новые средства расчетов, основанные на использовании электронно-вычислительных машин (ЭВМ). Одним из первых, кто применил термин «электронные деньги», был В. М. Усоскин. В труде «Теории денег» он определяет их как «записи в памяти банковских компьютеров, передаваемые по каналам дистанционной связи»[1] и отождествляет с деньгами депозитными.

М. Г. Назаров, Ю. В. Пашкус, А. Н. Шаров связывают термин «электронные деньги» с банковскими картами, что в корне неверно, поскольку «банковская карта является инструментом доступа к счету, на котором находятся денежные средства клиента или предоставляемые в качестве кредита. Электронные же деньги содержат запись не о счете, а запись определенной денежной стоимости. Другими словами, банковскую карточку можно условно рассматривать как безналичные деньги (потому что она предполагает наличие банковского счета), а электронные деньги рассматриваются как заменитель наличности (хранится денежная стоимость)»[2].

Безусловно, электронные и безналичные деньги имеют общие свойства: 1) и те, и другие являются виртуальными деньгами; 2) они могут выступать формой безналичных расчетов. Однако, как утверждает С. Овсейко, электронные деньги не есть безналичные, поскольку первые содержатся в электронном кошельке, а вторые – на банковском счете; при расчете первыми происходят операции между кредитором и должником, а при расчете вторыми – между банком должника и кредитором[3]. Такого же мнения придерживается и Ю. С. Бегма: «Электронные деньги, являясь виртуальными, как безналичные деньги, с одной стороны, но не привязанными к банковским депозитным счетам, т. е. автономными средствами платежа, как бу-

[1] Усоскин В. М. Теории денег. М.: Мысль, 1976. С. 86.

[2] Электронные деньги. URL: http://www.incore.me/informacionnyye-texnologii/elektronnye-dengi/ (дата обращения: 03.04.2021).

[3] См.: Овсейко С. Юридическая природа электронных денег // Юрист. 2007. № 9. С. 30–37.

мажные деньги – с другой, естественно, образуют качественно новую ипостась денежных средств. В этом плане вполне оправданным (хотя и достаточно радикальным) выглядит предложение рассматривать электронные деньги в качестве „новой, особой формы денег“, порождаемой условиями современной постиндустриальной экономики»[1]. Однако далее автор отмечает: «В рамках сегодняшней экономической теории электронные деньги – безусловно, суррогат денег, являющийся долговым обязательством эмитента, какого-либо участника платежной системы. И усилия центрального регулятора – Центрального банка РФ – направлены только на то, чтобы максимально усилить контроль над объемом эмиссии. Борьба за признание их „особыми“ деньгами (наличными, с одной стороны, по функциональным характеристикам, и одновременно безналичными – с другой, по форме носителя) мало что меняет в оценке их природы. Это не деньги в трактовке классической теории. Но в рамках той же самой общепринятой концепции и банковские кредитные деньги, и бумажные деньги, эмитируемые государством (тем же самым Центральным банком), также являются суррогатами денег, поскольку не имеют товарной стоимости, выступая в качестве долговых обязательств эмитента, в том числе и государства. Поэтому можно с полным правом говорить, что все обращающиеся денежные средства в современном государстве – это не деньги, это – суррогаты истинных денег, имеющих реальную товарную стоимость, и потому выступающие в качестве эквивалентного измерителя, средства расчета и средства накопления»[2].

Н. Н. Парасоцкая и М. А. Архипова подчеркивают, что электронные деньги правильнее всего сравнивать с наличными деньгами, а не с безналичными, поскольку «при обращении безналичных денег известны реквизиты обеих сторон, а когда расчеты производятся электронными деньгами, то достаточно знать лишь реквизиты получателя»[3]. Данная характеристика – отсутствие идентификации пользователя при переводе электронных денег или оплате ими – при-

[1] Бегма Ю. С. «Электронные деньги – деньги?». Еще раз к вопросу об интерпретации электронных денег // Вестник РГГУ. Серия «Экономика. Управление. Право». 2013. № 15 (116). С. 202.

[2] Там же. С. 204.

[3] Парасоцкая Н. Н., Архипова М. А. Электронные деньги: проблемы и перспективы // Бухгалтерский учет в бюджетных и некоммерческих организациях. 2014. № 14 (350). С. 38–42.

знается их главной особенностью. Однако, несмотря на это, оборот таких денег регламентируется положениями Центробанка и электронной системы платежей, через которую проходит транзакция[1].

Н. В. Олиндер оперирует понятием «электронная наличность» – «запись, юридически свидетельствующая о взаимных денежных обязательствах субъектов платежных систем»[2].

По мнению М. П. Березиной, «электронные деньги есть электронный аналог наличных денег в виде файла, записанного на носитель – жесткий диск компьютера или смарт-карту»[3]. Часто их определяют как дематериализованную форму банковского билета, вид предоплаченного продукта, средство обмена, меру стоимости и в несколько ограниченной степени средство накопления и сбережения мировых денег[4].

С точки зрения М. С. Марамыгина, Е. Н. Прокофьевой, А. А. Марковой, под электронными денежными средствами надлежит понимать «средство платежа, эмитированное в национальной, иностранной или криптовалюте, хранящееся в виде записи на электронном носителе. В то же время электронные деньги – это обязательство эмитента, которое должно быть выполнено в традиционных деньгах»[5]. Как видим, здесь отмечено внутреннее противоречие электронных денег: с одной стороны, они являются средством платежа, с другой – обязательством эмитента, которое должно быть выполнено в традиционных неэлектронных деньгах. Это можно объяснить с помощью исторической аналогии: в свое время банкноты тоже рассматривались как обязательство, которое подлежит оплате монетами или драгоценными металлами[6].

---

[1] См.: Электронные деньги вчера, сегодня, завтра – их плюсы и минусы. URL: https://business-poisk.com/elektronnye-dengi.html#chto-takoe-elektronnye-dengi (дата обращения: 23.02.2021).

[2] Олиндер Н. В. Криминалистическая характеристика электронных платежных средств и систем // Lex Russica. 2015. № 10. Т. CVII. С. 135.

[3] Березина М. П. Деньги в современной интерпретации // Бизнес и банки. 2002. № 22. С. 1–8.

[4] См.: Электронные деньги. URL: http://www.incore.me/informacionnyye-texnologii/elektronnye-dengi/ (дата обращения: 03.04.2021).

[5] Марамыгин М. С., Прокофьева Е. Н., Маркова А. А. Сущность электронных денег, преимущества и недостатки // Вестник Омского университета. Серия «Экономика». 2016. № 1. С. 60–65.

[6] См.: Природа электронных денег. URL: https://vuzlit.ru/1241419/priroda_-elektronnyh_deneg (дата обращения: 09.04.2021)

Д. А. Кочергин определяет электронные деньги как новое средство платежа, которое позволяет потребителям совершать платежные операции без обязательного доступа к депозитным счетам и участия эмитента в переводе стоимости, и отмечает, что «в вопросе интерпретации электронных денег ключевыми являются три фактора: эмиссионный фактор (происходит ли в результате эмиссии электронных денег продажа пассивов эмитента); платежный фактор (является ли платеж электронными деньгами окончательным расчетом); фактор принимаемости (насколько широко принимаются электронные деньги в качестве платежа третьими лицами)»[1]. При этом «формально можно идентифицировать два основных элемента новизны, связанных с появлением электронных денег: во-первых, уникальный механизм совершения платежа, во-вторых, специфическое устройство систем электронных денег, позволяющее включать в свои рамки как денежные, так и неденежные системы. В действительности подлинная новизна электронных денег как финансового продукта лежит глубже. Она состоит не столько в „электронности“, сколько в „виртуальности“ электронных денег. В большинстве случаев электронные деньги являются виртуальным представлением „счетных денег“. Виртуальность электронных денег позволяет увидеть деньги платежа: счетную единицу, эмитированную в трехстороннем банковском платеже. На практике появление электронных денег позволяет овеществить денежный носитель, который фактически исчез в связи с широким использованием депозитных денег»[2].

Существует мнение, согласно которому электронные денежные средства вообще нельзя отождествлять с деньгами. Так, В. И. Иванов отмечает, что это есть информация, услуга или финансовый продукт[3]. Данную позицию разделяет и С. И. Шимон: «По форме они являются электронной информацией, которая сохраняется на специальном устройстве и может передаваться на другие устройства с помощью различных электронных средств передачи информации»[4]. Однако с приведенной точкой зрения вряд ли можно согла-

[1] Кочергин Д. А. Интерпретация электронных денег и оценка их влияния на денежно-кредитную систему // Финансы и кредит. 2005. № 13 (181). С. 31.

[2] Электронные деньги. URL: https://bstudy.net/963360/ekonomika/vvedenie (дата обращения: 23.02.2021).

[3] Цит. по: Абрамовский А. Электронные деньги – валюта будущего? URL: https://readli.net/elektronnyie-dengi-valyuta-budushchego/ (дата обращения: 23.02.2021).

[4] Там же.

ситься, поскольку электронные денежные средства подвержены инфляции и эмиссии и имеют в своей основе реальную денежную массу.

Еще одной ошибкой является отнесение к электронным деньгам предоплаченных одноцелевых карт (подарочных, топливных, телефонных и т. д.): «Использование такого платежного инструмента не означает осуществления нового платежа. Реальный платеж осуществляется в момент покупки или пополнения… карты. Ее использование не порождает новых денежных потоков и является простым обменом информацией о потребленных товарах или услугах»[1], – и криптовалюты. Эксперты отмечают, что «линия разделения между криптоактивами и электронными деньгами проходит по техническим и отчасти экономическим характеристикам»[2], в число которых входят:

– децентрализация: криптовалюты не имеют единого центра хранения и обработки, как, например, WebMoney;

– анонимность: при использовании криптовалют пользователи не обязаны подтверждать свою личность, неверифицированные клиенты платежных систем могут отправлять и получать деньги, но с рядом ограничений;

– прозрачность: блокчейн открыт для всех желающих, а данные о счете пользователя электронной платежной системы имеются у оператора;

– нерегулируемая стоимость и эмиссия: «стоимость и порядок выпуска электронных денег устанавливает их эмитент (государство, разработчики игры и т. д.). Криптовалюта выпускается по заранее установленным правилам, а ее стоимость в фиате зависит от спроса… Исключением из этого правила можно считать стейблкоины – криптоактивы, стоимость которых привязана к фиатной валюте в соотношении 1:1. Эмиссию стейблкоина определяет его эмитент, который готов обеспечить криптоактив реальными фиатными резервами»[3].

---

[1] Эмиссия электронных денег. URL: https://megalektsii-ru.turbopages.org (дата обращения: 03.04.2021).

[2] Электронные деньги и криптовалюты: в чем разница? URL: https://bits.media/pr/elektronnye-dengi-i--kriptovalyuy-v-chem-raznitsa/ (дата обращения: 13.07.2021).

[3] Там же.

Наконец, электронные денежные средства нужно отграничивать от так называемых «виртуальных» денег: бонусов, накопительных скидок, «валюты», использующейся в компьютерных играх, и т. д. – т. е. от того, что, по мнению Г. З. Гаспаряна, представляет собой набор маркетинговых средств, направленных на продвижение товаров, работ и услуг, в целях удовлетворения рыночных потребностей[1].

Таким образом, в результате анализа приведенных точек зрения попытаемся сформулировать собственное определение электронных денежных средств. Для этого будем использовать денотативную (предметную, описательную) дефиницию, где укажем родовое понятие и дифференцирующие признаки. В толковании мы намеренно уходим от словосочетаний типа «средство платежа», «средство оплаты», «платежный инструмент» и т. д., чтобы не возникало смешения терминов «электронные денежные средства» и «электронные средства платежа» (о них речь пойдет далее). В качестве родового понятия будем использовать классический оборот «средство обращения, сохранения и измерения стоимости», восходящий к «Капиталу» К. Маркса[2]. Итак, *электронные денежные средства – средство обращения, сохранения и измерения стоимости, эксплицированное в форме записи в специализированных электронных системах, имеющее в своей основе реальную денежную массу, но не требующее использования при транзакции банковских счетов, при переводе которого или оплате которым нет идентификации пользователя, принимающееся как средство платежа иными, нежели эмитент, организациями.*

Председатель Ассоциации «Электронные деньги», объединяющей крупнейших российских операторов электронных платежей (WebMoney, QIWI и др.), В. Л. Достов называет электронные денежные средства инструментом оптимизации платежного оборота[3]. Дей-

[1] См.: Гаспарян Г. З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: дис. … канд. юрид. наук. М., 2020. С. 33.

[2] См.: Маркс К. Капитал. Т. 1. Критика политической экономии. Кн. 1. Процесс производства капитала / пер. И. И. Степанова-Скворцова. М.: Гос. изд-во полит. лит., 1952. 797 с.

[3] См.: Достов В. Л. Электронные деньги как инструмент оптимизации денежного оборота // Деньги и кредит. 2013. № 12. С. 7–13.

ствительно, по сравнению с наличными они имеют ряд бесспорных преимуществ:

– отсутствие необходимости выплаты сдачи при проведении платежа;

– высокая портативность: величина суммы вовсе не связана с большими размерами денег;

– низкая стоимость выпуска: не нужно изготавливать банкноты, чеканить монеты и т. д.;

– отсутствие необходимости физически пересчитывать деньги (эту функцию может выполнять инструмент хранения или же платежный инструмент);

– фиксация момента платежа электронными системами;

– идеальная сохраняемость: электронные деньги идеально сохраняются с течением времени, т. е. не теряют своих качеств;

– качественная однородность: ни один из экземпляров электронных денег не обладает какими-либо уникальными свойствами[1].

Л. Г. Ибрагимова среди безусловных достоинств электронных денег называет: быстроту и удобство использования, большую безопасность, меньшие транзакционные сборы, новые возможности для бизнеса с переносом экономической активности в Интернет[2].

П. В. Ревенков к числу преимуществ электронных денег относит: удобство для пользователей, интернет-магазинов и провайдеров (к системе электронных денег подключиться проще, чем обеспечить эквайринг), низкую стоимость эмиссии, доступность для небольших интернет-магазинов, конкурентоспособность, низкий уровень риска в связи с отсутствием транспортировки, адаптированность к удаленному характеру расчетов[3].

---

[1] См.: Марамыгин М. С., Прокофьева Е. Н., Маркова А. А. Сущность электронных денег, преимущества и недостатки. С. 62; Электронные деньги – преимущества и недостатки. URL: https://profinvestment.com/money-elektronnye/ (дата обращения: 09.04.2021).

[2] См.: Ибрагимова Л. Г. Проблемы внедрения электронных денег в денежных оборот Российской Федерации // Бизнес в законе. 2012. № 5. С. 90.

[3] См.: Ревенков П. В. Электронные деньги: международный опыт регулирования в области ПОД/ФТ. URL: http://lexandbusiness.ru/view-article.php?id=3910 (дата обращения: 09.04.2021).

Важно подчеркнуть, что у электронных денег имеется и ряд недостатков:

– отсутствует устоявшееся правовое регулирование, многие государства до настоящего времени не определили своего однозначного отношения к электронным деньгам;

– при физическом уничтожении носителя электронных денег владельцу невозможно будет восстановить их денежную стоимость;

– отсутствие узнаваемости;

– невозможно прямо передать часть денег от одного плательщика другому;

– возможны их хищения с помощью новейших методов[1].

Сегодня электронные деньги классифицируют по разным основаниям:

1) способу обращения:

– на базе смарт-карт – многоцелевых пластиковых карт с встроенными чипами, куда записан денежный файл. С. А. Мусалаева пишет: «Режим ведения лицевого счета смарт-карты отличается от режима ведения лицевого счета традиционных карт. Обычная карта сама по себе не содержит информации о состоянии счета, она лишь является инструментом доступа к расчетному счету. В момент зачисления банком денежных средств на карточный счет, к которому привязана обычная платежная карта, на саму банковскую карту никакого зачисления не производится. В момент пополнения средств смарт-карты остаток на лицевом счете уменьшается на сумму, на которую было произведено пополнение карты. На карте появляется электронная наличность, в результате чего и становится возможной и безопасной (с точки зрения возникновения овердрафта по счету) авторизация операций в режиме офлайн»[2];

– на основе сетей: деньги, функционирующие на основе программной системы – программы или сетевого ресурса (QIWI, Web-

[1] См.: Титова О. К. Значение электронных денег на современном этапе развития. URL: rep.polessu.by›bitstream/123456789/2760/1/171.pdf (дата обращения: 09.04.2021).

[2] Мусалаева С. А. Электронные деньги и платежные системы // Проблемы современной экономики. 2010. № 4 (36). С. 206.

Money, ЮMoney). Данный вид электронных денег имеет шифрование и электронную цифровую подпись[1];

– на базе виртуальных бумажников (выделяют не все исследователи), «размещенных на сервере эмитента, доступ к которому предоставляется посредством ввода персонального кода дистанционно. В таких системах для перевода стоимости держателю электронных денег требуется получить дистанционный доступ к серверу, и только после этого с помощью программно-аппаратных средств эмитента может осуществляться перевод электронных денег по коммуникационным сетям, таким как Интернет и др.»[2].

2) государственному влиянию, оказываемому на деньги:

– фиатные (деньги центрального банка), номинированные в национальной валюте;

– нефиатные (частные), номинированные в иных счетных единицах;

3) эмитенту:

– эмитируемые кредитным институтом – банковские формы электронных денег;

– эмитируемые некредитным институтом – частные формы электронных денег.

Скажем несколько слов про ввод и вывод средств со счета. Они могут быть осуществлены различными способами в зависимости от возможностей системы электронных денег. Первый чаще всего реализуется путем покупки и инициирования карты экспресс-оплаты (в отдельных платежных системах, например Rapida, карта может быть инициирована в виде электронного кошелька или использована для пополнения существующего электронного кошелька); внесения наличных с помощью автоматов приема наличных, оплаты в кассах торговых точек или пунктов приема наличных платежей; банковского перевода на расчетный счет оператора электронных денег; оплаты платежной или кредитной картой (через телебанк, банкоматы, сервисы, предоставляемые непосредственно платежной системой, внешние сервисы); конвертации средств из другого опе-

[1] См.: Электронные деньги и виды платежных систем – какую выбрать? URL: https://ezaym-info.turbopages.org/turbo/ezaym.info/s/wiki/vidy-elektronnyh-deneg (дата обращения: 09.04.2021).

[2] Кочергин Д. А. Интерпретация электронных денег и оценка их влияния на денежно-кредитную систему. С. 32.

ратора электронных денег. Вывод средств представлен такими способами, как получение наличных в кассе оператора системы или пункте выдачи наличных средств; почтовый перевод на имя, указанное владельцем электронного кошелька, банковский перевод на счет; пополнение счета кредитной карты электронными деньгами; конвертация в электронные деньги других операторов.

Электронные денежные средства необходимо отличать от электронных средств платежа, под которыми в соответствии с Федеральным законом «О национальной платежной системе» нужно понимать «средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать в распоряжение в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств»[1]. Иными словами, электронное средство платежа – это новая технология, с помощью которой можно оплачивать товары и услуги без использования наличных денег.

В настоящее время наиболее распространенными электронными средствами платежа являются банковские карты. Их принято делить на три вида:

– кредитные – карты, позволяющие совершать платежные операции за счет средств банка в пределах лимита, установленного в договоре;

– дебетовые – карты, с помощью которых совершаются платежные операции за счет собственных средств. Обычно на них перечисляют заработную плату, переводят деньги, их пополняют наличными и т. д. К дебетовой карте можно подключить овердрафт – функцию, которая позволяет по окончании собственных средств использовать средства банка;

– предоплаченные – карты, предусматривающие использование заранее внесенных на них средств. Этот пластик может выпускаться не только банками, но и магазинами, автозаправочными станциями, косметическими компаниями и т. д.

Кроме того, исходя из способов записи информации, различают магнитные пластиковые карты и чиповые карты (смарт-карты).

[1] О национальной платежной системе: федер закон от 27 июня 2011 г. № 161-ФЗ. URL: www.consultant.ru (дата обращения: 02.02.2021).

Первые представляют собой простые карты с фиксированной покупательной способностью. На их лицевой стороне имеется индекс изготовителя с фирменным знаком, имя владельца, его идентификационный код, на оборотной стороне – магнитная полоса и подпись владельца. Вторые отличаются встроенным микропроцессором, который содержит оперативную (для использования при обработке) и постоянную (для хранения неизменной информации) память с системой безопасности данных[1].

Еще одним распространенным электронным средством платежа являются электронные кошельки. Обычно под ними понимают «компьютерную программу, позволяющую хранить электронные деньги, а также производить с их помощью безналичные расчеты в сети Интернет»[2]. Н. В. Олиндер определяет электронный кошелек как «специальную программу (кипер), которая необходима для учета и управления электронной наличностью, как правило, представляет собой сложный код, отражающий состояние денег в системах»[3]. Электронный кошелек похож на обычный: деньги в него можно положить, отсюда взять, перевести, в случае необходимости трансформировать их в реальные. Однако важно подчеркнуть, что первый имеет свой личный идентификационный номер.

Сегодня в России и странах Содружества Независимых Государств особой популярностью пользуются QIWI кошелек, ЮMoney кошелек, WebMoney кошелек и PayPal кошелек. Каждый из них обладает рядом достоинств, главные из которых – быстрота создания (быстрее, чем открыть счет в банке или получить карту); низкая комиссия, взимаемая платежными системами; простота использования; возможность открытия мультивалютного кошелька; высокая скорость исполнения операций. Ранее в этом перечне мы указали бы возможность анонимного пополнения, однако с 3 августа 2020 г. в нашей

[1] См.: Алиев А. Т. Деньги. Кредит. Банки: учеб. пособие. URL: https://thelib.ru/books/adik_tagirovich_aliev/dengi_kredit_banki_uchebnoe-posobie-read-2.html (дата обращения: 19.05.2021).

[2] Электронный кошелек. URL: https://www.banki.ru/wikibank/elektronnyiy-koshelek/ (дата обращения: 13.07.2021).

[3] Олиндер Н. В. Криминалистическая характеристика электронных платежных средств и систем. С. 131.

стране для внесения наличных пользователю необходимо идентифицироваться и привязать к электронному кошельку банковский счет[1].

Говоря об электронных кошельках, уделим внимание вопросу обеспечения их безопасности. Безусловно, ее уровень во многом зависит от платежных систем и их клиентов. Первые проводят все операции «через защищенный протокол HTTPS, который поддерживает шифрование, поэтому передаваемые через него данные не могут быть перехвачены мошенниками. Некоторые платежные организации предлагают своим пользователям двухфакторную авторизацию, способную свести к минимуму вероятность взлома… Сотрудники электронных платежных систем регулярно проводят мониторинг сети, отслеживая мошеннические действия и сомнительные ресурсы, после чего их деятельность пресекается. Еще одним методом защиты является автоматический анализ паттерна поведения пользователя. Иными словами, специальный робот следит за тем, какие суммы денег пользователь списывает со своего счета, и проверяет, не напоминает ли это характер поведения мошенников»[2]. Клиентам же платежных систем эксперты рекомендуют соблюдать простые правила: устанавливать только лицензионное программное обеспечение и антивирусы, создавать для кошельков сложные пароли и не сообщать их третьим лицам, всегда поверять в строке браузера правильность написания сайта платежной системы.

В завершение параграфа сделаем два основных вывода:

1) при формулировании определения электронных денежных средств мы полагаемся на мнения экономистов и понимаем под ними (в отличие от юристов, считающих, что электронные денежные средства – это обязательство) средство обращения, сохранения и измерения стоимости, эксплицированное в форме записи в специализированных электронных системах, имеющее в своей основе реальную денежную массу, но не требующее использования при транзакции банковских счетов, при переводе которого или оплате

[1] См.: О внесении изменений в Федеральный закон «О национальной платежной системе» и отдельные законодательные акты Российской Федерации: федер. закон от 3 июля 2019 г. № 173-ФЗ // Рос. газ. 2019. № 145 (7903).

[2] Трегубова Е. И хочется, и колется. Насколько безопасны электронные кошельки? URL: https://aif.ru/money/mymoney/42997 (дата обращения: 14.07.2021).

которым нет идентификации пользователя, принимающееся как средство платежа иными, нежели эмитент, организациями;

2) электронные денежные средства и электронные средства платежа суть не одно и то же. Последние являются технологией, позволяющей оплачивать товары и услуги без использования наличных денег, и представлены сегодня преимущественно банковскими картами и электронными кошельками.

1.2. Типовые модели механизмов хищений электронных денежных средств

Механизм преступления является важнейшим компонентом общественно опасного деяния, поскольку имеет существенное значение для понимания «закономерностей процесса подготовки, совершения и сокрытия преступления, системного движения и преобразования действий преступника и иных лиц»[1].

Одним из первых механизм преступления как составную часть предмета криминалистики определил А. Н. Васильев. По его мнению, так необходимо называть «процесс совершения преступления, в том числе его способ и все действия преступника, сопровождающиеся образованием следов (материальных и интеллектуальных), которые могут быть использованы для раскрытия и расследования преступления»[2].

С точки зрения Р. С. Белкина, механизм преступления представляет собой сложную динамическую систему, включающую субъект преступления, его отношение к своим действиям, последствиям, соучастникам; предмет посягательства; способ совершения и сокрытия преступления; преступный результат; обстановку преступления, поведение и действия лиц, оказавшихся участниками события, и др.[3]

Механизм преступления формируется и функционирует под воздействием некоторых закономерностей. В. А. Образцов относил к их числу:

---

[1] Баринов С. В. Типовые механизмы преступных нарушений неприкосновенности частной жизни // Вестник удмуртского университета. 2019. Т. 29. Вып. 5. С. 639.

[2] Криминалистика / под ред. А. Н. Васильева. М.: Изд-во Московского ун-та, 1971. С. 8

[3] См.: Белкин Р. С. Криминалистика. Краткая энциклопедия. М.: Большая российская энциклопедия, 1993. С. 41.

– возникновение и развитие связей и отношений внутри механизма преступления;

– формирование и реализацию способа преступления;

– возникновение и течение «…связанных с преступлениями явлений до и после криминального порядка, имеющих значение для следственной, судебной, оперативно-розыскной и экспертной практики»[1].

Аналогичного мнения придерживался и А. М. Кустов: «Криминалистическая концепция механизма преступления… связана с фундаментальными положениями криминалистики, и прежде всего – с закономерностями:

– возникновения и развития связей и отношений в содержании преступной деятельности субъекта преступления;

– формирования и реализации способов подготовки, совершения и сокрытия преступления;

– возникновения и течения связанных с преступлением явлений до и после криминального события (имеющих значение для установления истины по делу);

– образования криминалистически значимой информации о преступлении и его участниках, которая используется для раскрытия и расследования преступлений»[2].

Д. В. Ким понимает под механизмом преступления «взаимодействующую систему элементов криминалистической характеристики преступлений, отражающую процесс подготовки, совершения и сокрытия преступления, приводящую к образованию следов, имеющих значение для решения задач уголовного судопроизводства»[3].

Е. В. Иванова подчеркивает, что механизм преступления представляет собой общую категорию, которая характеризует деятельность всех лиц, вовлеченных в преступное событие, обусловливает процесс следообразования, но при этом не затрагивает таких спе-

[1] Образцов В. А. О некоторых перспективах интеграции и дифференциации знаний в криминалистике // Актуальные проблемы советской криминалистики. М.: Изд-во Всесоюзного ин-та по изучению причин и разработке мер предупреждения преступности, 1979. С. 20.

[2] Кустов А. М. Криминалистическая концепция механизма преступления // Вестник МФЮА. 2016. № 2. С. 165.

[3] Ким Д. В. Проблемы теории и практики разрешения криминалистических ситуаций в процессе раскрытия, предварительного расследования и судебного рассмотрения уголовных дел: дис. … д-ра юрид. наук. Барнаул, 2009. С. 106.

цифических видов деятельности, как подготовка к преступлению и его сокрытие[1].

По мнению В. В. Коломинова, «механизм преступления, являясь структурным элементом криминалистической характеристики того или иного вида преступлений, имеет важное значение для понимания закономерностей процесса совершения преступления, обусловленного разнообразными факторами криминальной ситуации»[2]. Далее автор указывает два основных свойства механизма преступления: первое отражает системность, взаимосвязь и взаимодействие абсолютно всех его элементов; второе – динамичность[3].

В свою очередь, С. А. Копыткин отмечает, что «…основным отличием между категориями „механизм преступления“ и „криминалистическая характеристика преступления“ является отличие функциональное… „механизм преступления служит средством познания преступного события“, и именно его анализ является целью как для ученых-криминалистов, так и для практиков… криминалистическая характеристика преступления… сочетая в себе свойства системы и научной абстракции, выполняет функцию информационной модели, применяемой для решения непосредственных задач, возникающих в процессе раскрытия, расследования и предупреждения конкретной группы преступлений, формируя таким образом эмпирический базис для частных методик расследования… К другому ключевому различию можно отнести особенности формирования содержания исследуемых категорий. Если в рамках криминалистической характеристики мы имеем дело в большинстве случаев с типизированными данными, то механизм совершения преступления формируется в рамках познания объектов, процессов, явлений и обстоятельств конкретного преступного события… Механизм преступления… представляется…

[1] Иванова Е. В. Типичные механизмы преступлений, связанных с опасными для здоровья веществами // Научные ведомости Белгородского государственного университета. Серия: Философия. Социология. Право. 2012. № 20 (139). Вып. 22. С. 207.

[2] Коломинов В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Краснодар, 2017. С. 55.

[3] Там же. С. 57

теоретической категорией, способствующей практическому анализу любого преступного события»[1].

Особую роль в определении понятия «механизм преступления» необходимо отвести работам А. В. Самойлова. С его точки зрения, так надлежит именовать «комплекс взаимосвязанных элементов и динамически сменяющихся этапов специфической деятельности человека, в результате которой через совершение преступления предполагается достижение конкретной, поставленной субъектом перед собой цели»[2]. При этом автор выделяет уровни (общий механизм преступления – механизм преступления как явления; родовой – механизм преступлений, посягающих на однородный объект; видовой – механизм преступления, посягающего на определенную сферу общественных отношений) и элементы механизма преступления как статичного явления (субъект преступления, объект преступного посягательства, явления, способствующие и препятствующие преступнику в достижении его целей, результат преступной деятельности, связи и отношения между данными элементами), а также этапы преступления как динамичного явления, которые, в свою очередь, группируются в следующие комплексы:

«I. „Идеальный“ комплекс:

– предпосылки зарождения преступной идеи (жизненная ситуация; личностные качества субъекта и т. п.);

– зарождение преступного замысла (формирование убеждения, что преступление – единственно возможный или оптимальный путь для достижения цели; неотторжение (принятие) цели вместе с преступным путем ее достижения).

II. „Материальный“ комплекс:

– планирование преступных действий;

– реализация преступного замысла;

– финишная ситуация (наступление преступного результата или пресечение преступной деятельности);

---

[1] Копыткин С. А. О соотношении категорий «криминалистическая характеристика преступления» и «механизм преступления» // Вестник Самарского юридического института. 2010. № 2 (2). С. 78–79.

[2] Самойлов А. В. Понятие механизма совершения преступления как научной категории криминалистики. URL: http://www.rusnauka.com/16_PN_2016/Pravo/11_211242.doc.htm (дата обращения 28.07.2021).

– посткриминальная ситуация – действия преступника по сокрытию следов преступления и результатов преступной деятельности (если они были достигнуты)»[1].

Таким образом, механизм преступления есть категория познания преступного события, отражающая закономерные связи между отдельными этапами, факторами, обстоятельствами преступления и позволяющая создать его картину. При этом в криминалистический механизм преступления в качестве элементов входят только те обстоятельства, которые, взаимодействуя друг с другом, обусловливают развитие криминальной ситуации[2]. «Преступная деятельность, составляющая основное содержание расследуемого события, …представляет систему, элементы которой находятся во взаимосвязи, в силу чего каждый из них несет определенную информацию о других… В зависимости от характера существующей между элементами расследуемого события объективной связи могут быть построены категорические или вероятностные суждения о тех или иных свойствах личности субъекта или обстоятельствах… события»[3].

Расследование преступления предполагает моделирование его механизма, что, по словам Л. Н. Викторовой, необходимо для определения круга лиц, причастных к совершению уголовно наказуемого деяния, очевидцев и лиц, владеющих информацией о событии преступления, раскрытия связей между отдельными обстоятельствами, уточнения временных параметров совершения преступления[4].

Т. С. Волчецкая подчеркивает, что в следственной практике моделирование эффективно и целесообразно только в ряде случаев:

«1) когда объект познания существовал в прошлом и его уже нет на момент исследования (например, преступное событие, криминальные ситуации);

---

[1] Самойлов А. В. Понятие механизма совершения преступления как научной категории криминалистики. URL: http://www.rusnauka.com/16_PN_2016/Pravo/11_211242.doc.htm (дата обращения 28.07.2021).

[2] См.: Моделирование механизма совершения преступления. URL: https://sci-center/online/kniga-kriminalistika-scicenter/modelirovanie-mehanizma-soversheniya.html (дата обращения: 28.07.2021).

[3] Типовые модели и алгоритмы криминалистического исследования: учеб. пособие / под ред. В. Я. Колдина. М.: Изд-во Московского ун-та, 1989. С. 29.

[4] См.: Викторова Л. Н. Фактор времени и его значение для раскрытия и расследования преступлений: учеб. пособие. М.: Изд-во ВНИИ МВД СССР, 1983. С. 12.

2) когда объект познания еще только будет существовать в будущем (возможная следственная ситуация в ходе предстоящего допроса, моделируемая в процессе подготовки к нему);

3) когда объект существует реально на момент исследования, однако он либо чрезмерно сложен, либо вовсе не доступен для познания;

4) в тех случаях, когда познаваемый процесс протекает или слишком быстро, или же, наоборот, слишком медленно (отдельные виды следственных экспериментов)»[1].

Т. С. Волчецкая выделяет такие классы криминалистических моделей, как:

– материальные (используются в следственной практике главным образом при производстве следственных действий и экспертиз);

– мысленные или идеальные, умозрительные;

– логико-математические и кибернетические;

– информационно-компьютерные[2].

Исходя из предложенной классификации, применительно к хищениям электронных денежных средств в первую очередь нужно вести речь о мысленной и информационно-компьютерной моделях. Первая помогает преодолеть информационную неопределенность, существующую на первоначальном этапе расследования. При этом, по справедливому замечанию А. М. Кустова, создание мысленной модели совершенного преступления не есть механическое копирование преступного события и его механизма, а избирательный процесс, в ходе которого, зная закономерности познаваемого явления, субъект получает представление о свойствах и качествах, подлежащих выявлению в ходе расследования[3]. Вторая – повысить качество информационно-аналитической деятельности следователя, в том числе по планированию расследования преступления[4].

---

[1] Волчецкая Т. С. Современные проблемы моделирования в криминалистике и следственной практике: учеб. пособие. Калининград: Калининградский гос. ун-т, 1997. С. 11.

[2] Там же. С. 13.

[3] См.: Кустов А. М. Криминалистика и механизм преступления. Цикл лекций: учеб.-метод. пособие. М.: Московский псих.-социал. ун-т; Воронеж: МОДЕК, 2002. С. 254–255.

[4] См.: Ковалев С. А., Смагоринский Б. П. Использование криминалистического компьютерного моделирования при планировании расследования преступлений //

Итак, моделирование механизма преступления призвано решать комплекс задач:

– определять обстоятельства преступления;

– устанавливать круг лиц, причастных к его совершению;

– выявлять причины и условия, способствующие совершению уголовно наказуемого деяния;

– формировать мероприятия по предупреждению преступлений[1].

Сосредоточим свое внимание на преступлении как динамичном явлении и способе его совершения как элементе механизма преступного деяния, под которым А. В. Самойлов понимает «взаимосвязанную систему поведенческих актов субъекта, обусловленных объективными и субъективными факторами, направленную на достижение поставленной цели через подготовку, совершение и сокрытие преступления»[2].

Исходя из содержания ст. 158, 159.3 и 159.6 Уголовного кодекса Российской Федерации, можно говорить о том, что хищения электронных денежных средств совершаются тайно (кража), т. е. в отсутствие собственника или иного владельца имущества, или посторонних лиц либо незаметно для них, а также посредством обмана и злоупотребления доверием (мошенничество). При этом, по статистическим данным Генеральной прокуратуры Российской Федерации, мошенничество встречается наиболее часто[3]. Для совершения кражи, как правило, используются вредоносное программное обеспечение и программы удаленного доступа, которые наряду с приемами социальной инженерии применяют и мошенники. Устанавливая механизм совершения хищений электронных денежных средств в его

Юридическая наука и правоохранительная практика. 2013. № 4 (26). С. 111–123; Ковалев С. А. Использование метода криминалистического компьютерного моделирования в расследовании преступлений // Российский следователь. 2021. № 4. С. 35–37.

[1] См.: Глоссарий по информационному обществу / под ред. Ю. Е. Хохлова. М.: Ин-т развития информационного общества, 2009. С. 79.

[2] Самойлов А. В. Понятие способа совершение преступления и его роль в механизме совершения преступления. URL: jurnal.org/articles/2010/uri64.html (дата обращения: 28.07.2021).

[3] В 2020 г. в России каждое второе киберпреступление было мошенничеством. См.: Состояние преступности в России за январь–декабрь 2020 г. URL: genproc.gov.ru›upload/iblock/aab…декабрь2020.pdf (дата обращения: 20.06.2021).

целостной системе развивающегося в объективной действительности преступления с присущими ему закономерностями и зависимостью отдельных элементов друг от друга, отметим три относительно самостоятельных этапа:

1) начальный этап, характеризующийся формированием умысла со стороны субъекта преступления, подбором орудий и средств, места и времени совершения уголовно наказуемого деяния, поиском сообщников, если это необходимо для достижения преступной цели;

2) основной этап, на котором происходит непосредственное хищение электронных денежных средств;

3) завершающий этап, где наблюдаются окончание преступной деятельности, наступление преступного результата, сокрытие следов совершенного преступления[1].

Итак, выделим несколько типовых моделей хищений электронных денежных средств.

Модель 1. Тайное хищение электронных денежных средств, совершаемое при непосредственном контакте с устройством потерпевшего

Начальный этап характеризуется формированием преступного умысла, выбором места и времени совершения уголовно наказуемого деяния (когда устройство жертвы останется без присмотра), поиском лиц для обналичивания денежных средств. Из приговора № 1-1-25/2020 1-1-252/2019 от 28 января 2020 г. по делу № 1-1-25/2020 следует, что Л. 22 сентября 2018 г. около 03.00 находился в гостях у С. по адресу <…>, где, руководствуясь корыстным мотивом, направленным на противоправное и безвозмездное хищение чужого имущества, в целях неправомерного обогащения, решил совершить тайное хищение электронных денежных средств с электронного средства платежа NN платежного сервиса «Яндекс.Деньги», принадлежащего С. Для реализации своего преступного умысла Л. через социальную сеть <…> попросил разрешения М. воспользоваться банковской картой ПАО «Сбербанк России» NN, имеющей лицевой счет NN, принадлежащей последнему, для осуществления перевода денежных средств с электронного платежного сервиса «Яндекс.Деньги», принад-

[1] См.: Шишова Н. Е. Моделирование механизма преступлений, связанных с жестоким обращением с детьми // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2016. № 1. С. 119–124.

лежащих С., чтобы впоследствии обналичить их и распорядиться по своему усмотрению, о чем М. не был поставлен в известность. Во исполнение задуманного Л., находясь в комнате <…>, воспользовавшись тем, что С. уснул, достоверно зная, что к мобильному телефону марки «Samsung Galaxy J5», принадлежащему последнему, подключено приложение «Яндекс.Деньги» и пароль от него, взял указанный телефон, лежащий на столе в комнате, и покинул ее. Затем Л. проследовал к зданию ФГУП «Почта России», где встретился с М. и тот сообщил ему номер своей банковской карты ПАО «Сбербанк России»[1].

На основном этапе происходит совершение преступления (с помощью устройства жертвы похищаются денежные средства, принадлежащие ей).

На завершающем этапе злоумышленник скрывает следы преступления путем обналичивания денежных средств, их конвертации в криптовалюту, вывода через электронные кошельки, зарегистрированные на различных лиц, и т. д.).

Модель 2. Тайное хищение электронных денежных средств, совершаемое с использованием вредоносного программного обеспечения

Начальный этап характеризуется формированием умысла, подбором орудий и средств совершения преступления (созданием или приобретением вредоносного программного обеспечения, рассылкой спама или фишинговых писем, где может скрываться вирус), а также поиском лиц для обналичивания похищенных денег. Так, из материалов уголовного дела, возбужденного на территории Волгоградской области, следует, что Д, имея умысел на тайное хищение денег с электронных средств платежа граждан, в период не позднее 7 января 2017 г. по 13 января 2018 г. по информационно-телекоммуникационной сети Интернет за денежное вознаграждение неустановленному лицу, осуществлявшему создание, использование и распространение вредоносного программного обеспечения, предназначенного для несанкционированного копирования компьютерной информации и нейтрализации средств ее защиты с электронных

[1] См.: Приговор Собинского городского суда Владимирской области № 1-1-25/2020 1-1-252/2019 от 28 января 2020 г. по делу № 1-1-25/2020. URL: https://sudact.ru/regular/doc/WVxRhfsp0Hgn..._pos=3542#snippet (дата обращения: 28.07.2021).

устройств граждан, и неосведомленному о преступном умысле первого, неоднократно оплачивал доступ к ресурсам сети Интернет, расположенным по URL-адресам <…>, где размещались учетные данные <…>. Д. также установил на свой персональный компьютер специальное программное обеспечение, позволявшее подключиться к удаленному рабочему столу по протоколу безопасности RDP. При этом Д. в целях соблюдения полной анонимности в сети Интернет приобрел у хостинг-провайдеров во временное пользование выделенные виртуальные серверы, расположенные на территории Германии, Нидерландов и Российской Федерации, которые затрудняли установление местонахождения и идентификацию Д. Кроме того, Д. подыскал неустановленных лиц, готовых за денежное вознаграждение принимать на подконтрольные первому банковские счета похищаемые Д. денежные средства, обналичивать их в банковских терминалах, затем с помощью интернет-сервисов обмена электронной валюты конвертировать похищенные деньги в криптовалюту Bitcoin и переводить ее Д.[1]

Основной этап характеризуется непосредственным совершением преступления. В данном случае это могут быть взлом электронного кошелька с использованием вредоносного софта, похищение логина и пароля, подмена буфера обмена и т. д.

На завершающем этапе происходит сокрытие следов преступления (обналичивание похищенных денег, их конвертация в криптовалюту, вывод средств через несколько электронных кошельков, зарегистрированных на разных лиц, и т. д.).

Модель 3. Тайное хищение электронных денежных средств, совершаемое с помощью программ удаленного доступа

Специфической чертой данной модели является то, что в ней сочетаются тайное хищение и мошенничество (чтобы пользователь установил на свое устройство программу удаленного доступа, злоумышленники применяют приемы социальной инженерии). В целом начальному этапу присущи те же особенности, что и в предыдущем случае, только в качестве орудия здесь выступают программы удаленного доступа. Так, согласно материалам уголовного дела, возбужденного на территории Кабардино-Балкарской Республики, на ноутбуке потерпевшего экспертом не были обнаружены коды вредоносных программ,

[1] По данным ГУ МВД России по Волгоградской области.

однако найдены следы использования программы AnyDesk (дата создания <…>), предназначенной для удаленного управления устройством после получения цифрового кода, генерируемого программой, и следы наличия установки данного приложения от <…>, а также сообщения о переводе денежных средств через платежную систему QIWI[1].

Основной этап характеризуется совершением хищений электронных денежных средств (подбор логина и пароля или их кража, если они хранятся в файлах на устройстве, где была установлена программа удаленного доступа).

На завершающем этапе, как и в предыдущих случаях, происходит сокрытие следов преступления.

Модель 4. Хищение электронных денежных средств, совершаемое с использованием приемов социальной инженерии

На начальном этапе формируется преступный умысел, выбираются орудия и средства совершения преступления (создаются фейковые сайты, на торговых площадках размещаются фейковые объявления о продаже товаров, вакансиях и т. д.), в случае необходимости подыскиваются сообщники. По материалам уголовного дела, возбужденного на территории Кабардино-Балкарской Республики, в первой декаде сентября 2020 г. (более точные дата и время предварительным следствием не установлены) Л., находясь в г. Ростове-на-Дону, умышленно, из корыстных побуждений, желая материально обогатиться, вступил в предварительный преступный сговор с неустановленным лицом, направленный на хищение чужого имущества путем обмана группой лиц по предварительному сговору с распределением преступных ролей, согласно которому неустановленное лицо разместило на сайте «www.avito.ru» недостоверные сведения о продаже товаров, а затем убеждало граждан в необходимости внесения аванса перед покупкой на карты <…>, которые Л. подыскивал, затем обналичивал[2].

Основной этап характеризуется совершением хищения электронных денег, однако здесь это происходит при непосредственном контакте с потенциальным потерпевшем (его убеждают в необходимости перечисления денежных средств, запугивают, подогревают

[1] По данным МВД России по Кабардино-Балкарской Республике.
[2] По данным МВД России по Кабардино-Балкарской Республике.

его любопытство, в отдельных случаях ему могут угрожать и т. д.). Цель злоумышленников – усыпить бдительность жертвы и заставить ее перечислить деньги или сообщить конфиденциальную информацию, необходимую для доступа к электронному кошельку. Отметим интересный факт. Анализ уголовных дел и судебных решений позволил выявить следующую закономерность: мужчины, как правило, чаще по собственной воле переводят деньги незнакомым лицам, женщины охотнее предоставляют злоумышленникам свои личные данные, студенты становятся покупателями фейковых интернет-магазинов, пенсионеры передают конфиденциальную информацию.

Завершающий этап схож с предыдущими моделями.

Таким образом, с учетом способа совершения преступления как динамичного явления нами были выявлены четыре модели механизма хищений электронных денежных средств: тайное хищение электронных денежных средств, совершаемое при непосредственном контакте с устройством потерпевшего; тайное хищение электронных денежных средств, совершаемое с использованием вредоносного программного обеспечения; тайное хищение электронных денежных средств, совершаемое с помощью программ удаленного доступа; хищение электронных денежных средств, совершаемое с использованием приемов социальной инженерии.

В заключение заметим, что построение криминалистических моделей способствует правильной уголовно-правовой квалификации совершенного деяния; установлению событий, предшествующих, сопутствующих преступлению, и лиц, причастных к нему; определению целей и мотивов уголовно-наказуемого деяния; установлению связей между отдельными фактами и устранению противоречий между ними; определению направления поисково-познавательной деятельности следователя, формулированию общих и частных организационных, тактических и управленческих задач, а также методов и средств их решения.

1.3. Структура и содержание элементов криминалистической характеристики хищений электронных денежных средств

В числе базовых составляющих частных криминалистических методик традиционно называют криминалистическую характеристику преступлений, роль которой обычно сводят к использованию содержания криминалистически значимых элементов, а также взаимосвязей между ними в построении криминалистических (следственных) версий[1]. Л. А. Сергеев понимал под ней «особенности преступлений отдельных видов, имеющие значение для следственной практики и для разработки научных рекомендаций»[2]. В. П. Лавров – систему сведений о типичных признаках определенной категории преступлений, анализ которых позволяет сделать выводы об оптимальных путях их раскрытия и расследования[3].

По мнению Л. Я. Драпкина, В. Н. Карагодина, криминалистическая характеристика преступлений – это научная категория, где «с определенной степенью общности описаны типовые признаки и свойства события, обстановки, способа совершения общественно опасных деяний определенной классификационной группы, процесса образования и локализации следов, типологические качества личности и поведения виновных, потерпевших, устойчивые особенности иных объектов посягательства, а также связи и отношения между всеми перечисленными структурными элементами»[4].

С точки зрения Е. И. Зуева, Н. Г. Шурухнова, криминалистическая характеристика есть отражение системы криминалистических черт, свойств, признаков преступления, отобразившихся в объективной действительности, которая содержит данные о типичных способах совершения и сокрытия преступления, механизме преступного посягательства, следах, обстановке, в которой готовилось и происходило преступное событие, объекте и предмете преступного посяга-

[1] См.: Колесниченко А. Н., Коновалова В. Е. Криминалистическая характеристика преступлений. Харьков: Юрид. ин-т, 1985. С. 92.

[2] Сергеев Л. А. Криминалистика. М.: Изд-во МГУ, 1971. С. 425.

[3] См.: Лавров В. П. Криминалистика. М.: Норма, 1999. С. 33.

[4] Драпкин Л. Я., Карагодин В. Н. Криминалистика: учебник. 2-е изд., перераб. и доп. М.: Проспект, 2016. С. 349.

тельства, чертах личности преступника и потерпевшего, а также об обстоятельствах, способствовавших совершению преступлений[1].

На важную роль криминалистической характеристики преступлений обращают внимание и другие ученые. Так, А. Ф. Лубин определяет ее как «сущностное выводное знание о преступной деятельности», которое «выступает (наряду с техническими и организационными средствами) в качестве информационного средства расследования… это опережающие, предпосылочные сведения о закономерностях функционирования объекта (предмета), которые обусловливают закономерности расследования»[2]. А. Ю. Головин отмечает, что содержание криминалистической характеристики преступлений «позволяет более точно оценивать ситуации, возникающие на этапе предварительной проверки материалов, первоначальном и последующем этапах расследования преступлений, разрабатывать и выдвигать криминалистические версии, использовать более эффективные тактические приемы расследования»[3]. По мнению А. А. Бессонова, «по своей гносеологической природе криминалистическая характеристика преступлений является, во-первых, информационной основой формирования частных методик расследования (то есть категорией теоретического познания), а во-вторых, инструментом (средством) практического познания в процессе расследования. На ее основе должна строиться ретроспективная модель конкретного преступления, которая и есть продукт практического познания»[4]. Ю. В. Гаврилин полагает, что в условиях дефицита исходной информации на первоначальном этапе расследования криминалистическая характе-

[1] См.: Зуев Е. И., Шурухнов Н. Г. Криминалистическая характеристика преступлений // Криминалистика (актуальные проблемы). М.: Академия МВД СССР, 1988. С. 119.

[2] Лубин А. Ф. Механизм преступной деятельности. Н. Новгород: Нижегородский юрид. ин-т, 1997. С. 94.

[3] Головин А. Ю. К вопросу межэлементных связей в криминалистической характеристике преступления // Деятельность правоохранительных органов в современных условиях: сб. материалов междунар. науч.-практ. конф. Иркутск: ВСИ МВД России, 2018. С. 31–35.

[4] Бессонов А. А. Учение о криминалистической характеристике преступлений. URL: https://izron.ru/articles/problemy-i-perspektivy-razvitiya-sovremennoy-yurisprudentsii-sbornik-nauchnykh-trudov-po-itogam-mezh/sektsiya-7-ugolovnyy-protsess-kriminalistika-operativno-rozysknaya-deyatelnost-spetsialnost-12-00-09/uchenie-o-kriminalisticheskoypkharakteristike-prestupleniy/ (дата обращения: 14.07.2021).

ристика позволяет выдвигать обоснованные версии относительно неустановленных обстоятельств за счет устойчивых корреляционных связей между ее отдельными составляющими[1].

Элементы криминалистической характеристики преступлений образуют стройную систему, однако их перечень не является общепризнанным ни на уровне универсальной модели криминалистической характеристики преступлений, ни на уровне частных криминалистических методик. При этом, по мнению некоторых авторов, в криминалистическую характеристику преступления должно включаться наибольшее число признаков, имеющих криминалистическое значение[2].

Среди элементов криминалистической характеристики киберпреступлений, к которым относятся и хищения электронных денежных средств, А. А. Протасевич, Л. П. Зверянская называют способ свершения преступления, особенности следовой информации, особенности обстановки совершения преступления (место совершения преступления, время совершения преступления и др.), личностную характеристику преступника, особенности непосредственного предмета преступного посягательства[3].

По мнению В. В. Коломинова, в перечень элементов криминалистической характеристики мошенничеств в сфере компьютерной информации должны входить: «непосредственный объект преступного посягательства; способ совершения преступления; орудия и средства преступления; следы и механизм следообразования; обстановка совершения преступления, его пространственно-временной континуум, которые, в свою очередь, характеризуются корреляционной зависимостью между собой и специфичностью проявлений во внешней среде (киберпространстве)»[4].

---

[1] См.: Гаврилин Ю. В. Криминалистическая тактика и методика расследования отдельных видов преступлений в определениях и схемах: учеб. пособие. М.: Книжный мир, 2004. С. 125.

[2] См.: Колесниченко А. Н. Научные и правовые основы расследования отдельных видов преступлений: автореф. дис. … д-ра юрид. наук. Харьков, 1967. С. 7–9; Бахин В. П. Криминалистическая характеристика преступлений как элемент расследования // Вестник криминалистики. 2000. № 1. С. 16–22.

[3] См.: Протасевич А. А., Зверянская Л. П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С. 45–47.

[4] Коломинов В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа. С. 53–54.

Сразу сделаем оговорку. В нашем случае вопрос о месте совершения преступления вызывает множество дискуссий. Так, М. А. Степанова, Е. В. Царев пишут: «Если преступление совершается с использованием сети Интернет, то местом совершения преступления следует считать фактическое местонахождение лица, откуда он осуществлял общественно опасные деяния, непосредственно направленные на изъятие денежных средств»[1]. Иного мнения придерживаются, например, А. Забейда, Д. Данилов: «Местом совершения… преступления на основании п. 3 мотивировочной части постановления Конституционного Суда Российской Федерации от 16 октября 2012 г. № 22-П, – отмечают они, – следует считать место, где оно окончено – где был причинен ущерб потерпевшему. К нему сейчас суды относят место открытия счета потерпевшего или место ведения его электронного кошелька»[2]. Конец этому спору положил Пленум Верховного Суда Российской Федерации, внесший 29 июня 2021 г. изменения в постановление «О судебной практике по делам о мошенничестве, присвоении и растрате» от 30 ноября 2017 г.: «Местом окончания мошенничества, состоящего в хищении безналичных денежных средств, является место нахождения подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета»[3]. Наконец, есть третья позиция, согласно которой местом совершения хищений электронных денежных средств признается ноосфера, т. е. киберпространство[4], куда входят:

[1] Степанова М. А., Царев Е. В. Проблемы определения места совершения хищения денежных средств с использованием информационно-телекоммуникационных технологий // Вестник Белгородского юридического института МВД России. 2021. № 1. С. 14.

[2] Забейда А., Данилов Д. Исключить ст. 159.6 УК. Вопросы цифрового хищения в новом постановлении Пленума ВС о судебной практике по делам о мошенничестве. URL: https://www.advgazeta.ru/mneniya/isklyuchit-st-159-6-uk/ (дата обращения: 21.07.2021).

[3] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (с изм., внесенными постановлением Пленума от 29 июня 2021 г. № 22). URL: https://base.garant.ru/71823288 (дата обращения: 21.07.2021).

[4] См., например: Кургузкина Е. Б., Ратникова Н. Д. Место совершения компьютерных преступлений // Вестник Воронежского института ФСИН России. 2016. № 1. С. 79–87; Калентьева Т. А., Кузьмина А. О. Киберпространство как место совершения преступления // Актуальные проблемы правоведения. 2019. № 1 (61). С. 31–37.

«– отдельные помещения или их набор, в которых размещены автоматизированные информационно-вычислительные системы с соответствующим техническим комплексом обеспечения их деятельности (системы связи, электропитания, заземления и т. п.);

– средства автоматизированной обработки информации (вычислительные машины и их системы);

– каналы телекоммуникаций и передачи данных (в том числе звуковые волны и электромагнитные поля);

– машинные носители информации, обеспечивающие хранение информации в виде, пригодном для ее автоматизированной обработки;

– непосредственно сама информация, представленная в виде, пригодном для ее автоматизированной обработки (данные в соответствующих форматах, управляющие программы и т. п.);

– принятые порядок и последовательность (протоколы – по терминологии теории автоматизированных информационно-вычислительных систем) автоматизированной обработки информации, а также установленные правила и распределение обязанностей между должностными лицами автоматизированной информационной системы»[1].

Мы разделяем позицию Пленума Верховного Суда Российской Федерации и рассматриваем в качестве места хищения электронных денежных средств место, где был причинен ущерб потерпевшему, но не вносим его в перечень элементов криминалистической характеристики, в связи с тем что оно не образует информационной основы расследования данных преступлений.

А. И. Маилян отмечает, что «криминалистическая характеристика хищений, совершенных с банковского счета, в отношении электронных денежных средств и/или с помощью электронных средств платежа, включает следующие структурные элементы: особенности способов приготовления, совершения и сокрытия преступлений; особенности орудий и средств совершения преступлений (электронных платежных систем и средств и др.); особенности предмета преступного посягательства; особенности оставляемых следов; особенности личности лица, совершившего преступление, и потерпевшего»[2].

[1] Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. … д-ра юрид наук. Воронеж, 2001. С. 15–16.

[2] Маилян А. В. Общие положения криминалистической характеристики хищений, совершенных с банковского счета, в отношении электронных денежных

В приведенном перечне вызывает вопросы личность потерпевшего. «…На выбор злоумышленниками тех или иных способов совершения деяния, – пишет автор, – существенно влияют особенности личности потерпевшего, прежде всего, степень его виктимизации, наличие социально значимых отношений с субъектами преступлений и др.»[1]. Однако, как показывает практика, жертвой мошенников в сети Интернет может стать любой человек независимо от его пола, возраста, социального положения, манеры поведения и т. д.

По нашему мнению, в число элементов криминалистической характеристики хищений электронных денежных средств надлежит включить данные об объекте и предмете преступного посягательства, личности преступника, орудиях и средствах совершения преступления, способах подготовки, совершения и сокрытия преступления, особенностях механизма следообразования. Рассмотрим их содержание.

Для начала обратимся к объекту преступного посягательства. По мнению Е. С. Жулевой, В. К. Кулева, «общим объектом хищения электронных денег является круг общественных отношений, охраняемых Уголовным кодексом от преступного посягательства. Родовым объектом данного состава являются экономические отношения, видовым объектом выступают отношения собственности как родовое понятие по отношению ко всем формам собственности. Непосредственным объектом… денежные средства, бонусы, хранящиеся на счетах электронных кошельков пользователей сети Интернет»[2]. Поскольку общий объект позволяет нам отграничить преступное поведение от непреступного, но не дает возможности дифференцировать одно преступление от другого, т. е. квалифицировать, мы не будем останавливаться на нем подробно. Родовым объектом хищений электронных денежных средств выступают общественные отношения в сфере экономики – «совокупность общественных отношений в сфере производства, потребления, обмена и распределения продуктов, услуг и факторов производства, проявляющихся в отношениях собственности, отношениях организационно-экономического характера и отношениях по реализации экономиче-

средств и/или с помощью электронных средств платежа // Известия Тульского государственного университета. 2020. № 3. С. 125.

[1] Там же. С. 124.

[2] Жулева Е. С., Кулев В. К. Хищение электронных денег // Труды междунар. симпозиума «Надежность и качество», 2011. Т. 1. С. 177.

ских связей»[1]. Видовым объектом – правоотношения собственности. Непосредственным – электронные денежные средства. Бонусы, указанные Е. С. Жулевой, В. К. Кулевым, мы не рассматриваем в качестве непосредственного объекта, поскольку не относим их к электронным деньгам. Кроме того, вслед за Г. З. Гаспаряном[2] мы выделяем дополнительный объект – общественные отношения по обеспечению информационной безопасности, т. е. «состояния защищенности жизненно важных интересов личности, общества и государства в информационной сфере от информационных, программно-математических, физических и организационных угроз»[3]. Законодатель в качестве дополнительного объекта называет нарушение банковской тайны, что наряду с подготовительной работой, которая предшествует совершению преступления и может быть квалифицирована как приготовление к нему, и особенностями субъекта преступления (во-первых, он должен обладать специальными знаниями (хотя, на наш взгляд, это весьма спорно), во-вторых, его местоположением может быть любая точка мира) обусловливают высокую общественную опасность рассматриваемых преступлений. Все это нашло выражение в Федеральном законе «О внесении изменений в Уголовный кодекс Российской Федерации» от 23 апреля 2018 г. № 111-ФЗ, согласно которому ч. 3 ст. 158 «Кража» и ст. 159.6 «Мошенничество в сфере компьютерной информации» были дополнены новым квалифицирующим признаком. Кража с банковского счета, а равно электронных денежных средств независимо от размера была отнесена к категории тяжких преступлений, к которым кроме того относится, например, кража в крупном размере[4].

Большое криминалистическое значение имеют данные о предмете преступного посягательства в связи с тем, что позволяют следователю установить источник его получения, а также выявить возмож-

[1] Расторопова Д. С. К вопросу об определении родового и видового объекта преступления, предусмотренного ст. 185.6 УК РФ // Пробелы в российском законодательстве. 2018. № 6. С. 217.

[2] См.: Гаспарян Г. З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий. С. 26.

[3] Гаврилин Ю. В. Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы: моногр. Тула: Левша, 2009. С. 59.

[4] См.: О внесении изменений в Уголовный кодекс Российской Федерации: федер. закон от 23 апреля 2018 г. № 111-ФЗ. URL: https://base.garant.ru/71929752/ (дата обращения: 22.07.2021).

ных соучастников преступления. В нашем случае предмет преступного посягательства совпадает с непосредственным объектом и представляет собой электронные денежные средства. Однако отметим, что некоторое время назад суды Российской Федерации практически единогласно отмечали, что электронные деньги не могут рассматриваться в качестве предмета хищения, поскольку не являются вещью материального мира и не существуют в физически осязаемой форме. Таким образом, преступные посягательства в отношении электронных денежных средств квалифицировались по нормам о мошенничестве. В ноябре 2017 г. Пленум Верховного Суда Российской Федерации в постановлении № 48 указал, что «если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу положений пункта 1 примечаний к статье 158 УК РФ и статьи 128 Гражданского кодекса Российской Федерации содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб»[1], т. е. с этого времени электронные денежные средства были приравнены к наличным и стали рассматриваться в качестве предмета хищения чужого имущества.

Следующим важным элементом криминалистической характеристики преступлений является личность преступника, необходимость изучения которой продиктована не только задачами криминалистики, но и требованиями уголовно-процессуального законодательства[2].

Н. Т. Ведерников определяет криминалистическое изучение личности как выявление, анализ и оценку криминалистически значимой информации о преступнике, жертве преступления и других участниках

[1] О судебной практике по делам о мошенничестве, присвоении и растрате. URL: https://base.garant.ru/71823288 (дата обращения: 21.07.2021).

[2] Согласно ст. 73 Уголовно-процессуального кодекса Российской Федерации «при производстве по уголовному делу подлежат доказыванию... виновность лица в совершении преступления, форма его вины и мотивы; обстоятельства, характеризующие личность обвиняемого», т. е. необходимо установить, что преступление совершено именно этим лицом при наличии умысла или неосторожности, цель и мотив преступления независимо от того, имеют ли они уголовно-правовое значение квалифицирующих признаков, а также формальные данные о личности обвиняемого (фамилия, имя, отчество, год рождения и т. д.) и данные, характеризующие его как члена общества.

уголовного процесса, необходимой для их идентификации, решения тактических задач и установления действительной картины преступления, а также для разработки и реализации предупредительно-профилактических мер[1]. По мнению названного автора, эффективное расследование преступления возможно при установлении «социально-демографических сведений о личности преступника; сведений о его отношении к труду (учебе), об общественно-политической деятельности, поведении в быту, проведении культурного досуга; сведений о наличии (или отсутствии) прошлой антиобщественной или преступной деятельности; сведений о темпераменте, эмоционально-волевых и других психологических качествах»[2].

С точки зрения М. В. Савельевой, А. Б. Смушкина, под криминалистическим изучением личности преступника надлежит понимать «деятельность, направленную на получение и анализ информации, содержащей сведения о биографических, антропометрических, психологических и иных данных, характеризующих личность, имеющую отношение к расследуемому событию»[3]. Ю. Л. Дяблова отмечает, что личностью в криминалистике нужно называть совокупность относительно постоянных свойств, принадлежащих биологической, социальной либо биосоциальной сферам и находящих свою реализацию в признаках, которые важны как для теоретического изучения личности, так и для ее практического познания при расследовании того или иного преступления[4]. Д. Н. Балашов, Н. М. Балашов и С. В. Маликов подчеркивают, что криминалистическое изучение личности преступника позволяет следователю создать наиболее благоприятную следственную ситуацию, где можно принять оптимальное тактическое решение. По мнению авторов, объем такого изучения должен исчерпываться сведениями, которые помогут ус-

[1] Ведерников Н. Т. Криминалистическое изучение личности // Криминалистика: учебник / под ред. А. Ф. Волынского, В. П. Лаврова. 2-е изд., перераб. и доп. М.: Юнити-Дана; Закон и право, 2008. С. 104–123.

[2] Ведерников Н. Т. О проблеме предела изучения личности преступника в криминалистике // Вестник Томского государственного университета. 2014. № 385. С. 137.

[3] Савельева М. В., Смушкин А. Б. Криминалистика: учебник. М.: Издат. дом «Дашков и К», 2009. С. 99.

[4] Дяблова Ю. Л. Понятие и структура личности в криминалистике // Известия Тульского государственного университета. Серия «Экономические и юридические науки». 2016. № 2-2. С. 108.

тановить состав преступления и иные обстоятельства, дающие всестороннюю характеристику человека и имеющие значение для правильного разрешения дела[1].

Таким образом, можно заключить, что криминалистическое изучение личности преступника – это сбор, анализ и оценка криминалистически значимой информации о нем, куда входят сведения о его биологических, психологических, социальных свойствах, необходимые для эффективного решения тактических задач и установления картины события преступления. Оно позволяет определить, какие группы имеют наибольшую преступную активность, мотивы и цели (прежде всего связанные с субъективными данными, социальными установками и взглядами), которыми руководствуются преступники, и в дальнейшем выработать рекомендации по выявлению и расследованию преступлений.

Сегодня выделяются различные категории так называемых компьютерных преступников: фрикеры, ботоводы, впариватели, вирусописатели, вирмейкеры, крипторы, спамеры, крэкеры, фроды, кардеры, фишеры, скамеры и т. д. Для нас особый интерес представляют последние девять. Условно их можно разделить на две группы.

1) вирусописатели, вирмейкеры, крипторы, крэкеры и кардеры тайно похищают чужие денежные средства. Эти категории преступников часто используют специально созданные программы, с помощью которых крадут коды доступа к банковским картам, подменяют реквизиты при операциях в электронных платежных системах, перехватывают вводимые данные при нажатии определенных клавиш и т. д. При этом ими не всегда движет корыстный мотив. Совершать преступления они могут из желания показать себя гениями, прославиться (престижный мотив);

2) фроды, фишеры, спамеры и скамеры действуют обманным путем, используя методы социальной инженерии (манипулирование поведением человека посредством социальных и психологических навыков). Иначе говоря, это мошенники. Их отличают высокий интеллектуальный контроль поведения, хорошее ориентирование в нюансах социальных взаимодействий. Им свойственна постоянная потребность в риске, поиске острых ощущений. В их действиях корыстные мотивы часто переплетаются с «игровыми», поскольку для

[1] Балашов Д. Н., Балашов Н. М., Маликов С. В. Криминалистика: учебник. М.: ИНФРА-М, 2005. С. 21.

этих преступников одинаковую важность имеют материальные выгоды, полученные в результате совершения преступлений, и эмоции, переживаемые непосредственно в момент совершения преступления[1]. Фроды создают псевдосайты (несуществующий интернет-магазин либо сайт, где люди могут оказать помощь «нуждающимся»), на которых выманивают деньги у доверчивых граждан. Фишеры с помощью обмана заставляют жертву добровольно сообщить им пароли учетных записей и иную персональную информацию. Спамеры занимаются рассылкой сообщений, посредством которых могут собирать личные данные пользователей: логины, пароли, паспортные данные. Скамеры получают личную информацию о гражданах и обманывают их до тех пор, пока последние не заплатят нужную сумму.

В. В. Поляков и Л. А. Попов пишут, что сегодня «в киберпреступность потянулись предприимчивые, авантюристичные и даже харизматичные люди, которые могут получить крупные преступные доходы, с большой вероятностью избежав при этом уголовной ответственности»[2]. Такие преступники, по мнению А. А. Лихолетова и П. Е. Кулешова, психологически готовят себя к встрече с сотрудниками правоохранительных органов и ищут места для возможного укрытия. «Во время задержания и проведения следственных действий эти лица идут на разные ухищрения. Их главная цель – войти в доверие к следователю и облегчить свою участь»[3].

Анализ 123 уголовных дел, возбужденных и оконченных производством по ст. 158, 159.3 Уголовного кодекса Российской Федерации за 2018–2020 гг. в различных регионах России, и 172 судебных решений показал, что чаще всего (77 %) хищения электронных денежных средств совершают мужчины 18–35 лет. Лишь четвертая часть преступлений (23 %) была совершена женщинами 20–35 лет. Такое соотношение (3:1 в пользу мужчин) специалисты в области

[1] См.: Антонян Ю. М., Еникеев М. И., Эминов В. Е. Психология преступника и расследование преступлений. URL: http://yurpsy.com/files/ucheb/anton/04.htm (дата обращения: 23.06.2020).

[2] Поляков В. В., Попов Л. А. Особенности личности компьютерных преступников // Известия Алтайского государственного университета. Юридические науки. 2018. № 6 (104). С. 258.

[3] Лихолетов А. А., Кулешов П. Е. Особенности квалификации и расследования преступлений, связанный с хищением денежных средств с использованием платежных карт (ст. 159.3 Уголовного кодекса Российской Федерации): учеб. пособие. Волгоград: Волгоградская академия МВД России, 2018. С. 33.

юридической психологии объясняют разной социальной направленностью мужчин и женщин: первые устремлены во внешний мир, пытаются самоутвердиться, заработать авторитет, разбогатеть; вторые же нацелены на создание семьи, воспитание детей – а также нравственным складом, наличием/отсутствием склонности к авантюризму и т. д. Возраст преступников свидетельствует о сформировавшемся характере их личности.

Незначительная часть преступников (7 %) имела высшее образование, только 4 % – специальные познания в области информационных технологий. Так, 28 декабря 2018 г. примерно в 13 ч 30 мин М., имея умысел, направленный на тайное хищение чужого имущества, находясь по адресу <...>, обладая специальными познаниями и навыками в области электронно-вычислительных машин, с помощью принадлежащего ему сотового телефона «IPhone X» из корыстной заинтересованности в целях совершения хищения электронных денежных средств путем ввода логина и пароля от персонального аккаунта Потерпевшей № 1 интернет-ресурса <...> под учетной записью <...>, которые стали ему известны 26 ноября 2018 г. при создании и регистрации им указанной учетной записи по просьбе последней, осуществил неправомерный доступ в указанный персональный аккаунт Потерпевшей № 1 интернет-ресурса <...>.

Затем, реализуя свой преступный умысел, М. внес изменения в разделе «платежные системы» персонального аккаунта Потерпевшей № 1 интернет-ресурса <...>, заменив имеющийся в строке «Advcash» номер электронного кошелька Потерпевшей № 1, привязанного к ее электронной почте <...>, платежной системы «Advanced Cash» на номер созданного им электронного кошелька, привязанного к электронной почте <...>, этой же платежной системы, после чего в графе «секретный код для сохранения» ввел секретный код, полученный им ранее 26 ноября 2018 г. при регистрации персонального аккаунта, принадлежащего Потерпевшей № 1, и сохранил внесенные им изменения. В результате указанных противоправных действий М. получил возможность неограниченного доступа к персональному аккаунту Потерпевшей № 1 для дальнейшего хищения электронных денежных средств.

Затем 28 декабря 2018 г. в 14 ч 02 мин М., продолжая реализовывать свой преступный умысел, направленный на тайное хищение чужого имущества из корыстных побуждений, находясь по адресу

<...>, с помощью сотового телефона «IPhone X», будучи осведомлен о дате и времени поступления электронных денежных средств на счет персонального аккаунта интернет-ресурса <...> под учетной записью <...>, зарегистрированного на имя Потерпевшей № 1, осознавая общественную опасность и противоправный характер своих действий, путем ввода ранее известных ему логина и пароля от персонального аккаунта Потерпевшей № 1 осуществил вход в него и перевел находящиеся на данном счете электронные денежные средства в сумме 1 007 долларов США, принадлежащие Потерпевшей № 1, на свой электронный кошелек, тем самым похитил их. Далее 28 декабря 2018 г. в 15 ч 42 мин М. в целях сокрытия преступления перевел деньги со своего электронного кошелька на электронный кошелек <...>, привязанный к его электронной почте, платежной системы «Advanced Cash». Затем 28 декабря 2028 г. в 16 ч. 19 мин М. посредством сайта www.nixexchange.com произвел обмен похищенных им денежных средств, которые в дальнейшем были переведены на его лицевой счет <...>, открытый в ПАО «Сбербанк», после чего обналичены и использованы М. по его усмотрению.

Аналогичные действия М. произвел и в отношении Потерпевшей № 2, причинив ей ущерб на сумму 2 000 долларов США[1].

Специальные знания в области информационных технологий и навыки работы с ЭВМ помогают преступникам осуществить взлом чужих электронных кошельков, которые сегодня надежно защищены. Однако иногда такие знания применяют и мошенники. Например, С., имеющий навыки работы с ЭВМ и программным обеспечением через провайдера АО «ЭР-Телеком холдинг», руководствуясь корыстным преступным умыслом, направленным на неправомерный доступ к охраняемой законом компьютерной информации, находясь по адресу: <...>, на интернет-сайте <...> приобрел логин и пароль аккаунта <...> интернет-магазина «OZON.ru», принадлежащего Потерпевшему № 1, на пользовательском счете у которого находились денежные средства в сумме 11 500 руб., в целях последующего их хищения путем мошенничества в сфере компьютерной информации.

[1] См.: Приговор Ленинского районного суда г. Махачкалы № 1-281/2019 от 11 июня 2019 г. по делу № 1-281/2019. URL: https://sudact.ru/regular/doc/u64vRKWrBYVL/ (дата обращения: 21.04.2020).

При реализации своего преступного умысла С., действуя умышленно, из корыстных побуждений, достоверно зная требования, которые необходимо соблюдать при использовании информационных возможностей сети «Интернет», осуществил неправомерный доступ к аккаунту <...> интернет-магазина «OZON.ru» Потерпевшего № 1 и без его разрешения изменил логин <...> на <...> и пароль, тем самым осуществил вход в учетную запись Потерпевшего № 1 и получил доступ к компьютерной информации аккаунта и пользовательскому счету, блокировав при этом доступ Потерпевшему № 1. Далее С. сформировал заказ на приобретение товаров на общую сумму 11 596 руб., оплатив 11 500 рублей с пользовательского счета Потерпевшего № 1 и 96 руб. через собственный QIWI кошелек. Однако сотрудниками ООО «Интернет решения» из-за подозрения в несанкционированном доступе заказ был аннулирован, аккаунт заблокирован, денежные средства возвращены на пользовательский счет Потерпевшего № 1. После этого С. сформировал аналогичный заказ на приобретение товаров на общую сумму 11 634 руб., оплатив 11 500 руб. с пользовательского счета Потерпевшего № 1 и 134 руб. через собственный QIWI кошелек. Но и этот заказ был отменен[1].

Ранее считалось, что преступления, связанные с использованием компьютера и Интернета, могут совершать лишь талантливые, любознательные люди с высоким уровнем интеллекта, имеющие специальные знания. Однако, как справедливо отмечают В. В. Поляков и Л. А. Попов, «в совершение компьютерных преступлений втянут довольно широкий круг лиц, среди которых встречаются как дилетанты, так и высококвалифицированные специалисты»[2]. Хищение электронных денежных средств, за исключением взлома электронных кошельков, не предполагает наличия специальных знаний, достаточно навыков пользователя, которые часто приобретаются самостоятельно.

Примерно в 50 % рассмотренных нами случаев преступники были трудоспособны, однако не имели постоянного места работы или учебы, при этом на их иждивении находились малолетние дети.

[1] См.: Приговор Мотовилихинского районного суда г. Перми № 1-72/2019 от 20 февраля 2019 г. по делу № 1-72/2019. URL: https://sudact.ru/regular/doc/kgD0-AP0FckUW/ (дата обращения: 21.04.2020).

[2] Поляков В. В., Попов Л. А. Особенности личности компьютерных преступников. С. 258.

3 % преступников в момент совершения преступления проходили службу по призыву в Вооруженных силах Российской Федерации.

16 % преступников находились в состоянии алкогольного опьянения. 4 % имели психическое расстройство личности, что свидетельствует об умышленном и спланированном характере большинства совершаемых преступлений.

В 92 % преступник действовал в одиночку, лишь 8 % преступлений были совершены в соучастии.

Примерно 22 % преступников имели судимость, что позволяет сделать вывод о влиянии криминального прошлого на поведение преступников, об отсутствии признаков его исправления и о совершенствовании посредством свойств сети «Интернет» ранее полученных преступных навыков.

Таким образом, в результате проведенного нами исследования можно заключить, что в большинстве случаев хищения электронных денежных средств совершают мужчины 18–35 лет, имеющие среднее или среднее специальное образование, трудоспособные, но без постоянного места работы или учебы, содержащие малолетних детей, дееспособные, действующие в одиночку, не обладающие специальными знаниями в области информационных технологий и навыками работы с ЭВМ.

Сосредоточим свое внимание на орудиях и средствах совершения хищений электронных денег, выбор которых тесно связан со способами совершения преступления, но для начала определим, что следует понимать под данными терминами. А. С. Денисова отмечает, что орудиями надлежит называть предметы материального мира, используемые в целях разрушающего воздействия на предметы преступления или причинения физического вреда человеку, полностью находящиеся под контролем воли и сознания субъекта, применяющиеся для непосредственного осуществления преступного деяния путем уменьшения количества затрачиваемых усилий или концентрации силы; средствами – различные вещества, предметы, газы и т. д., химические, биологические и иные свойства которых используются преступником в процессе совершения преступления для создания

благоприятных условий, не поддаются полному контролю воли субъекта, а только включаются им в преступную деятельность[1].

В нашем случае орудиями совершения преступления являются персональные компьютеры, смартфоны и прочие девайсы, электронные носители информации (накопители на оптических компакт-дисках, флэш-накопители и др.), вредоносное программное обеспечение, куда входят и программы удаленного доступа (типа TeamViewer, AnyDesk и т. д.). Не будем останавливаться на первых двух, сделаем акцент на последнем.

С сожалением приходится констатировать, что в настоящее время рынок вредоносного софта весьма обширен. Сегодня различают несколько программ, нацеленных на кражу личных данных пользователей и их денежных средств:

1) стиллеры – программы, похищающие логины и пароли, данные автозаполнения;

2) клипперы – скрытые программы для подмены буфера обмена (скопированных пользователем кошельков или ссылок на заданные преступником);

3) бэкдоры – вредоносное программное обеспечение, используемое киберпреступниками для получения несанкционированного удаленного доступа к компьютерной системе, которое работает в фоновом режиме и скрывается от пользователя. Специалисты отмечают, что данные программы входят в число самых опасных, так как позволяют злоумышленникам выполнять любые действия на зараженном компьютере: следить за пользователем, управлять его файлами, устанавливать дополнительное программное обеспечение или вирусы, контролировать операционную систему и атаковать другие хосты[2]. Бэкдоры часто используются для объединения группы компьютеров-жертв в ботнет или зомби-сеть для использования в криминальных целях[3];

---

[1] См.: Денисова А. С. Уголовно-правовое значение орудий и средств совершения преступления: автореф. дис. … канд. юрид. наук. М., 2005. С. 8–9.

[2] См.: Что такое бэкдоры и как это удалить. URL: https://bedynet.ru/%D0%B1%D1%8D%D0%BA%D0%B4%D0%BE%D1%80%D1%8B/ (дата обращения: 21.06.2021).

[3] См.: Что такое троянская программа. URL: https://kaspersky-ru.turbopages.org/turbo.kasersky.ru/s/resource-center/threats/trojans (дата обращения: 21.06.2021).

4) кейлоггеры – программы, запоминающие все данные, которые водятся с помощью клавиатуры, преимущественно логины и пароли;

5) шифровальщики и винлокеры – программы, блокирующие файлы в целях вымогания денег, и др.

Кроме того, по мнению Е. Р. Россинской и И. А. Рядовского, для совершения преступлений злоумышленники могут применять и легальное программное обеспечение: «Большинство легальных программ, используемых в противоправной деятельности, предназначено для удаленного несанкционированного доступа к компьютеру, управления системой и ее администрирования. Для своих целей преступники модифицируют их, скрывая от пользователя явно отображаемые на дисплее уведомления и иные признаки удаленного подключения»[1]. Данную точку зрения разделяют и другие авторы[2]. Наиболее часто для хищения электронных денег злоумышленники применяют программы удаленного доступа AnyDesk и TeamViewer (нередко в совокупности с приемами социальной инженерии и SIM-swapping[3]) – легальные продукты, которые пользователи скачивают с сайтов разработчиков или из магазина приложений Google Play и не подозревают об угрозе. По словам менеджера по развитию бизнеса Kaspersky Fraud Prevention Е. Даниловой, с их помощью мошенникам удается обмануть граждан в 48 % случаев[4]. Таким образом легальные программные продукты превращаются во вредоносные. Согласно ст. 273 Уголовного кодекса Российской Федерации вредоносными программами признаются те, которые заведомо нацелены на несанкционированное уничтожение, блокирование, мо-

[1] Россинская Е. Р., Рядовский И. А. Концепция вредоносных программ как способов совершений компьютерных преступлений: классификации и технологии противоправного использования // Всероссийский криминологический журнал. 2020. Т. 14. № 5. С. 702.

[2] См., например: Алескеров В. И., Баранов В. В. Некоторые способы хищения денежных средств, совершаемых в системе дистанционного банковского обслуживания // Академическая мысль. 2020. № 2 (11). С. 12–16; Поддубный И. В. К вопросу об использовании злоумышленниками программ удаленного доступа и вредоносного ПО как средств совершения хищений с банковских карт граждан // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 99–105.

[3] Техника подмены SIM-карты.

[4] См.: Герасюкова М. Удаленный доступ: как мошенники обманывают клиентов банков. URL: https://www.gazeta.ru/tech/2020/05/15/13084063/new_ways.shtml (дата обращения: 20.06.2021).

дификацию, копирование компьютерной информации или нейтрализацию средств компьютерной защиты[1]. Однако авторы одного из первых комментариев к УК РФ отмечали: «Вредоносность или полезность соответствующих программ для ЭВМ определяется не в зависимости от их назначения, способности уничтожать, блокировать, модифицировать, копировать информации (это вполне типичные функции абсолютно легальных программ), а в связи с тем, предполагает ли их действие, во-первых, предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает программу для ЭВМ вредоносной»[2]. Мы солидарны с приведенной точкой зрения, поэтому считаем программы Anydesk и TeamViewer, *использующиеся для несанкционированного доступа* к личным данным юзеров, вредоносными.

Средствами совершения хищений электронных денег выступают информационно-телекоммуникационная сеть Интернет и средства обеспечения доступа к ней; программное обеспечение операторов электронных платежных средств (электронные кошельки); мессенджеры, информационные ресурсы торговых площадок (Avito, Youla и др.), где размещается недостоверная информация о продаже товаров, вакансиях, об услугах и т. д.; фишинговые сайты; социальные сети. При этом злоумышленники могут использовать сразу несколько средств совершения преступления. Так, Ленинским районным судом г. Омска было установлено, что Г. в 2017 г. решил совершить хищение денег путем обмана в сети Интернет. Реализуя задуманное, используя принадлежащий ему ноутбук <…> на интернет-ресурсе <…> он размещал заведомо ложные объявления о продаже спортивных товаров, указывая при этом их стоимость ниже рыночной для привлечения большего количества покупателей, не имея в действительности указанных товаров, возможности выступить

[1] См.: Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021). URL: www.consultant.ru (дата обращения: 21.06.2021).

[2] Комментарий к Уголовному кодексу Российской Федерации. Особенная часть / под ред. Ю. И. Скуратова, В. М. Лебедева. М.: Норма – Инфра-М, 1996. С. 419.

посредником при их продаже, а также намерения совершать сделки купли-продажи. Кроме того, Г. приобрел сим-карты операторов сотовой связи <…>, которые были необходимы ему для общения с потенциальными покупателями. Отводя от себя подозрения, Г. решил использовать найденный им в 2017 г. паспорт гражданина Российской Федерации серии <…> на имя Ф.Д.С. ДД.ММ.ГГГГ рождения, утерянный последним.

Г. создал фиктивные сайты интернет-магазинов, якобы специализирующиеся на продаже и поставке спортивных товаров. Используя сеть Интернет, Г. зарегистрировал на незнакомых ему лиц, сведения о которых были получены им в сети Интернет, а также на своих знакомых электронные средства платежа платежного сервиса <…>. В дальнейшем Г. намеревался использовать их в своей преступной деятельности в качестве электронных средств платежа, куда потерпевшие затем переводили деньги в счет оплаты приобретаемых товаров. Принятые на себя обязательства Г. не выполнил, после перечисления денежных средств на телефонные звонки и сообщения потерпевших не отвечал, похищенными денежными средствами распоряжался по своему усмотрению[1].

Важнейшим элементом криминалистической характеристики преступлений являются данные о способах подготовки, совершения и сокрытия преступлений, под которыми, по мнению Г. Г. Зуйкова, надлежит понимать систему действий преступника по подготовке, совершению и сокрытию преступления, детерминированных объективными и субъективными факторами и связанных с использованием орудий и средств[2]. Р. С. Белкин, уточняя приведенное определение, предложил дополнить его указанием на объединение системы этих действий общим преступным замыслом[3]. С точки зрения Р. С. Бел-

[1] См.: Постановление Ленинского районного суда г. Омска № 1-300/2019 от 24 июня 2019 г. по делу № 1-300/2019. URL: https://sudact.ru/regular/doc/r3Gy6n1iafHw/ (дата обращения: 26.07.2021).

[2] См.: Зуйков Г. Г. Поиск преступников по признакам способов совершения преступлений: учеб. пособие. М.: ВШ МВД СССР, 1970. С. 84; Зуйков Г. Г. Развитие криминалистического учения о способе совершения преступления и проблема способа сокрытия преступления // Повышение эффективности расследования преступлений: сб. науч. тр. Иркутск: Изд-во ИГУ, 1986. С. 50.

[3] См.: Белкин Р. С. Курс криминалистики: в 3 т. Т. 3. Криминалистические средства, приемы и рекомендации. М.: Юристъ, 1997. С. 359.

кина, «...способ совершения и сокрытия преступления, точнее – знание о нем, определяют путь познания истины по делу, т. е. метод раскрытия и расследования»[1].

Н. П. Яблоков понимал под способом совершения преступления объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющую различного рода характерные следы вовне, которые позволяют с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить наиболее оптимальные методы решения задач раскрытия преступления[2].

По мнению А. А. Бессонова, способ преступления «включает в себя триединый комплекс действий по подготовке, совершению и сокрытию преступления. Каждое из этих действий в структуре способа может существовать как само по себе, так и в совокупности с другими из них: „подготовка к преступлению“, „подготовка – совершение преступления“, „совершение преступления“, „подготовка – совершение – сокрытие преступления“, „совершение – сокрытие преступления“, „ сокрытие совершенного преступления иными лицами“»[3].

М. С. Уткин различает следующие способы совершения преступлений:

– полноструктурные или наиболее квалифицированные (охватывают подготовку, совершение и сокрытие преступлений);

– менее квалифицированные или усеченные первого типа (совершение и сокрытие преступлений);

– менее квалифицированные или усеченные второго типа (подготовка и совершение преступлений);

---

[1] Белкин Р. С. Курс криминалистики: учеб. пособие. М.: ЮНИТИ-ДАНА; Закон и право, 2001. С. 805.

[2] См.: Яблоков Н. П. Криминалистика: учебник. 2-е изд., перераб. и доп. М.: Норма, 2009. С. 34; Яблоков Н. П. Криминалистическая характеристика отражаемой преступлением информации // Криминалистика: учебник / под ред. А. И. Бастрыкина. М.: Экзамен, 2014. Т. 1. С. 76.

[3] Бессонов А. А. Способ преступления как элемент его криминалистической характеристики // Пробелы в российском законодательстве. 2014. № 4. С. 172.

– неквалифицированные или упрощенные (только совершение преступления)[1].

Полагаем, что применительно к хищениям электронных денежных средств речь должна идти о полноструктурных способах совершения преступлений, поскольку они требуют тщательной подготовки и сокрытия.

В числе основных действий по подготовке к совершению хищений электронных денежных средств необходимо назвать принятие решения о совершении преступления; определение цели, времени, места, средств и методов ее достижения; распределение ролей среди участников преступной группы, если таковая имеется (организаторы, разработчики, взломщики, заливщики или вбивалы, обнальщики, дропы и т. д.); подбор потенциальных жертв; подготовку средств совершения преступления (SIM-карт; фишинговых сайтов; средств преодоления защиты информации, ее уничтожения, блокирования, копирования и модификации; необходимых документов и т. д.). Б. П. Смагоринский и А. В. Сычева отмечают: «Планируя совершение „вирусных“ кибермошенничеств, преступники занимаются поиском необходимых документов для того, чтобы зарегистрировать их владельцев в качестве идентификаторов в электронных платежных системах и затем регистрировать на их имя SIM-карты, открыть электронные кошельки для перевода и обналичивания похищенных денежных средств»[2]. Согласимся с мнением Г. З. Гаспаряна о том, что в действия по подготовке к совершению хищений денежных средств с использованием информационных банковских технологий нужно включить изучение специальных вопросов функционирования программных продуктов, аппаратно-программных средств и сетей передачи данных, а также изучение их уязвимостей и возможностей преодоления защиты информации[3].

Ю. В. Гаврилин полагает, что способы совершения преступлений, посягающих на информационную безопасность в сфере эконо-

[1] См.: Уткин М. С. Особенности расследования и предупреждения хищений в потребительской кооперации: автореф. дис. … канд. юрид. наук. Свердловск, 1975. С. 6.

[2] Смагоринский Б. П., Сычева А. В. Новые способы совершения мошенничеств, связанных с распространением коронавирусной инфекции // Вестник Волгоградской академии МВД России. 2020. № 2 (53). С. 114.

[3] См.: Гаспарян Г. З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий. С. 42.

мики, можно разделить на несколько групп с учетом формы контакта с носителем охраняемой законом информации:

– способы непосредственного доступа к охраняемой законом информации путем физического контакта с ее носителем;

– способы дистанционного, опосредованного доступа к охраняемой законом информации, при реализации которых противоправное воздействие на нее осуществляется с использованием информационно-телекоммуникационных технологий;

– смешанные способы, осуществляющиеся как непосредственно, так и опосредованно[1].

В случае с электронными денежными средствами главным образом речь идет о дистанционном доступе, что, в том числе, обусловливает сложность установления личностей преступников. Анонимное интернет-пространство и безграничное доверие граждан дают злоумышленникам широкие возможности для получения чужих денег разнообразными способами, наиболее распространенными из которых являются:

– предложение товаров и услуг по выгодным ценам: часто действия преступников замаскированы под интернет-магазин, где регулярно проходят акции и действуют привлекательные скидки. Так, в 2018 г. накануне «черной пятницы» в Интернете появилось больше 400 сайтов-копий AliExpress и еще 200 интернет-страниц, стилизованных под известные бренды и магазины[2]. После создания таких сайтов на них настраивается «редирект», затем через мессенджеры, социальные сети, поисковую оптимизацию (SEO) ссылка продвигается. Пройдя по ней, покупатель попадает на сайт несуществующего магазина, где мошенники убеждают его приобрести тот или иной товар. Подобным образом действуют маркетологи, поэтому отличить фейковый сайт от обычного особенно в период распродаж – задача не из легких. Цель злоумышленников – усыпить бдительность потенциальной жертвы и заставить ее заплатить деньги или передать личные данные (логин, пароль, адрес электронный почты для доступа

[1] См.: Гаврилин Ю. В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы: автореф. дис. … д-ра юрид. наук. М., 2010. С. 33–34.

[2] См.: Игорь Зубков. К «черной пятнице» мошенники создали 400 сайтов-клонов AliExpress. URL: https://rg.ru.turbopages.org/rg.ru/s/2018/11/22…400-sajtov-klonov-aliexpress.html (дата обращения: 05.12.2020).

к электронному кошельку и др.). После внесения покупателем стопроцентной предоплаты или передачи необходимых преступникам данных продавец перестает отвечать на сообщения, его профиль оказывается заблокированным, а интернет-магазин прекращает свою работу;

– фишинг (от англ. fishing – рыбная ловля) – письма, сообщения от имени электронных платежных систем WebMoney, Яндекс.Деньги, PayPal и др. о блокировании счета с указанием ссылки для его реактивации. Пользователь направляется на сайт – копию сайта платежной системы, принадлежащую преступникам, вводит логин и пароль, тем самым предоставляет последним доступ к своему электронному кошельку. Кроме того, довольно часто фишинговые письма рассылаются якобы от имени крупных компаний. При этом мошенники используют фиктивные адреса электронной почты, которые на первый взгляд выглядят весьма правдоподобно. Так, с адреса autoshipping@amazon.com, внешне напоминающего адрес гиганта электронной коммерции – компании Amazon, были разосланы тысячи писем, содержащих вымогатель «Locky» – вирус, шифрующий данные пользователей, затем требующий плату за дешифровку. Вредоносное программное обеспечение может содержаться в приложениях, которые мошенники предлагают скачать пользователям для получения скидки, а также в электронных купонах или сертификатах;

– интернет-попрошайничество: преступники создают сайт – аналог сайта благотворительной организации, фонда, где просят оказать помощь нуждающимся, однако реквизиты сайтов отличаются друг от друга;

– кви про кво (услуга за услугу) – потерпевшего информируют о необходимости проведения профилактических работ на персональном компьютере и предлагают установить программу удаленного доступа, после чего потенциальная жертва передает преступникам цифровой код, и они через удаленные каналы похищают денежные средства или учетные записи. Однако последнее не всегда возможно благодаря двухфакторной аутентификации (2FA). Если мошенники сталкиваются с таким препятствием, то, как правило, применяют SIM-swapping, и все звонки и текстовые сообщения, предназначенные потенциальному потерпевшему, поступают им.

В основе всех перечисленных способов совершения хищений электронных денег лежит социальная инженерия – «совокупность

приемов, методов и технологий создания такого пространства, условий и обстоятельств, которые максимально эффективно приводят к конкретному необходимому результату, с использованием социологии и психологии»[1]. Иначе говоря, это манипулирование сознанием людей для получения доступа к конфиденциальной информации. По данным информационного агентства ТАСС, число кибератак с помощью социальной инженерии в 2020 г. выросло в 1,9 раза[2].

Кроме того, хищения электронных денег могут совершаться посредством вредоносного программного обеспечения, которое взламывает электронные кошельки. Наконец, деньги могут красть сотрудники платежных систем или фирм, оказывающих им поддержку. Подобный случай был зафиксирован еще в июле 2009 г. 23-летний программист из Сыктывкара в обеденный перерыв проник в служебный компьютер своего коллеги и скопировал файлы, содержащие электронные сертификаты доступа к счету в платежной системе. Затем злоумышленник, зная, что проводимые в электронной платежной системе транзакции можно проследить, в помещении одного из Сыктывкарских интернет-клубов, используя анонимные прокси-серверы, зарегистрировал на вымышленные данные несколько электронных кошельков в различных платежных системах. Ночью 30 июля 2009 г., посетив другой интернет-клуб, с помощью похищенных сертификатов он получил неправомерный доступ к счету индивидуального предпринимателя <…> в платежной системе <…> и похитил все имевшиеся на счету средства, переведя их на один из зарегистрированных ранее электронных кошельков. Впоследствии программист несколько раз из разных мест переводил похищенные деньги из одной платежной системы в другую, стремясь скрыть следы преступления. Деньги в итоге были выведены на счет одного из знакомых злоумышленника и обналичены[3].

Применительно к юридическим лицам мошенники используют способ «человек посередине, известный еще с 1980-х гг. и представ-

[1] Тепляков С. П., Тимохович А. С. Социальная инженерия. Анализ и методы защиты // Academy. 2018. № 7 (34). С. 26.

[2] См.: Число кибератак с помощью социальной инженерии в 2020 г. увеличилось в 1,9 раза. URL: https://tass-ru.turbopages.org/turbo/tass/ru/s/ekonomika/10971205 (дата обращения: 26.07.2021).

[3] См.: В Коми осужден программист, похитивший деньги с расчетного счета предпринимателя. URL: https://komiinform.ru/news/64150 (дата обращения: 17.04.2021).

ляющий собой внедрение в беседу двух сторон и подмену реквизитов. Раньше это делали во время телефонных разговоров, теперь – при переписке по электронной почте. Злоумышленники выявляют организацию, которая будет вести переписку с зарубежными контрагентами и переводить им какие-либо деньги, затем устанавливают данные ее электронных ящиков. С помощью взлома, подбора пароля они получают удаленный доступ к почте, изучают переписку между сторонами, а когда речь заходит о заключении договора, подменяют его фейковым[1].

В целях сокрытия преступной деятельности злоумышленники все чаще используют:

1) криптографические алгоритмы защиты информации: сегодня различают такие виды шифрования, как симметричное (для шифрования и расшифрования используется один и тот же ключ); ассиметричное или шифрование с открытым ключом (используются открытый и закрытый ключи, математически связанные между собой, при этом первый может передаваться по незащищенным каналам, применяется для шифрования данных и проверки электронной цифровой подписи, второй нужен для генерации цифровой подписи и расшифровки данных); хеширование – одностороннее шифрование, при котором начальные данные независимо от их длины превращаются в битовую строку фиксированной длины (хеш). Идеальным считается такой алгоритм, когда обратное преобразование хеша невозможно[2];

2) ремейлеры – серверы, получающие сообщения электронной почты и перенаправляющие их по адресу, указанному отправителем. При этом при переадресации вся информация об отправителе уничтожается. Некоторые ремейлеры позволяют шифровать письма и указывать фиктивный адрес отправителя. В таком качестве могут

[1] См.: Жур Я. Встревают в беседу и поглощают сотни тысяч рублей: вид мошенничества из 80-х принял новую форму. «Человек посередине» вернулся. URL: https://sb-by.turbopages.org/turbo/sb.by/s/articles/chelovek-poseredine-vernulsya.html (дата обращения: 17.04.2021).

[2] См.: Криптография для хакеров. Основы алгоритмов шифрования. URL: https://hacker-basement.ru/2019/08/23/kryptografia-dlya-hakerov-algorytmy-shifrovaniy/ (дата обращения: 27.07.2021).

выступать специализированные веб-сайты, открытые SMTP-серверы и анонимные сети типа Mixminion[1];

3) анонимайзеры – инструменты для обеспечения анонимности веб-серфинга, обхода блокировки веб-фильтров и локальных законодательных ограничений посещения веб-сайтов посредством перенаправления веб-трафик пользователя через свои серверы, сокрытия реального IP-адреса и удаления специальных cookie-файлов. Сегодня существует несколько типов анонимайзеров:

– веб-анонимайзеры представлены в виде сайтов, обеспечивают работу пользователя без дополнительных программ, подходят для быстрого доступа к простым сайтам;

– прокси-серверы не требуют установки дополнительного программного обеспечения (нужно лишь указать адрес прокси-сервера в настройках браузера), работают как посредник (пропускают весь трафик через себя) для всех сайтов сразу, подменяя действительный IP-адрес пользователя на другой;

– VPN – технология, которая способна перенаправлять трафик, однако нуждается в VPN-доступе или дополнительном программном обеспечении. Внутри этой системы существуют серверы и выходной узел, т. е., если соединение с Интернетом происходит через VPN, узел назначения может видеть только адрес VPN-сервера;

– расширения для браузеров – для их использования нужно установить специальную программу, принцип работы заключается в перенаправлении трафика через серверы системы;

– анонимная сеть TOR, перенаправляющая трафик через несколько анонимных серверов (не менее трех), что дает возможность скрыть реальный источник информации путем «запутывания» метаданных. Такая система перенаправления называется луковой маршрутизацией: каждый узел в сети может расшифровать только часть сообщения с инструкциями о перенаправлении трафика. Выходной узел полностью расшифровывает сообщение и перенаправляет его конечному узлу открытой сети, для чего TOR формирует канал перенаправления и получает ключи шифрования от всех узлов сети, входящих в этот канал. Ключи же передаются отправителю, который,

[1] См.: Электронная почта. Ремейлер. URL: https://google--info-org.turbopages.org...-balancer-8080-BAL-7957&trb (дата обращения: 26.07.2021).

в свою очередь, использует их для шифрования данных перед отправкой[1];

4) специальные программные средства для безвозвратного уничтожения цифровой информации. Естественно, что любой носитель информации можно подвергнуть физическому уничтожению (механическому разрушению, металлотермическому нагреву, разрушению в химически агрессивной среде, ионизирующему излучению, размагничиванию или намагничиванию рабочего слоя, нагреву до потери точки намагниченности (800–1000°С), однако в настоящее время имеются средства, позволяющие сохранить носитель, но при этом гарантированно стереть всю информацию на нем. Как правило, такими средствами являются специальные программы типа CCleaner, File Shredder, Delete Files Permanently и др. Большинство из них очищают жесткий диск и реестр операционной системы, а также удаляют программы, затирают свободное место на жестком диске, что дает возможность уничтожить данные без их дальнейшего восстановления[2].

Знания о способах действий преступников необходимо в связи с тем, что уровнем осведомленности следователя о содержании и специфике поведения преступника во многом определяются направление и объем предварительного следствия по уголовным делам, криминалистическое содержание рекомендаций о приемах и средствах раскрытия и расследования преступлений.

В числе базовых элементов криминалистической характеристики хищений электронных денежных средств мы также выделили особенности механизма следообразования.

Традиционно следы преступлений принято делить на две группы: материальные (изменения в элементах вещной обстановки, которые образуются в результате механического, термического, химического и иного воздействия) и идеальные (отображение криминалистически значимой информации в сознании людей). Однако следы компьютерных преступлений, в том числе хищений электронных денежных средств (так называемые «виртуальные»), нельзя включить ни в одну из них, поэтому они были выделены В. А. Мещеряковым в особую категорию. На их природу также обращают внимание Н. Д. Асколь-

[1] См.: «Игра в прятки»: немного о технологиях анонимности в Интернете. URL: https://habr.com/ru/company/cloud_mts/blog/312032 (дата обращения: 27.07.2021).

[2] См.: Программы для безвозвратного удаления файлов. URL: https://www.–soft-salad.ru/articles/best-programs/permamemtly-delete-files (дата обращения: 27.07.2021).

ская, А. А. Бессонов, А. Г. Волеводз, О. Ю. Введенская, В. А. Козлов, Е. Р. Россинская, И. А. Рядовский, А. И. Семикаленова и другие ученые.

А. Г. Волеводз определяет виртуальные следы как данные о происхождении информации: таблицы размещения файлов, системные реестры операционных систем, отдельные кластеры магнитного носителя, файлы и каталоги хранения сообщений электронной почты, файлы конфигурации программ удаленного доступа и иное[1].

Е. Р. Россинская и И. А. Рядовский используют термин «цифровые следы», которые представляют собой криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи[2].

Е. С. Переверзева и А. В. Комов отмечают, что «виртуальные следы находятся исключительно в сетевом пространстве в отличие от цифровых, которые могут находиться на материальных носителях информации»[3]. По мнению названных авторов, данные понятия соотносятся как часть (виртуальные следы) и целое (цифровые следы).

В. Б. Вехов называет следы компьютерных преступлений материальными, поскольку они оставлены на материальных носителях путем изменения их свойств или состояния отдельных элементов[4].

Ю. В. Гаврилин и В. В. Шипилов отмечают, что следы киберпреступлений как специфическая форма преобразования компьютерной информации обладают следующими признаками:

1) отражают событие преступления в информационном поле;

2) являются материальными по своей природе, но не отражают пространственной формы следообразующего объекта;

---

[1] См.: Волеводз А. Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь.2002. № 1. С. 4.

[2] См.: Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы междунар. науч.-практ. конф. (19 февраля 2019 г.). Алматы: Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2019. С. 6–8.

[3] Переверзева Е. С., Комов А. В. Виртуальные и цифровые следы: новый подход в понимании // Вестник Санкт-Петербургского университета МВД России. 2021. № 1 (89). С. 176.

[4] См.: Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: моногр. Волгоград: Волгоградская академия МВД России, 2008. С. 94.

3) являются результатом преобразования компьютерной информации;

4) обладают способностью к дублированию, т. е. к копированию на другие электронные носители без изменения их характеристик[1].

По мнению А. Л. Осипенко, следы компьютерных преступлений сложно обнаружить, поскольку они распределяются по множеству субъектов (компьютерная система жертвы, преступника, провайдера, промежуточные сетевые узлы и т. д.)[2]. Применительно к хищениям электронных денежных средств подобными субъектами могут быть операторы платежных систем; электронные торговые площадки; интернет-провайдеры; серверы компаний, предоставляющих услуги пользования той или иной социальной сетью; сервисы электронных сообщений; «облачные» хранилища; компьютерные системы потерпевшего и подозреваемого.

Если говорить об операционных системах операторов платежных систем, то здесь большое криминалистическое значение имеют информация о совершенных переводах денежных средств, об остатках электронных денежных средств; данные, которые клиент указывает в распоряжении. Согласно ч. 1 ст. 7.2. Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 7 августа 2001 г. № 115-ФЗ физическим лицам следует указывать фамилию, имя, отчество; гражданство; дату рождения; реквизиты документа, удостоверяющего личность; идентификационный номер налогоплательщика. Юридическим лицам – наименование, организационно-правовую форму, идентификационный номер налогоплательщика, основной государственный регистрационный номер, адрес[3].

Не менее важна информация, хранящаяся в ресурсах электронных торговых площадок: персональные данные пользователя, раз-

[1] См.: Гаврилин Ю. В., Шипилов В. В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013. № 23. С. 2–6.

[2] См.: Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы: моногр. Омск: Омская академия МВД России, 2009. С. 11.

[3] См.: О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: федер. закон от 7 августа 2001 г. № 115-ФЗ. URL: www.consultant.ru (дата обращения: 27.07.2021).

местившего объявление о товаре, вакансии, услуге; контактные данные; время создания объявления; cookie-файлы – файлы, автоматически сохраняющиеся на устройстве при посещении сайта.

Информационные системы интернет-провайдеров содержат данные пользователя, включая его идентификатор, сетевой адрес и время регистрации, информацию о произведенных денежных операциях, приеме текстовых, мульмедийных, голосовых сообщений. Серверы компаний, предоставляющих услуги пользования той или иной социальной сетью, – наличие аккаунта, его привязку к номеру телефона или адресу электронной почты, текстовые сообщения, мульмедийные файлы, статистику активности пользователя. Сервисы электронных сообщений – текстовые сообщения, мульмедийные файлы. «Облачные» хранилища – учетные данные, платежные реквизиты, мульмедийные файлы.

К следам, содержащимся в персональных компьютерах и пользовательском оборудовании, подключаемом к сети подвижной связи, прежде всего, относятся log-файлы – текстовые файлы, где содержится информация о действиях программного обеспечения или пользователей (хронология событий, их источников, ошибок и причин, по которым они произошли)[1]. Кроме того, здесь же необходимо упомянуть журналы администрирования и безопасности, реестры компьютера, «метаданные» свойств файлов, коды вредоносных программ, текстовые и мультимедийные файлы. В случае если речь идет о пользовательском оборудовании, подключаемом к сети подвижной связи, стоит обращать внимание на контакты, текстовые сообщения, сообщения электронной почты, чаты, базы данных, поисковые запросы, данные приложений, карты и т. д.

В завершение параграфа резюмируем сказанное. В число базовых элементов криминалистической характеристики хищений электронных денежных средств входят данные об объекте и предмете преступного посягательства, личности преступника, орудиях и средствах совершения преступления, способах подготовки, совершения и сокрытия преступления, особенностях механизма следообразования. Родовым объектом хищений электронных денежных средств выступают

[1] См.: Какие виды лог-файлов бывают. URL: https://ru.hostings.info/termins/log-fayly.html (дата обращения: 27.07.2021).

общественные отношения в сфере экономики, видовым – отношения собственности, непосредственным – электронные денежные средства. Непосредственный объект совпадает с предметом преступного посягательства. В большинстве случаев хищения электронных денег совершают мужчины 18–35 лет, имеющие среднее или среднее специальное образование, трудоспособные, но без постоянного места работы или учебы, содержащие малолетних детей, дееспособные, действующие в одиночку, не обладающие специальными знаниями в области информационных технологий и навыками работы с ЭВМ. Орудиями совершения преступления являются персональные компьютеры, смартфоны и прочие девайсы, электронные носители информации, вредоносное программное обеспечение. Средствами – информационно-телекоммуникационная сеть Интернет и средства обеспечения доступа к ней; программное обеспечение операторов электронных платежных средств; мессенджеры, информационные ресурсы торговых площадок; фишинговые сайты; социальные сети. Способ совершения хищений электронных денежных средств полноструктурный (включает подготовку, совершение и сокрытие преступления), чаще всего дистанционный. В основе значительного количества способов совершения преступлений лежат приемы социальной инженерии. Следы хищений электронных денежных средств можно обнаружить в операционных системах операторов платежных систем, ресурсах электронных торговых площадок, информационных системах интернет-провайдеров, серверах компаний, предоставляющих услуги пользования той или иной социальной сетью, сервисах электронных сообщений, «облачных» хранилищах, компьютерных системах потерпевшего и подозреваемого.

ГЛАВА 2 СПЕЦИФИКА СТАДИИ ВОЗБУЖДЕНИЯ УГОЛОВНЫХ ДЕЛ О ХИЩЕНИЯХ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ И ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ

2.1. Проблемы стадии возбуждения уголовных дел о хищениях электронных денежных средств

В соответствии со ст. 146 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) «при наличии повода и основания… орган дознания, дознаватель, руководитель следственного органа, следователь в пределах компетенции, установленной настоящим Кодексом, возбуждают уголовное дело, о чем выносится соответствующее постановление»[1]. При этом, исходя из ст. 140 УПК РФ, «поводами для возбуждения уголовного дела служат:

1) заявление о преступлении;

2) явка с повинной;

3) сообщение о совершенном или готовящемся преступлении, полученное из иных источников;

4) постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании <…>.

2. Основанием для возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления»[2].

Возбуждение уголовного дела есть важнейшая стадия уголовного процесса. Ее значимость подчеркивают многие авторы[3]. Так, Председатель Верховного Суда Российской Федерации В. М. Лебедев

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 01.07.2021). URL: www.consultant.ru (дата обращения: 10.08.2021).

[2] Там же.

[3] См., например: Андреева О. И. О необходимости стадии возбуждения уголовного дела в современном уголовном процессе России // Вестник Томского государственного университета. 2012. № 356. С. 109–112; Сергеев А. Б., Хохрякова Э. А. Стадия возбуждения уголовного дела – «атавизм» уголовного процесса? // Вестник Челябинского государственного университета. 2015. № 17 (372). Право. Вып. 43. С. 163–170; Яковлев М. М., Федоров И. К. К вопросу о понятии и значении стадии возбуждения уголовного дела в уголовном процессе России // Проблемы науки. 2018. № 11 (35). С. 22–25 и др.

отмечает: «Возбуждение уголовного дела – это уголовно-процессуальная деятельность и уголовно-процессуальные отношения, образующие начальную стадию уголовного процесса, задачей которой является рассмотрение, а в некоторых случаях проверка методами, установленными законом, обнаруженных первичных данных о совершенном или готовящемся преступлении, в результате чего уполномоченными на то должностными лицами принимается решение о возбуждении или об отказе в возбуждении уголовного дела»[1]. Аналогичного мнения придерживаются и другие ученые: «Возбуждение уголовного дела – это самостоятельная первоначальная стадия уголовного процесса, в ходе которой компетентное должностное лицо (орган), получив первичную информацию о готовящемся или совершенном преступлении, принимает решение о возбуждении уголовного дела и начале производства по нему <…> Значение стадии возбуждения уголовного дела состоит в том, что с момента вынесения постановления о возбуждении уголовного дела создаются предпосылки для осуществления уголовного преследования и правовые основания для производства следственных и иных процессуальных действий органа дознания, следствия и суда, принятия процессуальных решений, в том числе о применении мер правоограничительного характера… Данная стадия препятствует незаконному расследованию»[2]. Кроме того, некоторые авторы утверждают, что своевременное и обоснованное возбуждение уголовных дел выполняет предупредительную и воспитательную функции, «поскольку способствует укреплению убежденности населения в неотвратимости наказания, справедливости законодательства, надлежащем уровне борьбы с преступностью, надежности защиты правоохранительными органами интересов граждан и государства от преступных посягательств»[3].

С криминалистической точки зрения стадия возбуждения уголовного дела представляет собой деятельность правоохранительных органов по сбору, анализу и оценке информации о преступном событии,

[1] Лебедев В. М. Уголовно-процессуальное право: учебник. М.: Юрайт, 2012. С. 426.

[2] Уголовный процесс: учебник: в 3 ч. Ч. 2. Досудебное производство по уголовным делам / под ред. В. Г. Глебова, Е. А. Зайцевой. 5-е изд., перераб. и доп. Волгоград: Волгоградская академия МВД России, 2017. С. 3, 5.

[3] Возбуждение уголовного дела. URL: https://yandex.ru/turbo/be5.biz/s/pravo/u-034/10.html (дата обращения: 10.08.2021).

которая включает в себя выявление, сбор и исследование сведений о следах – отражениях преступного события, оценку и использование данных, указывающих на признаки преступления[1].

По мнению М. Р. Кангезова, на стадии возбуждения уголовного дела подлежат выяснению многие аспекты, от которых зависят правильность и эффективность его рассмотрения. Прежде всего, уточняются повод и основание возбуждения уголовного дела, место совершения преступления, его квалификация и подследственность, лицо, совершившее преступление; выявляется круг лиц, вовлеченных в уголовный процесс по определенному уголовному делу; в процессуальном порядке проводится проверка заявлений и сообщений о преступлении; выносятся решения[2].

В случае с хищениями электронных денежных средств больше всего вопросов вызывает место совершения преступления, соответственно, территориальность его расследования. В постановлении Пленума Верховного Суда Российской Федерации «О судебной практике по делам о мошенничестве, присвоении и растрате» от 27 декабря 2007 г. № 51 содержалось указание на момент, когда преступление считалось оконченным: «…когда… имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность (в зависимости от потребительских свойств этого имущества) пользоваться или распорядиться им по своему усмотрению»[3], – что создавало правовую неопределенность и передачу материалов предварительных проверок по территориальности. Сотрудники следственных подразделений направляли их в те субъекты Российской Федерации, где якобы работал мобильный номер, с которого звонили мошенники, или был открыт счет, куда поступили деньги. При этом все они возвращались по месту их регистрации и уголовные

[1] См.: Криминалистическая сущность стадии возбуждения уголовного дела. URL: https://lawbook.online/kriminalisticheskaya-taktika/kriminalisticheskaya-suschnost-stadii-80428.html (дата обращения: 10.08.2021).

[2] См.: Кангезов М. Р. Проблемы доказывания на стадии возбуждения уголовного дела // Пробелы в российском законодательстве. 2018. № 4. С. 323.

[3] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. № 51 (утратило силу). URL: https://base.garant.ru/products/ipo/prime/doc/1685377/ (дата обращения: 10.08.2021).

дела возбуждались именно там. Разумеется, данные обстоятельства затягивали сроки осуществления предварительных проверок и влекли за собой несвоевременное вынесение соответствующих решений. Отдельные авторы обращали внимание на подмену понятий в тексте постановления (с этим нужно согласиться) и подчеркивали, что здесь «разъясняется уголовно-правовой аспект – момент, с которого мошенничество считается оконченным, а не место совершения или окончания преступления. …указанные пункты[1] постановления не могут являться основанием для направления материала проверки по мошенничеству… по территориальности и ссылка на них в постановлениях, оформляющих решение, недопустима»[2].

Далее названное постановление Пленума Верховного Суда Российской Федерации было признано утратившим силу, в действие вступило постановление Пленума Верховного Суда Российской Федерации «О судебной практике по делам о мошенничестве, присвоении и растрате» от 30 ноября 2017 г. № 48, где опять-таки в качестве момента окончания мошенничества, совершенного в отношении безналичных, в том числе электронных, денежных средств указывался момент «изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб»[3]. Такой подход Пленума сочли «революционным»: в связи с тем что момент окончания преступления был перенесен на более раннюю стадию (по сути, подозреваемый не достиг своей корыстной цели), начали возникать вопросы об отграничении покушения на мошенничество в сфере компьютерной информации от других смежных составов; неясной оказалась роль лица, на счет которого поступили похищен-

[1] Речь идет о пп. 4 и 12 постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о мошенничестве, присвоении и растрате» от 27 декабря 2007 г. № 51.

[2] Самойлов П. А. К вопросу об основаниях для направления по территориальности материалов доследственных проверок на примере мошенничеств с использованием средств сотовой связи и Интернета // Вектор науки ТГУ. Серия: Юридические науки. 2017. № 3 (30). С. 48.

[3] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48. URL: https://base.garant.ru/products/ipo/prime/doc/71723288 (дата обращения: 10.08.2021).

ные деньги; встала проблема определения территориальной подследственности и подсудности уголовного дела. При обсуждении проекта постановления Пленум посчитал, что местом совершения цифрового хищения является место фактического нахождения виновного лица в момент совершения противоправных действий, что, однако, не нашло отражения в итоговом документе[1].

На практике ситуация осталась прежней. Так, в обзоре Генеральной прокуратуры Российской Федерации о состоянии законности при противодействии преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, в том числе сети Интернет, за первое полугодие 2021 г. отмечается: «…поступившие сообщения о преступлениях зачастую без достаточных оснований направляются между территориальными подразделениями ОВД по месту расположения банка, в котором открыт счет потерпевшего, злоумышленника или проводилось снятие наличных. При этом не учитывается, что указанные обстоятельства не позволяют достоверно определить место совершения неочевидного преступления, поскольку не раскрывают всех обстоятельств его объективной стороны. К примеру, подразделениями полиции ГУ МВД России по г. Москве заявления о мошенничестве с использованием интернет-ресурсов, поступившие от З., И., М., М., М., Ш., вместо принятия безотлагательных мер к возбуждению уголовных дел переданы по подследственности в территориальные ОВД Республики Коми, Московской, Новосибирской областей и Кемеровской области – Кузбасса»[2]. В случае с хищениями электронных денег такие действия недопустимы, поскольку отнимают слишком много времени, соответственно, дают злоумышленникам возможность скрыть следы преступления, а также затягивают сроки осуществления предварительных проверок и в целом противоречат принципу разумности процессуальных сроков.

[1] См.: Забейда А., Данилов Д. Исключить ст. 159.6 УК. Вопросы цифрового хищения в новом постановлении Пленума ВС о судебной практике по делам о мошенничестве. URL: https://www.advgazeta.ru/mneniya/isklyuchit-st-159-6-uk/ (дата обращения: 10.08.2021).

[2] О состоянии законности при противодействии преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, в том числе сети Интернет: обзор Генеральной прокуратуры Российской Федерации за первое полугодие 2021 г.

Наконец, 29 июня 2021 г. в постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 были внесены изменения, теперь «*местом окончания мошенничества* (выделено нами – С. Г.), состоящего в хищении безналичных денежных средств, является место нахождения подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета»[1]. Исходя из ст. 126 Конституции Российской Федерации[2], данное указание следует принимать во внимание, прежде всего, судам при определении территориальной подсудности. Что касается места возбуждения уголовного дела, не стоит забывать о том, что нередки случаи, когда потерпевший проживает в одном регионе, а учет денег ведется в другом, поэтому сотрудникам органов внутренних дел при поступлении сообщения (заявления) о хищении электронных денежных средств нужно в первую очередь ориентироваться на приказ МВД России «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений» от 3 апреля 2018 г. № 196, подп. 1.2 которого предписывает руководителям территориальных органов МВД России обеспечить принятие решения о возбуждении уголовного дела в органе внутренних дел Российской Федерации, куда поступило сообщение о преступлении, при наличии достаточных данных, указывающих на признаки преступлений, предусмотренных ст. 158, 159–159.3, 159.5, 159.6 Уголовного кодекса Российской Федерации, совершенных с использованием платежных карт, средств мобильной связи и информационно-телекоммуникационной сети Интернет. В свою очередь, подп. 1.4 того же приказа гласит, что направление уголовного дела в порядке, предусмотренном ст. 152 УПК РФ[3], возможно только после получения достаточных доказательств о совер-

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (с изм., внесенными постановлением Пленума от 29 июня 2021 г. № 22). URL: https://base.garant.ru/71823288 (дата обращения: 10.08.2021).

[2] См.: Конституция Российской Федерации (принята всенар. голосованием 12 декабря 1993 г. с изм., одобренными в ходе общерос. голосования 1 июля 2020 г.). URL: www.consultant.ru (дата обращения: 10.08.2021).

[3] Место производства предварительного расследования.

шении преступления на территории обслуживания другого территориального органа МВД России и выполнения всех необходимых процессуальных действий по месту возбуждения уголовного дела[1]. Из изложенного вытекает, что безосновательное направление материалов предварительной проверки факта хищения электронных денег по территориальности является прямым нарушением приказа МВД России и влечет за собой дисциплинарную ответственность.

Итак, главная задача стадии возбуждения уголовного дела заключается в сборе достаточных данных, указывающих на признаки преступления. В случае с хищениями электронных денежных средств обязательным из них будет причинение собственнику материального ущерба. Чтобы установить, имел ли место он и иные признаки (обман или злоупотребление доверием, если речь идет о мошенничестве, наличие умысла и т. д.), необходимо не только тщательно изучить источники информации, но и использовать специальные знания в целях определения характера события и восстановления недостающих элементов, а также организовать взаимодействие с кредитными организациями, которое приобретает особую актуальность в связи с тем, что похищенные электронные денежные средства для сокрытия следов преступления часто переводятся банковским блиц-переводом на один или несколько счетов, а затем обналичиваются (анализ уголовных дел и судебных решений показал, что это наблюдается в 68 % случаев).

Естественно, что принятие решения о возбуждении уголовного дела тесно связано с объемом поступившей информации и ее источником. Исходя из этого на этапе предварительной проверки сообщения о хищении электронных денежных средств можно выделить следующие типовые ситуации:

1) сведения о преступлении получены от потерпевшего или из иных неофициальных источников, информации для принятия законного и обоснованного решения недостаточно;

[1] См.: О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений: приказ МВД России от 3 апреля 2018 г. № 196. URL: https://43.xn--b1aew.xn--p1ai/Moni/item/13373340 (дата обращения: 10.08.2021).

2) сведения о преступлении получены в результате оперативно-разыскной деятельности, информации для принятия законного и обоснованного решения достаточно.

В первой из них Н. И. Малыхина, С. В. Кузьмина рекомендуют придерживаться приведенного далее алгоритма:

– получить объяснение от заявителя и лиц, указанных в первичной информации в качестве очевидцев;

– истребовать выписку о движении денежных средств со счета потерпевшего;

– провести осмотр места происшествия, компьютерных и иных устройств с привлечением специалистов в области информационных технологий для выявления и фиксации данных, свидетельствующих о совершении преступления[1].

Однако на практике реализация перечисленных действий сопровождается рядом трудностей. Анализ материалов, поступивших из ГУ МВД России по Волгоградской области, ГУ МВД России по Ростовской области, МВД России по Республике Ингушетия, МВД России по Кабардино-Балкарской Республике, МВД России по Карачаево-Черкесской Республике, позволил выявить здесь несколько важных проблем:

1) довольно часто невозможно принять решение о возбуждении уголовного дела по причине отсутствия информации о движении денежных средств по счетам, поскольку заявители нередко не имеют представления об их списании за длительное неиспользование электронного кошелька, платные подписки и т. д. Соответственно, в подобных обстоятельствах нет признаков состава преступления;

2) отсутствует оперативность в получении судебных решений по указанным материалам, а также в направлении запросов операторам сотовой связи и платежных систем для установления данных абонентов и преступников, мест их расположения на момент совершения уголовно наказуемых деяний, поскольку не принято решение о возбуждении уголовного дела;

3) большинство хищений электронных денежных средств совершается дистанционно жителями иных субъектов Российской Федерации, а вся нагрузка по раскрытию таких преступлений ложится

[1] См.: Малыхина Н. И. Кузьмина С. В. Алгоритм действий следователя в типовых ситуациях расследования мошенничеств, совершенных с использованием сети Интернет // Вестник Томского государственного университета. 2021. № 462. С. 239.

на сотрудников правоохранительных органов по месту нахождения потерпевшего. В ходе командировок в другие регионы расходуются значительные материальные ресурсы, иногда в несколько раз превышающие причиненный потерпевшим ущерб, или же командировки вообще невозможны по причине несвоевременного финансирования.

Остановимся на них подробнее.

Подпункт 1.1 приказа МВД России «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений» от 3 апреля 2018 г. № 196 налагает на руководителей территориальных органов МВД России обязанность проведения проверки сообщения о преступлениях, предусмотренных ст. 158, 159–159.3, 159.5, 159.6 Уголовного кодекса Российской Федерации, совершенных с использованием платежных карт, средств мобильной связи и информационно-телекоммуникационной сети Интернет, в ходе которой им надлежит направлять в установленном порядке запросы в кредитные организации, операторам связи, оказывающим услуги связи, в том числе по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети Интернет[1]. В то же время ч. 4 ст. 13 Федерального закона «О полиции» гласит: «Требования (запросы, представления, предписания) уполномоченных должностных лиц полиции, предусмотренные пунктами 4, 12, 17, 21, 22, 27 части 1 настоящей статьи, обязательны для исполнения всеми государственными и муниципальными органами, организациями, должностными лицами и иными лицами в сроки, установленные в требовании (запросе, представлении, предписании), но не позднее одного месяца с момента вручения требования (запроса, представления, предписания)»[2], т. е. здесь указан предельный срок исполнения требований сотрудников полиции – 30 дней, что, однако, не отменяет сроков, прописанных в иных актах. К сожалению, на практике этому не придается должного значения, как следствие, время получения ответов от кредитных организаций и операторов

[1] См.: О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений: приказ МВД России от 3 апреля 2018 г. № 196. URL: https://43.xn--b1aew.xn--p1ai/Moni/item/13373340 (дата обращения: 10.08.2021).

[2] О полиции: федер. закон от 7 февраля 2011 г. № 3-ФЗ. URL: www.consultant.ru (дата обращения: 11.08.2021).

сотовой связи составляет 30 и более дней. В случае с электронными денежными средствами данный срок является критическим, поскольку скорость расчетов ими и их перевода высока: в соответствии с ч. 10 ст. 7 Федерального закона «О национальной платежной системе» от 27 июня 2011 г. № 161-ФЗ «перевод электронных денежных средств… осуществляется путем одновременного принятия оператором электронных платежей средств распоряжения клиента, уменьшения им остатка электронных денежных средств плательщика и увеличения им остатка электронных денежных средств получателя средств на сумму перевода электронных денежных средств»[1], – т. е. *незамедлительно* после принятия оператором распоряжения клиента, если иное не прописано в договоре. Согласно ч. 11 ст. 7 комментируемого федерального закона «перевод электронных денежных средств с использованием предоплаченной карты осуществляется в срок не позднее трех рабочих дней после принятия оператором электронных платежных средств распоряжения клиента, если более короткий срок не предусмотрен договором…»[2]. Вывод похищенных денег, как правило, осуществляется в первые часы после перевода через электронные кошельки или банковские счета, оформленные на подставных лиц – «заливщиков». При этом похищенные средства обычно дробятся на не несколько мелких сумм и выводятся через десятки счетов. Кроме того, для сокрытия следов деньги перед обналичиванием могут пересылаться по цепочке несколько раз. Приведем пример.

ДД.ММ.ГГГГ около <данные изъяты> минут, З., находясь на законных основаниях в <адрес>, действуя тайно, умышленно, из корыстных побуждений, в целях хищения электронных денежных средств со счета QIWI кошелька № Потерпевшей, используя сотовый телефон с подключением к сети Интернет, создал временный аккаунт на сайте <данные изъяты>. Имея доступ к аккаунту на сайте <данные изъяты>, ранее созданному и сохраненному Потерпевшей, зная о том, что счет QIWI кошелька № Потерпевшей привязан к сайту <данные изъяты>, имея единый умысел, ДД.ММ.ГГГГ в <данные изъяты> тайно похитил электронные денежные средства в сумме 350 руб., ДД.ММ.ГГГГ в <данные изъяты> тайно похитил

[1] О национальной платежной системе: федер. закон от 27 июня 2011 г. № 161-ФЗ (ред. от 02.07.2021). URL: www.consultant.ru (дата обращения: 10.08.2021).

[2] Там же.

электронные денежные средства в сумме 350 руб., ДД.ММ.ГГГГ в 03 ч 45 мин тайно похитил электронные денежные средства в сумме 700 руб., ДД.ММ.ГГГГ в 04 ч 03 мин тайно похитил электронные денежные средства в сумме 172 руб., всего на общую сумму 1 572 руб., осуществив их перевод со счета QIWI кошелька № Потерпевшей на счет временного аккаунта на сайте <данные изъяты>, после чего указанные электронные денежные средства со счета временного аккаунта на сайте <данные изъяты> перевел на счет № принадлежащей ему карты ПАО «Сбербанк». Затем З. скрылся с места происшествия и распорядился похищенными средствами по своему усмотрению[1].

Сказанное в очередной раз подтверждает необходимость заключения соглашений между правоохранительными органами, кредитными организациями и операторами сотовой связи об оперативном обмене информацией в электронном виде, где будут четко прописаны сроки исполнения требований первых. Сегодня в ряде субъектов Федерации это уже реализовано с ПАО «Сбербанк» и ВТБ. Так, в Республике Марий Эл для взаимодействия с ПАО «Сбербанк» используется система удаленного доступа «SBERSIGN», позволяющая в течение семи дней получить информацию об открытых счетах клиента, движении денежных средств, подключении дистанционных банковских услуг и привязанных к картам номерах телефонов. В Кабардино-Балкарской Республике банк в случаях и порядке, установленных в законодательстве Российской Федерации, предоставляет по запросу органов внутренних дел имеющиеся в его распоряжении документы (и сформированные в электронном виде, и полученные с использованием сканирующих устройств), отчеты по банковским картам за период с указанием места проведения операции, подключение услуг удаленных каналов обслуживания, источник зачисления/списания денежных средств, иные документы, предоставление которых предусмотрено законодательством Российской Федерации. Срок исполнения требования составляет 7–30 календарных дней. Однако, полагаем, что в соглашениях об обмене информацией в электронном виде он должен быть сокращен до одного–трех кален-

[1] См.: Приговор Центрального районного суда г. Оренбурга № 1-395/2019 от 24 сентября 2019 г. по делу № 1-395/2019. URL: https://sudact.ru/regular/doc/vmW1-hq3bpkH/&page...80%D0%B5%D0%B4%D1%8 (дата обращения: 12.08.2021).

дарных дней. Это позволит не затягивать времени, отведенного законодателем на предварительную проверку сообщения о преступлении. Отметим, что ранее именно *в течение трех суток* QIWI Банк должен был предоставлять информацию сотрудникам органов внутренних дел. За данный период правоохранители могли получить сведения о владельце QIWI кошелька и произведенных им транзакциях.

Считаем также необходимым установить ответственность кредитных организаций за непредоставление информации в указанный в соглашении срок (например, в виде штрафа), поскольку несвоевременные ответы банков на запросы сотрудников органов внутренних дел часто приводят к отказу в возбуждении уголовных дел и, как следствие, к безнаказанности виновных.

Соглашения об обмене информацией в электронном виде нужно заключать и с операторами платежных систем: именно они могут предоставить сведения об IP-адресе администрирования WM идентификатора[1] и по прикрепленному кошельку данные о транзакциях, сведения, которые пользователь указал о себе при регистрации (адрес электронной почты, номер мобильного телефона и т. д.), ее дату и время. Операторы платежных систем обычно хранят сведения о доступе за последние 2–3 месяца. Срок исполнения требований правоохранителей и в этом случае не должен превышать трех календарных дней.

Заместитель Министра внутренних дел Российской Федерации – начальник Следственного департамента МВД России С. Н. Лебедев отмечает: «…максимальная скорость обмена информацией между правоохранительными органами и банковскими учреждениями, операторами сотовой связи и интернет-провайдерами сегодня могла бы существенно повлиять на эффективность расследования таких преступлений и своевременное установление личности преступников. В настоящее время для следователя существует крайне заформализованный механизм получения информации… Он осуществляет первоначальный сбор доказательств, достаточных для обращения в суд с соответствующим ходатайством, подготовку документов

[1] WM идентификатор – это 12-значная цифровая последовательность, определяющая личный адрес пользователя, к которому прикрепляются кошельки и другие финансовые инструменты.

и самого ходатайства, получение судебного решения, направление его в учреждение для исполнения. В случае многоступенчатой схемы хищения такой круг повторяется неоднократно… При проведении работы по раскрытию и расследованию преступлений правоохранители должны получать необходимую информацию максимально быстро, в идеале – онлайн. К примеру, сегодня у Центрального банка для обнаружения и закрытия так называемых фишинговых сайтов уходит три дня, но и этого недостаточно»[1].

Вполне закономерно возникает вопрос об уклонении кредитных организаций от сотрудничества с правоохранительными органами, что иногда мы наблюдаем не только в нашей стране, но и за рубежом[2]. Согласно письму МВД России «О рассмотрении обращения» от 16 августа 2021 г. № 3/217716140559: «В ходе проработки вопросов организации обмена информацией в электронном виде с кредитно-финансовыми учреждениями большинство из них отказались от заключения соглашений по причинам правового и (или) технического характера. В целом неготовность организаций к заключению соглашений с МВД России связана с отсутствием норм законодательного закрепления обязанности осуществлять информационное взаимодействие в электронном виде и применением различных подходов к организации обмена информацией»[3]. К сожалению, решить данный вопрос средствами криминалистики нельзя, однако стоит сказать о том, что сегодня объективно назрела потребность в нормативном закреплении алгоритма взаимодействия правоохранительных органов с кредитными организациями. Полагаем, законодателю нужно

[1] Сергей Лебедев: в виртуальном мире не выстроены барьеры для преступников. URL: https://ria.ru/20210820/kibermoshennichestvo-1746425415.html (дата обращения: 01.09.2021).

[2] Исследование, проведенное доцентом Университета Лаваля С. Куртуа и профессором Университета Лаваля И. Жендроном, показало, что все чаще компании ведут борьбу с мошенничеством самостоятельно, поскольку, по их мнению, цель полиции – наказать мошенника, а не вернуть деньги, кроме того, у нее не хватает технических ресурсов и знаний для противодействия злоумышленникам, чьи схемы год от года становятся сложнее. См.: Куртуа С., Жендрон И. Почему бизнес предпочитает наказывать мошенников самостоятельно. URL: https://hbr-russia.ru/management/korporativnyy-opyt/834473 (дата обращения: 12.08.2021).

[3] О рассмотрении обращения: письмо МВД России от 16 августа 2021 г. № 3/217716140559. URL: https://www.garant.ru/products/ipo/prime/doc/402538962 (дата обращения: 12.08.2021).

сосредоточить здесь максимум своего внимания, поскольку количество мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий увеличивается, а их раскрываемость оставляет желать лучшего.

Рассмотрим еще одну проблему: нередко кредитная организация не дает сотрудникам следственных подразделений выписки по счету, ссылаясь на положения Федерального закона «О банках и банковской деятельности» от 2 декабря 1990 г. № 395-1, согласно которому может быть предоставлена только информация о наличии или об отсутствии счета, а не об операциях по нему[1]. В этой ситуации чаще всего следователи направляют в отдел (отделение) уголовного розыска поручение на проведение оперативно-разыскного мероприятия (ОРМ) «Наведение справок» или сам материал предварительной проверки, чтобы было получено судебное решение, на основании которого кредитная организация предоставит нужную выписку. Однако данные действия занимают определенное время и затягивают сроки осуществления предварительной проверки и вынесения решения о возбуждении уголовного дела либо об отказе в его возбуждении. В ряде субъектов Федерации, например в Воронежской области, удалось сформировать практику, когда проведение предварительной проверки по заявлениям о хищениях денежных средств со счетов граждан поручается следователю или дознавателю. Используя возможности УПК РФ, они получают всю нужную информацию в банках и компаниях сотовой связи без проведения оперативно-разыскных мероприятий. Здесь важно отметить, что срок исполнения запросов устанавливается следователем (дознавателем) и составляет не более пяти–семи дней. Таким образом, к моменту принятия решения о возбуждении уголовного дела в материалах проверки уже имеются все необходимые ответы. «Областной суд… практику поддержал. В отличие от ходатайств о разрешении на проведение ОРМ инициаторами которых выступают оперативные сотрудники, правом обращения с ходатайством о даче разрешений на производство отдельных следственных действий, то есть в порядке, установлен-

[1] См.: О банках и банковской деятельности: федер. закон от 2 декабря 1990 г. № 395-1. URL: https://base.garant.ru/10105800 (дата обращения: 12.08.2021).

ном статьей 165 УПК РФ[1], наделены дознаватели – с согласия прокурора и следователи – с согласия руководителя следственного органа. При этом такое обращение в суд возможно и до возбуждения уголовного дела»[2]. Считаем, что этот опыт необходимо распространить и на иные регионы страны.

Не менее важной является проблема взаимодействия правоохранительных органов разных стран, поскольку преступление может совершаться на территории одной страны, а преступник находиться в другой. По мнению Е. С. Шевченко, «сложности сотрудничества по расследованию и раскрытию киберпреступлений с правоохранительными органами иностранных государств усугубляются тем, что в действующих законодательствах разных стран установлены свои нормы в отношении компьютерных преступлений, выработаны свои подходы к назначению и производству компьютерных экспертиз»[3]. Примерно об этом же говорили участники Европейской комиссии. По их мнению, шанс обнаружения киберпреступников крайне низок. Причины сложившейся ситуации они видят в отсутствии обмена информацией между странами, различных возможностях для проведения расследования и судебных экспертиз, несогласованном сотрудничестве между правоохранительными органами и другими участниками, обладающими ценной информацией о совершенных преступлениях (провайдерами платежных систем и сотовой связи)[4].

Согласно материалам, поступившим из следственных подразделений, отсутствие взаимодействия между правоохранительными органами влечет за собой трудности в установлении данных:

– соединения о прохождении вызова от абонента IP-телефонии, использующего VPN-сервисы и адресное пространство операторов связи и интернет-провайдеров стран, не поддерживающих международное сотрудничество правоохранительных органов;

---

[1] Судебный порядок получения разрешения на производство следственного действия.

[2] Зарубина Е., Ивлиева Н. Получить ответ непросто // Полиция России. 2021. № 1. С. 42.

[3] Шевченко Е. С. Тактика производства отдельных следственных действия при расследовании киберпреступлений: дис. … канд. юрид. наук. М., 2016. С. 35.

[4] См.: Frequently Asked Questions: the new European Cybercrime Centre. URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_12_221 (дата обращения: 05.10.2020).

– владельцев доменных имен, зарегистрированных в странах, не поддерживающих международное сотрудничество правоохранительных органов;

– об электронных платежах, совершаемых с использованием интернет-ресурсов по технологии «card2card», а также платежных систем и банковских карт банков-эмитентов, находящихся на территории стран, не поддерживающих международное сотрудничество правоохранительных органов;

– пользователей социальных сетей, использующих VPN-сервисы и адресное пространство операторов связи и интернет-провайдеров стран, не поддерживающих международное сотрудничество правоохранительных органов.

Препятствием для взаимодействия России с иными государствами в сфере борьбы с киберпреступностью является Конвенция Совета Европы о киберпреступности 2001 г., к которой наша страна не присоединилась. Причиной послужили положения п. «b» ст. 32: «Сторона может без согласия другой Стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным и получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему»[1], – которые создают угрозу суверенитету России. Однако в сфере обеспечения кибербезопасности наша страна активно сотрудничает с государствами – участниками Содружества Независимых Государств, Организации Договора о коллективной безопасности, БРИКС др. В целях его укрепления, полагаем, нужно не только совершенствовать законодательство, но и привести к единообразию методики производства компьютерно-технических судебных экспертиз, которые сегодня отличаются не только в разных странах, но и в разных ведомствах в пределах одного государства. Здесь еще раз подчеркнем важность использования специальных знаний на стадии возбуждения уголовных дел, поскольку в условиях научно-технического прогресса многие преступления можно обнаружить только благодаря им. Приведем пример.

[1] CETS 185 – Convention on Cybercrime. URL: rm.coe.int (дата обращения: 12.08.2021).

На этапе предварительной проверки по факту хищения чужого имущества (неустановленное лицо ввело в заблуждение Ш. и получило от нее денежные средства на свой банковский счет) была проведена компьютерно-техническая судебная экспертиза. У Ш. изъят ноутбук модели <…> серийный номер <…>, с помощью которого она общалась с неизвестным лицом. Перед экспертом поставлены следующие вопросы:

1. Какие программы с вредоносным кодом или для удаленного управления устройствами установлены и использовались на предоставленном объекте?

2. Имеются ли следы перевода денежных средств, общения с какими-либо представителями финансовых структур и т. п. на данном ноутбуке?

В результате экспертизы было установлено, что на представленном на исследование ноутбуке вредоносных кодов (вирусов, троянов и др.) с возможностями доступа к онлайн-сервисам банковских систем не обнаружено. Однако имеются следы использования программы «AnyDesk» (дата создания <…>, обновлено <…>), предназначенной для удаленного управления устройством после получения цифрового кода генерируемого программой, а также следы получения сообщений посредством электронной почты <…> с представителями брокерской конторы «CFXpoint» <…>, в частности рекомендации по установке программы «AnyDesk», запрос копии паспорта, подтверждение перевода депозита. Для справки эксперт указал, что согласно информации, размещенной в сети Интернет, брокерская контора «CFXpoint» является ресурсом для проведения мошеннических операций с пользователями путем введения в заблуждение относительно своих намерений (обмана) под видом участия в купле-продаже на фондовых рынках «Forex»[1]. Справочный материал найден экспертом в глобальной сети и принят во внимание следователем.

Стоит сказать, что сегодня в Интернете в свободном доступе размещен ряд ресурсов, которые могут оказать сотрудникам правоохранительных органов помощь на стадии возбуждения уголовного дела и первоначальном этапе расследования (о них речь пойдет в параграфе 2.2). По словам О. Б. Дроновой, К. В. Проваторовой, А. А. Сапу-

[1] По материалам МВД России по Кабардино-Балкарской Республике.

хина, ими не следует пренебрегать при осуществлении сбора информации о механизме совершенного преступления, личности преступника и его местонахождении[1], но при этом помнить о возможных неточностях таких сведений. Разумеется, эти ресурсы носят ориентирующий характер и требуют проверки. Однако заметим, что практике известны случаи, когда подобная информация была признана вещественным доказательством по уголовному делу. Так, ДД.ММ.ГГГГ в неустановленное время у Ч., находящегося по адресу своего проживания <адрес>, в целях незаконного завладения денежными средствами граждан возник преступный умысел, направленный на совершение мошеннических действий в сети Интернет. Осуществляя задуманное, Ч., не желая выполнять взятых на себя обязательств и не имея такой реальной возможности, предлагал в сети Интернет свои посреднические услуги при выдаче кредитов и займов до 6 000 000 руб. на основании расписок с перечислением денежных средств в любые регионы России, при этом просил за свои услуги денежное вознаграждение, которое требовалось перечислить на указанный им QIWI кошелек. Для продвижения своих услуг Ч. размещал на бесплатных и общедоступных информационных ресурсах сети Интернет объявления соответствующего содержания, а также осуществлял массовую рассылку электронных писем на случайные электронные адреса в целях привлечения потенциальных заемщиков. Далее Ч., продолжая свою преступную деятельность, направленную на незаконное обогащение и завладение денежными средствами граждан, создал интернет-сайт по продаже телевизоров и ноутбуков, поставляемых из Китая, где разместил каталог с техникой, которую он якобы продает по цене, ниже рыночной <…> В результате противоправных действий Ч. потерпевшим был причинен ущерб на суммы 5 000 руб., 9 000 руб., 14 500 руб., 6 000 руб., 34 600 руб. В числе вещественных доказательств по данному уголовному делу суд среди прочего указал сведения с сервера «Whois», полученные в рамках предварительной проверки[2].

[1] См.: Дронова О. Б., Проваторова К. В., Сапухин А. А. Интернет-ресурсы, используемые в процессе информационного обеспечения раскрытия и расследования мошенничеств, совершенных с использованием средств мобильной связи и сети Интернет // Вестник Волгоградской академии МВД России. 2021. № 3 (58). С. 139–140.

[2] См.: Приговор Волжского городского суда (Волгоградская область) № 1-998/2016 по делу № 1-998/2016. URL: https://sudact.ru/regular/doc/IwoDKKQidEUn/ (дата обращения: 12.08.2021).

М. Р. Кангезов считает, что процесс доказывания на стадии возбуждения уголовного дела сопровождается проблемами как объективного, так и субъективного характера[1]. Коллизии и пробелы законодательства, а также отсутствие должного взаимодействия между органами внутренних дел и кредитными организациями, правоохранительными органами разных стран относятся к первым. В числе вторых, прежде всего, стоит назвать невысокую компетенцию полицейских и небольшой опыт их работы со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов[2], о чем свидетельствует низкий процент раскрываемости анализируемых преступлений: «Производство по уголовным делам… в 75 % случаев приостанавливают за неустановлением обвиняемого, примерно 6 % уголовных дел прекращают по реабилитирующим основаниям, и только 7 % уголовных дел направляют с обвинительным заключением в суд для дальнейшего разбирательства»[3]. С точки зрения А. С. Шаталова, «…здесь как нигде высока вероятность того, что те доказательства, что все же были обнаружены, могут быть непреднамеренно изменены и даже утрачены как в результате допущенных ошибок при их фиксации или, например, изъятии, так и в ходе их исследования. Подготовка в ходе досудебного производства по уголовному делу доказательств такого рода для дальнейшего представления их в суде требует обязательного наличия не только основательной профессиональной подготовки, но и регулярного обновления имеющихся знаний у следователей, дознавателей, оперативных работников и, разумеется, у специалистов и экспертов»[4]. В случае с электронными денежными средствами ситуация усугубляется тем, что они утрачивают свойства материальных объек-

[1] См.: Кангезов М. Р. Проблемы доказывания на стадии возбуждения уголовного дела. С. 323.

[2] См.: Нестерович С. А. Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов // Вестник науки и образования. 2018. Т. 2. № 8 (44). С. 46–49.

[3] Немцева М. «Их слишком много»: почему киберпреступления остаются нераскрытыми. URL: https://iz-ru.turbopages.org/iz.ru/s/1166840/mariia-nemtceva/ikh-slishkom-mnogo-pochemu-kiberprestupleniia-ostaiutsia-neraskrytymi (дата обращения: 11.08.2021).

[4] Шаталов А. С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции // Вестник Сибирского юридического института МВД России. 2018. № 3 (32). С. 11.

тов, что, по справедливому замечанию М. В. Лелетовой, Д. В. Климова, усложняет уголовно-процессуальные возможности проведения в отношении них некоторых следственных и процессуальных действий[1].

Отсутствие в МВД России высококвалифицированных специалистов в области IT-технологий (с сожалением вынуждены констатировать это), полагаем, можно компенсировать взаимодействием органов внутренних дел с IT-компаниями, например с Лабораторией Касперского, чьи сотрудники могут привлекаться к производству следственных действий, а разработки использоваться для выявления и фиксации фактов мошенничества. Подобный опыт имеется в некоторых зарубежных странах, считаем важным обратить на него внимание. Так, в Нидерландах правоохранительные органы используют платформу Bitfury Crystal, анализирующую и выявляющую подозрительные транзакции с криптовалютой, в США – аналитическую систему криптовалютных транзакций Chainalysis и приложение CipherTrace Scout, позволяющее идентифицировать, отслеживать и документировать криминальные транзакции в полевых условиях, а также визуализировать их. Кроме того, Федеральное бюро расследований США активно применяет систему Mayhem, предназначенную для распознавания индивидуального почерка хакеров и хакерских группировок, обнаружения атак, тестирования и преследования преступников вплоть до установления их местонахождения.

В настоящее время некоторые крупные компании создают технологические решения специально для правоохранителей: еще в 2014 г. IBM презентовала «Систему обнаружения мошенничества на основе анализа взаимодействия пользователя и браузера». Ее разработчики утверждают, что каждый пользователь заходит в Интернет с определенного устройства и имеет свою линию поведения на различных сайтах, в том числе в интернет-магазинах, банках и т. д., которая сразу меняется, если в дело вступает бот или злоумышленник. В данном случае система требует дополнительной идентификации[2].

[1] См.: Лелетова М. В., Климов Д. В. Особенности возбуждения уголовного дела и первоначального этапа расследования хищений электронных денежных средств // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2014. № 3 (27). С. 124.

[2] См.: IBM получила патент на новую технологию борьбы с интернет-мошенничеством. URL: https://m/habr.com/ru/company/ibm/blog/225933 (дата обращения: 10.05.2021).

Это особенно важно с учетом того факта, что сегодня наблюдается автоматизация социальной инженерии: все чаще мошенничество совершается с помощью ботов – программ, способных по определенному алгоритму выполнять какие-либо действия, в том числе вести диалоги в социальных сетях или на форумах. А. П. Суходолов, А. М. Бычкова отмечают: «Продвинутым вариантом социальной инженерии является ситуация, когда человек, участвующий в диалоге с ботом, уверен, что общается с человеком, поскольку программа способна обратиться к пользователю-человеку и поддерживать с ним беседу, оперируя такими репликами, которые человек-собеседник сочтет естественными <…> способна оправдать ожидания человека-собеседника, она „социализирована“, ведет диалог в рамках, принятых в данном обществе, ориентирована разработчиками на побуждение человека к выполнению определенных действий, что и является критерием ее успешности»[1] и создает реальную угрозу кибербезопасности собеседника.

В подтверждение сказанного приведем мнение профессора А. С. Шаталова: «Главная криминалистическая особенность киберпреступлений заключается в том, что их предотвращение, выявление, раскрытие и расследование невозможно без использования современных информационных технологий»[2], – которые в системе МВД России сегодня только появляются[3].

---

[1] Суходолов А. П., Бычкова А. М. Математические методы и цифровые технологии в современной криминологии // Всероссийский криминологический журнал. 2018. Т. 12. № 6. С. 757–758.

[2] Шаталов А. С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции. С. 10.

[3] К 25 декабря 2021 г. МВД России планирует запустить новый модуль «Антимошенник». В техническом задании к нему сказано: «Мобильное приложение МВД России должно иметь функционал сверки локального массива телефонных номеров, хранящихся на мобильном устройстве пользователя, с массивом телефонных номеров, содержащихся в локальной системе управления базами данных зеркалирующего сервера, с последующим добавлением новых телефонных номеров или удалением неактуальных телефонных номеров из локального массива телефонных номеров, хранящегося на мобильном устройстве пользователя». Безусловным достоинством модуля является не только его способность оповещать пользователя о том, что ему звонят или пишут сообщения с номера, откуда ранее совершались противоправные действия, с последующей блокировкой, но и наличие так называемого «белого списка», который не подлежит блокировке и может пополняться пользователем самостоятельно.

В завершение параграфа подведем некоторые итоги:

1. При поступлении сообщений (заявлений) о фактах хищения электронных денежных средств сотрудникам органов внутренних дел в первую очередь необходимо руководствоваться приказом МВД России «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений» от 3 апреля 2018 г. № 196, который предписывает обеспечить принятие решения о возбуждении уголовного дела в органе внутренних дел Российской Федерации, куда поступило сообщение о преступлении, при наличии достаточных данных, указывающих на признаки преступлений, предусмотренных ст. 158, 159–159.3, 159.5, 159.6 Уголовного кодекса Российской Федерации, совершенных с использованием платежных карт, средств мобильной связи и информационно-телекоммуникационной сети Интернет, а не направлять безосновательно материал в те регионы, где ведется учет денег, со ссылкой на постановление Пленума Верховного Суда Российской Федерации «О судебной практике по делам о мошенничестве, присвоении и растрате» от 30 ноября 2017 г. № 48. Указание Пленума следует принимать во внимание судам при определении территориальной подсудности.

2. Федеральный закон «О полиции» устанавливает предельный срок исполнения требований правоохранителей – 30 дней, что не отменяет сроков, прописанных в иных документах. К сожалению, последнее положение нередко игнорируется кредитными организациями, и ответов на запросы органы внутренних дел вынуждены ждать 30 и более дней, что, естественно, затягивает время, отведенное законодателем на предварительную проверку сообщения о преступлении. В соглашениях о сотрудничестве, заключенных между подразделениями органов внутренних дел и кредитными организациями (ПАО «Сбербанк» и ВТБ), срок предоставления ответов на запросы первых составляет семь–тридцать календарных дней. Поскольку речь идет об обмене информацией в электронном виде, полагаем, его нужно сократить до одного–трех календарных дней, что в свое время было прописано в соглашении с QIWI Банком. Договоры о сотрудничестве необходимо заключить и с операторами платежных систем, срок исполнения требований правоохранителей и здесь не должен превышать трех календарных дней. Кроме того, считаем нужным установить ответственность кредитных организаций за не-

предоставление информации в указанный в соглашении срок (например, в виде штрафа) в связи с тем, что несвоевременные ответы банков на запросы сотрудников органов внутренних дел часто влекут за собой отказ в возбуждении уголовных дел и, как следствие, безнаказанность виновных.

3. Невысокую компетенцию полицейских и небольшой опыт их работы со специфическими источниками доказательственной информации, полагаем, можно компенсировать взаимодействием органов внутренних дел с IT-компаниями, как это происходит в ряде зарубежных стран.

2.2. Организационные особенности первоначального этапа расследования хищений электронных денежных средств

Деление расследования на этапы имеет своей целью расстановку акцентов на тех задачах, которые являются приоритетными для каждого из них[1]. В настоящее время в криминалистической науке утвердилась точка зрения о трехэтапной структуре расследования (первоначальный, последующий и завершающий). При этом они рассматриваются «не только как простые временные отрезки исследуемого процесса, сменяющие друг друга, а главным образом как подсистемы следственных, оперативно-разыскных, контрольно-проверочных, организационно-подготовительных и других действий, объединенных на основе единства разрешаемых с их помощью задач, обусловленных устойчивой повторяемостью типичных следственных ситуаций»[2].

В настоящем параграфе сосредоточим свое внимание на первоначальном этапе расследования, цель которого, по мнению М. В. Кардашевской, Е. С. Шипиловой, состоит в сборе достаточных доказательств, дающих основание для обвинения лица в совершении преступления[3]. Обычно данный этап носит проблемно-ситуационный характер, что в первую очередь детерминировано объемом и досто-

[1] См.: Кардашевская М. В., Шипилова Е. С. Этапы расследования преступлений и их характеристика // Таврический научный обозреватель. 2015. № 2. С. 8.

[2] Драпкин Л. Я., Карагодин В. Н. Криминалистика. С. 353.

[3] См.: Кардашевская М. В., Шипилова Е. С. Этапы расследования преступлений и их характеристика. С. 8.

верностью исходной информации. Именно от ее качества зависит содержание следственных ситуаций, выступающих фундаментом для выдвижения версий и планирования расследования.

Кроме первоначальной информации, полученной при проверке сообщений (заявлений) о преступлении, В. П. Лавров предлагает включать в число факторов, определяющих содержание следственных ситуаций, объективные условия, характеризующие получение этой информации; силы и средства, которые имеются в распоряжении следователя для дальнейшей работы по использованию исходной информации в этих условиях; позиции подозреваемого, потерпевшего, свидетелей, результаты их противодействия установлению истины в начале расследования и возможности противодействия; иные факторы, препятствующие или способствующие успешному решению криминалистических задач[1], но первостепенное значение все же имеет информация. Если говорить о расследовании преступлений, совершаемых в отношении электронных денежных средств, на основе ее содержания можно выделить такие следственные ситуации, как:

– сложная ситуация, в которой нет достаточной информации о событии преступления, необходимо установить лицо, совершившее его, а также обстоятельства по данному делу;

– простая ситуация, в которой известно событие преступления и лицо, совершившее его, и нужно установить обстоятельства по данному делу.

С точки зрения Н. И. Малыхиной, С. В. Кузьминой, перечень следственных ситуаций необходимо дополнить еще одной: установлены способ совершения преступления, потерпевшие и свидетели, выявлены цифровые следы, имеются некоторые данные о лице, совершившем преступление, но его местонахождение неизвестно[2].

Анализ уголовных дел и материалов судебной практики свидетельствует о том, что в случае совершения хищений электронных денежных средств наиболее частыми являются сложные ситуации (54 %), среди которых выделяются проблемные, обусловленные

[1] См.: Исходные следственные ситуации и криминалистические методы их разрешения: сб. науч. тр. / отв. ред. В. П. Лавров. М.: Высшая юрид. заоч. школа, 1991. С. 7.

[2] См.: Малыхина Н. И. Кузьмина С. В. Алгоритм действий следователя в типовых ситуациях расследования мошенничеств, совершенных с использованием сети Интернет. С. 242.

семантической неопределенностью. Они всегда имеют одинаковую структуру: «совокупность неполных, недостаточных сведений, и противостоящее им неизвестное искомое, а также возникающее между этими двумя компонентами специфическое познавательное отношение логического противоречия, основанное на остром недостатке информации»[1]. По мнению А. И. Анапольской, процесс расследования здесь «усложняется дефицитом информации, прежде всего, о личности преступника и событии преступления; потребностью одновременной проверки многих следственных версий и проведением значительного количества оперативно-разыскных мероприятий и следственных действий по установлению неизвестных обстоятельств»[2]. Важно также подчеркнуть, что хищения электронных денежных средств обычно трудно привязать к конкретному географическому месту: преступник может действовать сразу в нескольких регионах одной страны или разных государствах. Приведем пример.

К. в неустановленный период, но не позднее 31 декабря 2014 г., узнав через информационно-телекоммуникационную сеть Интернет на форуме сайта <…> от неустановленного лица, зарегистрированного под именем пользователя «…@exploit.ru», информацию о преступной схеме получения прибыли путем хищения денежных средств граждан… с использованием вирусного программного обеспечения, сформировал у себя умысел, направленный на совершение таких преступных деяний.

Имея достаточные познания в области компьютерной техники и пользовании сетью Интернет, К., осознавая, что осуществление неправомерного доступа к компьютерной информации в системе ЭВМ невозможно без специальных программ, функционал которых позволит реализовать его умысел и незаконно обогатиться, находясь в Томске, вступил в преступный сговор с указанным неустановленным лицом для совместного систематического хищения денежных средств граждан по уже имеющейся у данного лица схеме с использованием вредоносного программного обеспечения.

---

[1] Драпкин Л. Я., Карагодин В. Н. Криминалистика. С. 38–39.

[2] Анапольская А. И. Типичные следственные ситуации и версии первоначального этапа расследования мошенничеств с электронными счетами // Вестник Тамбовского государственного университета. Серия: Гуманитарные науки. 2015. Вып. 8 (148). С. 134.

Неустановленное лицо должно было посредством специальных вредоносных программ… путем ввода, удаления, блокировки, модификации компьютерной информации осуществлять доступ к счетам граждан… с помощью заражения мобильных устройств потерпевших через рассылку SMS-сообщений…, после чего без ведома владельца устройства давать от имени потерпевших указание банку о переводе денег с их счетов на счета, подконтрольные К., который, в свою очередь, подыскивал лиц для оформления на их имена банковских и sim-карт. Результатом реализации этих действий стало хищение денежных средств в сумме 7 800 руб. со счета №, открытого в Благовещенске.

Позже к организованной группе присоединились еще двое лиц, которые взяли на себя функции К. по поиску граждан, на чьи имена можно регистрировать банковские и sim-карты. После этого преступники совершили хищение денежных средств в сумме 7 950 руб. со счета №, открытого в Ростове-на-Дону; хищение денежных средств в сумме 7 800 руб. со счета №, открытого в Кургане; хищение денежных средств в сумме 7 800 руб. со счета №, открытого в Перми… хищение денежных средств в сумме 7 800 руб. со счета №, открытого в Архангельске…[1].

В сложных следственных ситуациях, если хищение электронных денег было совершено в режиме реального времени (онлайн), М. В. Лелетова, Д. В. Климов рекомендуют придерживаться следующего алгоритма действий:

1. Получить от заявителя подробное объяснение об обстоятельствах хищения.

2. Установить местонахождение электронно-вычислительной техники, которая использовалась в качестве орудия преступления:

2.1. Получить сведения о движении денежных средств путем направления запроса в кредитную организацию.

2.2. Проверить полученную информацию посредством открытых интернет-сервисов.

2.3. Направить в организацию-провайдер запрос о предоставлении информации об абоненте, который работал в сети Интернет во время совершения операций с похищенными электронными денежными средствами.

[1] См.: Приговор Советского районного суда г. Томска № 1-25/2019 1-377/2018 от 9 декабря 2019 г. по делу № 1-275/2018. URL: https://sudact.ru/regular/doc/hktokOrwZgbO/&regular...D1%82%D0%B5%D1%80 (дата обращения: 09.09.2021).

3. Установить информацию о собственниках объектов недвижимости, где находится техника, с помощью которой было совершено преступление.

4. Провести в установленном порядке с участием специалиста изъятие этой техники и ее осмотр.

5. Назначить компьютерно-техническую судебную экспертизу[1].

В приведенном перечне вызывает вопросы формулировка пункта 2.2 о проверке информации на открытых интернет-сервисах. В предыдущем параграфе мы говорили, что сведения, размещенные на подобных площадках, носят вспомогательный характер и сами требуют проверки, поэтому удостоверять какую-либо информацию здесь нельзя. Однако они могут сориентировать следователя в том, какому из интернет-провайдеров или операторов сотовой связи нужно направить запрос, что тоже важно, ибо, как писал профессор Р. С. Белкин, информация ориентирующего характера полезна для выдвижения версий, определения направлений расследования, планирования следственных действий, прогнозирования возможной линии поведения участников расследования и т. п.[2]

Прежде чем обратиться к тому или иному вспомогательному сервису, нужно узнать, как было совершено хищение. Некоторые его обстоятельства можно восстановить из показаний потерпевшего (примерное время и способ совершения преступления, если речь не идет о краже денежных средств с использованием вредоносного программного обеспечения). В расследовании хищений электронных денег показания потерпевшего особенно важны, поскольку большинство способов совершения таких преступлений не предполагает очевидцев либо сотрудники органов внутренних дел сталкиваются с определенными трудностями при их установлении. Кроме того, надлежит акцентировать внимание на информации, хранящейся в устройстве потерпевшего (компьютере, смартфоне и т. д.): переписке с предполагаемым преступником в социальных сетях, электронной почте, с помощью SMS-сообщений, если она имела место, истории движения денежных

[1] См.: Лелетова М. В., Климов Д. В. Особенности возбуждения уголовного дела и первоначального этапа расследования хищений электронных денежных средств. С. 123–126.

[2] См.: Белкин Р. С. Криминалистическая энциклопедия. 2-е изд., доп. М.: Мегатрон XXI, 2000. С. 83.

средств, логах и др. Большое значение работа с устройством потерпевшего приобретает в тех случаях, когда хищение денежных средств было совершено с использованием вредоносного программного обеспечения, в том числе программ удаленного доступа: в файлах можно обнаружить коды вредоносных программ, найти следы установки программ удаленного доступа, приложения, содержащие вирусы и т. д. Естественно, этим должен заниматься человек, обладающий специальными знаниями. После того как показания потерпевшего получены, а его устройство осмотрено, стоит принять меры по деанонимизации преступника. Именно здесь можно воспользоваться открытыми интернет-ресурсами.[1]

Если *хищение электронных денег произошло путем оплаты товара в интернет-магазине*, прежде всего, следует определить хостинг-провайдера. На данный способ мы обращаем внимание в первую очередь в связи с тем, что в 2020 г. 60 % успешных мошеннических атак были совершены по сценарию продажи-покупки товаров на сайтах реальных маркетплейсов и сайтах-клонах[2]. Хостингом называется услуга по предоставлению ресурса на сервере – «аренда дискового пространства, где будут храниться все необходимые для правильного функционирования сайта файлы и данные»[3]. Помочь в этом могут интернет-сервисы «2IP.UA», «WHOIS», «Dig» и др. В поисковой строке нужно ввести доменное имя сайта (интернет-магазина), где была совершена покупка, таким образом можно узнать адрес DNS-сервера[4], а по нему – хостинг-провайдера, который, в свою очередь, в ответе на запрос сотрудников правоохранительных органов предоставит информацию о владельце сайта: данные, указанные им при регистрации, а также его IP-адрес – уникальный идентификатор устройства в сети.

---

[1] Обращение к открытым интернет-сервисам может оказать помощь и тогда, когда преступник известен, но требуется установить его местонахождение.

[2] См.: Эксперты назвали самый популярный способ мошенничества в Интернете. URL: https://www.rbc.ru/technology_and_media/09/02/2021/602184e19a794726a2165b6b (дата обращения: 09.09.2021).

[3] Хостинг: что это, зачем и как выбрать. URL: https://vc.ru/services/74241-hosting-chto-eto-zachem-i-kak-vybrat (дата обращения: 09.09.2021).

[4] Представляет собой специализированный компьютер, который хранит IP-адреса сайтов.

IP-адрес назначается интернет-провайдером, как только это происходит, первый принимает либо статическую (фиксированную), либо динамическую (меняющуюся) форму. Отметим, что большинство пользователей имеют временные IP-адреса, сменяющиеся при каждом подключении к Интернету или через определенный период. Кроме того, под одним IP в сети, построенной по протоколу IPv4 (99 % сетей в России именно такие), может находиться множество пользователей[1]. Однако интернет-провайдер сохраняет логи, благодаря которым иногда удается установить, какой абонент был связан с IP-адресом в то или иное время. Если же злоумышленник использовал для совершения преступления публичный Wi-Fi, его активность можно отследить только до данной точки доступа[2]. После выяснения, какому именно провайдеру принадлежит IP-адрес, у него нужно узнать, с кем был заключен договор об оказании услуг связи. Здесь могут возникнуть трудности с доказыванием того, что именно это лицо использовало техническое устройство для совершения неправомерных действий. IP-адрес также может быть зарегистрирован на территории другого государства. О. А. Науменко отмечает: «Свободный и несложный способ использования зарубежных IP-адресов, серверов и ресурсов (например, серверов почтовых ящиков @google.com, @yahoo.com, @aol.com), находящихся вне юрисдикции РФ, практически полностью исключает возможность получения необходимой информации сотрудниками МВД России. Поэтому серьезным препятствием в расследовании преступлений данной категории является отсутствие у России договоров с некоторыми иностранными государствами об оказании правовой помощи в расследовании уголовных дел»[3], – что возвращает нас к проблеме взаимодействия правоохранительных органов различных государств, которую мы рассматривали в параграфе 2.1.

---

[1] См.: Как узнать IP-адрес чужого компьютера и есть ли в этом смысл. URL: https://compconfig.ru/net/kak-uznat-ip-adres-chuzhogo-kompyutera.html (дата обращения: 12.08.2021).

[2] См.: Могут ли правоохранительные органы действительно отследить кого-то по IP-адресу. URL: https://guidepc-ru/turbopages.org/turbo/guidepc.ru/s/articles/mogut-li-pravoohranitelnye-organy-dejstvitelno-otsledit-kogo-to-po-ip-adresu/ (дата обращения: 09.09.2021).

[3] Науменко О. А. Проблемы в расследовании уголовных дел о мошенничестве, совершенном с использованием информационно-телекоммуникационной среды // Вестник Краснодарского университета МВД России. 2019. № 3 (45). С. 62.

IP-адрес, а также MAC-адрес[1] будут важны и в тех ситуациях, когда имел место перевод денежных средств на счет оператора электронных денег (оплата товара или услуги, предлагаемых на площадках объявлений, в социальных сетях и т. д.). Заметим, что MAC-адрес часто называют физическим адресом, поскольку он присваивается устройству изготовителем и раскрывается при включенном Wi-Fi-модуле. Благодаря этому выстраиваются популярные маршруты, формируются данные о времени и регулярности посещений тех или иных сайтов. «Информация о геопозиционировании, перемещениях и пользовательском портрете (пол, возраст, интересы и т. д.) владельцев MAC-адресов собирается на таких рекламных площадках, как: Яндекс.-Аудитории, myTarget, Facebook, Instagram, Вконтакте, Одноклассники, Mail.ru»[2]. Узнать MAC-адрес можно по IP-адресу, однако устройства должны быть подключены к одной сети. Если MAC-адрес девайса известен, установить его местоположение можно посредством обращения, например, к интернет-сервису https://wingle.net/. Но заметим, что MAC-адрес сетевой карты может быть изменен.

Если *злоумышленник позвонил жертве по телефону и посредством приемов социальной инженерии убедил ее перевести деньги*, следами преступления будут абонентский номер, с которого звонили потерпевшему; сведения об операторе сотовой связи и регионе, где зарегистрирован этот номер; данные о соединениях абонентского номера, базовой станции, IMEI-коде; информация о владельцах абонентских номеров, зарегистрированных во время совершения преступления в сети. Абонентский номер останется в журнале вызовов на телефоне потерпевшего. Установить его принадлежность к оператору сотовой связи и региону можно путем обращения к таким сайтам, как www.spravportal.ru, https://region-operator.ru/, https://codificator.ru/ и др., либо в личном кабинете абонента сотовой связи (для этого у оператора сотовой связи нужно запросить детализацию расходов за определенный период (она тут же будет направлена на электронную почту потерпевшего), где отразятся номер абонента, который звонил, регион и оператор (рис. 1)).

[1] Уникальный идентификатор (шестибайтный номер), который присваивается сетевой карте любого устройства, способного подключаться к сети Интернет.

[2] Отслеживание людей по MAC-адресу их гаджетов. URL: https://camslider.ru/-otslezhivanie-ljudej-po-mac-adresu-ih-gadzhetov/ (дата обращения: 09.09.2021).

24 сен 2021 Пт, 20:43:37	Входящее SMS --	VTB	-	Основной баланс	0,00 руб.	0,00 руб.
24 сен 2021 Пт, 17:42:47	Входящий звонок с Теле2 (Волгоградская обл.)	+7 902 382-78-65	3 мин 51 сек	Основной баланс	0,00 руб.	656,45 руб.
24 сен 2021 Пт, 17:19:55	Входящий звонок с Теле2 (Волгоградская обл.)	+7 902 382-78-65	8 сек	Основной баланс	0,00 руб.	656,45 руб.
24 сен 2021 Пт, 16:30:30	Входящий звонок с Теле2 (Волгоградская обл.)	+7 902 381-42-06	1 мин 33 сек	Основной баланс	0,00 руб.	656,45 руб.
24 сен 2021 Пт, 13:53:16	Входящий звонок с МегаФон (Волгоградская обл.)	+7 937 540-16-10	1 мин 17 сек	Основной баланс	0,00 руб.	656,45 руб.

Рис. 1. Детализация расходов для номера <…> за 24 сентября

Затем конкретному оператору сотовой связи необходимо направить запрос о местонахождении мобильного устройства, его IMEI-коде, номере sim-карты и т. д. Однако здесь могут возникнуть некоторые проблемы:

1. В связи с использованием неавторизованных sim-карт или sim-карт с внесенными в учетные документы недостоверными сведениями часто возникают сложности с идентификацией их владельцев. Сотрудники следственных подразделений отмечают, что сегодня наметилась четкая тенденция к упрощению оформления абонентских договоров и внедрению сервисов, обеспечивающих защищенность и анонимность абонентов сотовой связи.

2. В настоящее время среди злоумышленников пользуются популярностью различные сервисы IP-телефонии, позволяющие без должной идентификации дистанционно подключать абонентские номера из емкости номеров, относящихся к стационарным телефонам Москвы и Московской области. Посредством SIP-протокола звонки можно осуществлять с помощью компьютера (нужна специальная программа), через сети WiFi или 3G/4G (необходимы SIP-программы для планшетов и мобильных телефонов), используя специальный стационарный SIP-телефон, который включаются в роутер, либо через обычный телефон, подключив его к VoIP-шлюзу, а сам шлюз – к роутеру. Данный вид связи позволяет совершать звонки лицам, находящимся в любых субъектах Федерации.

3. Довольно часто преступники используют технологии подмены вызывающего номера (чаще всего имитируют реальные номера службы поддержки банков), что возможно из-за значительного количества уязвимых для взлома действующих виртуальных АТС. При этом следов взлома и использования данных АТС в криминальных целях, как правило, не остается.

4. В числе причин, создающих трудности для идентификации мошенников, также следует назвать использование ими VPN и Proxy-сервисов (анонимайзеров) для интернет-соединений при совершении вызовов по системе IP-телефонии. Это позволяет полностью скрыть или усложнить процесс получения данных о местоположении серверов и абонентских устройств. Маршрутизация в VPN и Proxy-сервисах построена с учетом угрозы возможных блокировок отдельных серверов, в связи с чем прохождение сигнала в них контролируется и поддерживается дублирующими серверами. Технически подавить работу VPN и Proxy-сети нельзя, однако можно организовать отдельную защищенную сеть, не подключенную к VPN-серверам.

Сотрудники следственных подразделений могут столкнуться с тем, что оператор сотовой связи не предоставляет им сведений об IMEI-коде устройства[1] без судебного решения, ссылаясь на законодательство Российской Федерации о тайне телефонных переговоров. Однако выразим солидарность с мнением Е. Зарубиной, Н. Ивлиевой о том, что «информация об IMEI-коде не передается от абонента к абоненту, не имеет адресата и сохраняется оборудованием при авторизации в сети без волеизъявления абонента. То есть взятое отдельно от информации о соединениях абонента не может относиться к охраняемой законодательством Российской Федерации тайне телефонных переговоров»[2]. IMEI используется только для идентификации устройства и не имеет постоянного отношения к абоненту. Его можно использовать для определения местонахождения устройства, даже если телефон работает с другой sim-картой. Доступ к геолокации есть у оператора сотовой связи, расположение телефона определяется с точностью до пары домов. Однако не все так просто: злоумышленникам не стоит труда «перебить» IMEI-коды, причем такие действия в нашей стране не влекут за собой никакой ответственности[3].

Важно также отметить, что операторам сотовой связи доступна информация об использовании абонентом Интернета, включая адреса сайтов и объем переданных данных. В случае если речь идет об iPhone, то правильно оформленный запрос (так называемый Device

[1] Международный идентификатор мобильного оборудования, состоящий из 15 цифр.

[2] Зарубина Е., Ивлиева Н. Получить ответ непросто. С. 41.

[3] В 2018 г. законопроект о введении штрафов за перекодировку активно обсуждался, но так и не вступил в силу.

Request – запрос, в котором нет ничего, кроме IMEI) позволит полиции получить и те данные, которые собирает о пользователе Apple. Сегодня эта компания активно сотрудничает с правоохранительными органами разных стран и находится в процессе запуска онлайн-портала, на котором полицейские смогут подавать правомерные запросы, проверять статус их выполнения и своевременно получать ответы[1].

Если хищение электронных денег было совершено с использованием средств сотовой связи, для примерного установления местонахождения абонента можно воспользоваться интернет-сервисом xinit.ru. Он показывает зоны действия базовых станций – системных комплексов приемопередающей аппаратуры. Сегодня смартфоны, работающие на базе операционных систем Android и iOS, приложения Гугл.Карты и Яндекс.Карты постоянно отслеживают местонахождения телефонов, собирают информацию о расположенных рядом базовых станциях, Wi-Fi-точках доступа, bluetooth-устройствах и отправляют все это вместе с координатами устройств на свои серверы, но такие данные обезличены и обобщены[2]. Здесь важно помнить о том, что сведения, полученные таким образом, не будут точными, поскольку сигнал, исходящий от сотового телефона может быть как прямым, так и отраженным от стен домов и иных застроек, на него оказывают определенное влияние особенности рельефа и т. д., при этом человек может находиться рядом с одной базовой станцией, но обслуживаться отраженным сигналом другой. Эксперты отмечают, что «амплитуда сигналов, угол их прихода и значение расстояния база–трубка могут непрерывно изменяться в очень больших пределах, а определение фактических координат становится почти невозможным»[3].

Отметим, что деанонимизация преступника, разумеется, не должна ограничиваться только обращением к открытым интернет-сервисам. Здесь нужно использовать и иные ресурсы. Согласимся с мнением Ю. Б. Имаевой о том, что при расследовании преступлений, совер-

[1] См.: Мы твердо убеждены, что национальная безопасность может быть обеспечена без нарушения конфиденциальности. URL: https://www.apple.com/ru/privacy/government-information-requests/ (дата обращения: 09.09.2021).

[2] См.: Как это работает: координаты базовых станций. URL: https://xinit.ru/ (дата обращения: 09.09.2021).

[3] Бозов А. А. Методические рекомендации: использование возможностей сотовой связи при раскрытии и расследовании преступлений. URL: https://alexboz.pravorub.ru/personal/30734.html (дата обращения: 09.09. 2021).

шенных в отношении электронных средств платежа (как, впрочем, и в отношении электронных денег), не стоит пренебрегать разыскными и криминалистическими учетами. В частности, учет преступлений по способу их совершения поможет очертить круг лиц, способных совершить хищение определенным способом, а также ответить на вопрос о том, могло ли преступление быть совершено конкретным лицом, которое ранее зарегистрировано как лицо, совершившее хищение определенным способом[1]. Однако полагаем, что это может сработать в случае с кражами, если же речь идет о кибермошенничестве, то способы его совершения постоянно меняются, становятся более технологичными.

Особого внимания заслуживает точка зрения В. О. Давыдова, И. В. Тишутиной, согласно которой повышению эффективности установления лиц, совершивших преступления, и, как следствие, своевременному направлению дел в суд будет способствовать систематизация в рамках единой базы данных информации о зарегистрированных мошенничествах, совершаемых с помощью Интернета, а также создание автоматизированных систем мониторинга сети Интернет, в частности, значимых в криминалистическом аспекте информационных систем поиска по метаданным[2].

Метаданные («данные о данных») представляют собой набор сведений, которые содержат в себе сами медиаактивы (изображения, видео и иные файлы)[3]: время и дата создания файла, его формат, название, геометка и т. д. Сегодня метаданные принято делить на несколько групп (рис. 2).

[1] См.: Имаева Ю. Б. Особенности расследования хищений, совершенных с использованием кредитных и расчетных карт: дис. … канд. юрид. наук. Уфа, 2015. С. 148.

[2] См.: Давыдов В. О., Тишутина И. В. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2020. № 2 (14). С. 85.

[3] См.: Что такое метаданные и как они облегчают работу с файлами в цифровом архиве. URL: https://picvar.io/blog/chto-takoe-metadannye/rus (дата обращения: 09.09.2021).

Рис. 2. Типы метаданных

В настоящее время анализ данных, включая метаданные, как ответ на перманентный рост телефонного и интернет-мошенничества активно применяют компании сотовой связи и финансовый сектор. Так, китайскому сотовому оператору China Mobile принадлежит приложение Tiandum («Небесный щит»). В основу его работы положены анализ Big Data и технологии машинного обучения, благодаря которым система может распознавать характерные для мошенников фразы, перехватывать спам и звонки от злоумышленников. Для обучения системы разработчики использовали обширную базу дел о мошенничестве, предоставленную полицейскими управлениями. В числе безусловных достоинств «Небесного щита» нужно назвать его умения идентифицировать группы пользователей, наиболее подверженные угрозе мошенничества, предупреждать о возможной атаке, в случае подозрения на совершение мошенничества направлять номера потенциальных жертв полицейским[1].

[1] См.: China Mobile привлек к борьбе с мошенничеством ИИ-технологии и Big Data. URL: https://nag.ru/news/newsline/102103/china-mobile-privlek-k-borbe-s-moshennichestvom-ii-tehnologii-i-big-data (дата обращения: 09.05.2021).

Анализ данных с успехом применяют банки и платежные гиганты PayPal, MasterCard и др. Практически все они имеют антифрод-сервисы – системы, ориентированные на оценку транзакций в Интернете на предмет подозрительности. Для выявления потенциальных мошенников антифрод анализирует большое количество параметров, которые помогают создать профиль среднестатистического плательщика. На его основе присваивается уровень возможной опасности проведения мошеннической операции. Подозрение системы могут вызвать пользователи, не оставляющие цифровых следов. В случае если доступ осуществляется через аккаунты в социальных сетях, антифрод выявляет фейковых пользователей[1]. Несколько лет назад подобные технологии стала применять компания VISA: с помощью платформы с открытым исходным кодом для надежной, масштабируемой, распределенной обработки больших наборов данных посредством простых моделей программирования Apache Hadoop за один раз изучаются сразу 500 аспектов сделки и поверяются 16 видов возможных мошеннических схем[2].

В связи со сказанным большое значение приобретает создание в рамках федерального проекта «Информационная безопасность»[3] государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), в число субъектов которой планируется включить и МВД России, киберполигона для подготовки специалистов в соответствующей сфере, а также разработка Лабораторией Касперского технологического решения класса SIEM (Security Information and Event Management) Kaspersky Unified Monitoring and Analysis Platform (KUMA), предназначенного «для централизованного сбора, анализа и корреляции ИБ-событий из различных источников данных для выявления потенциальных киберинцидентов и своевременной их нейтрализации»[4].

---

[1] См.: Банкиры и операторы начинают обмен мошенниками. В России запускается несколько новых антифрод-платформ. URL: https://www.rbc.ru/newspaper/-2020/12/09/5fce307f9a7947fa67b4bcfc (дата обращения: 10.05.2021).

[2] См.: Большие данные против большого мошенничества. URL: https://www.kaspersky.ru/blog/bolshie-dannye-protiv-bolshogo-moshennichestva/14902/ (дата обращения: 10.05.2021).

[3] См.: Паспорт федерального проекта «Информационная безопасность». URL: digital.ac.gov.ru (дата обращения: 09.09.2021).

[4] Kaspersky Unified Monitoring and Analysis Platform (KUMA). Новая SIEM-система от Лаборатории Касперского. URL: https://kuma-kaspersky.axoftglobal.com/kuma...65-07543299597591463 (дата обращения: 09.09.2021).

Помочь в установлении лиц, совершивших хищение электронных денег, могут и специализированные информационно-поисковые системы, которые имеются сегодня в ряде субъектов Российской Федерации (Астраханской, Мурманской, Омской, Псковской областях) и ведут сбор и учет сведений о дистанционных мошенничествах. В них накапливается криминалистически значимая информация: номера банковских карт, электронных кошельков, IMEI-коды, номера мобильных телефонов, персональные данные физических лиц, адреса банкоматов и т. д., – позволяющая субъектам расследования выявлять преступления, совершенные по признакам серийности, и объединять их в одно производство. При этом территориальные органы внутренних дел, не имеющие возможности создать подобные системы, имеют доступ к уже существующим[1].

Скажем несколько слов и о подсистеме ИБД-Ф «Дистанционное мошенничество», администратором которой является Главный информационно-аналитический центр МВД России. Здесь автоматически накапливается следующая информация: данные о номере обращения, зарегистрированного в книге учета заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях (КУСП); номере уголовного дела; фабуле преступления; способе его совершения; сумме ущерба; решении, принятом по окончании доследственной проверки; территориальном органе, зарегистрировавшем сообщение о преступлении и расследующем его; данные о международном идентификаторе мобильного абонента (IMSI) и IMEI; номера банковских счетов, карт, электронных кошельков, которые использовались при совершении преступления; адреса сайтов, IP-адреса, адреса электронной почты, имевшие место в совершении преступления; установочные данные лиц, зафиксированные в материалах проверки сообщения о преступлении или уголовном деле; названия и ИНН организаций, зафиксированных в материалах проверки сообщения о преступлении или уголовном деле, – которая также может оказать существенную помощь в установлении лиц, совершивших хищение электронных денежных средств.

В числе сложных следственных ситуаций, возникающих на первоначальном этапе расследования рассматриваемых преступлений, необходимо также упомянуть организационно-неупорядоченные

[1] См.: Дорофеев К. И. Особенности организации расследования мошенничеств, совершенных дистанционным способом // Академическая мысль. 2019. № 4 (9). С. 59.

ситуации, детерминированные рядом проблем, в частности отсутствием системы эффективного взаимодействия в процессе расследования (о чем мы говорили в предыдущем параграфе), недостатками финансирования и т. д. Здесь же стоит назвать и техническое оснащение рабочих мест следователей, нуждающееся в настоящее время в модернизации. От этого будут зависеть оперативность и мобильность раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, включая хищения электронных денег, дефицит которых отмечается на разных уровнях[1].

Сегодня в большинстве территориальных подразделений МВД России к сервисам ИСОД МВД России постоянный доступ имеют только начальники и их заместители. Полагаем, что подобное будет наблюдаться и в том случае, если МВД России удастся запустить сервис межведомственного электронного документооборота, который в идеале должен быть доступен каждому следователю. Чтобы добиться мобильности и оперативности расследования преступлений, для следователей стоит создать специализированную цифровую экосистему – группу взаимосвязанных информационных технологических ресурсов, которые могут функционировать как единое целое[2]. В ее рамках должны действовать сервис межведомственного электронного документооборота, инструменты совместной работы (электронная почта), инструменты планирования (типа диаграммы Ганта) и обучающие площадки. Первый и вторые поспособствуют быстрому обмену информацией межу правоохранителями, банками и операторами сотовой связи, а также внутри системы МВД России, третьи визуализируют запланированные задачи и обеспечат своевременность их выполнения, четвертые позволят проходить обучение и повышать квалификацию непосредственно на рабочем месте, что особенно важно, поскольку традиционное юридическое образование, которое имеют большинство следователей, ориентировано

[1] См., например: Сергей Лебедев: в виртуальном мире не выстроены барьеры для преступников. URL: https://ria.ru/20210820/kibermoshennichestvo-1746425415.html (дата обращения: 01.09.2021); Немцева М. «Их слишком много»: почему киберпреступления остаются нераскрытыми. URL: https://iz.ru/1166840/mariia-nemtceva/ikh-slishkom-mnogo-pochemu-kiberprestupleniia-ostaiutsia-neraskrytymi (11.08.2021) и др.

[2] См.: Алейникова Ю. В., Матвеев В. В. Цифровая экосистема. Анализ применения искусственного интеллекта // Здоровье – основа человеческого потенциала: проблемы и пути их решения. 2020. Т. 15. № 3. С. 1481.

на решение правовых проблем и не предполагает связи с техническими науками, без чего невозможно понимание механизма совершения киберпреступления и его эффективное расследование.

Скажем несколько слов и о простых следственных ситуациях первоначального этапа расследования хищений электронных денежных средств. Чаще всего они возникают, когда речь идет о тайном хищении электронных денежных средств, совершенном при непосредственном контакте с устройством потерпевшего. Анализ уголовных дел и судебных решений показывает, что нередко такие преступления совершаются в состоянии алкогольного опьянения. Умысел формируется довольно быстро, время на подготовку к преступлению, как правило, отсутствует. После его совершения вывод и снятие денежных средств производятся самим злоумышленником, иногда иным лицом, предоставившим первому номер счета для перевода денег. Задача, стоящая здесь перед следователем, – собрать фактические данные, доказывающие факт совершения кражи конкретным лицом.

Алгоритм действий следователя в подобных ситуациях должен включать: получение показаний от потерпевшего и свидетелей преступления, если таковые имеются; осмотр устройства потерпевшего с привлечением специалиста; если подозреваемый задержан, осмотр устройства, принадлежащего ему; направление запроса в кредитную организацию для установления суммы причиненного ущерба и счета, куда поступили денежные средства; направление поручения в орган дознания в целях получении информации с камер видеонаблюдения системы «Безопасный город», а также с камер видеонаблюдения, установленных в банкоматах, о лице, осуществившем снятие денежных средств; в случае необходимости проведение очной ставки между потерпевшим и подозреваемым.

Резюмируя сказанное, сделаем некоторые выводы:

1. Анализ следственной и судебной практики свидетельствует о том, что на первоначальном этапе расследования хищений электронных денежных средств наиболее часто имеют место сложные следственные ситуации: проблемные, обусловленные семантической неопределенностью, и организационно-неупорядоченные, детерминированные отсутствием должного взаимодействия, недостатками финансирования, несовершенством технического оснащения рабочих мест следователей.

2. В решение данных ситуаций существенную помощь способны оказать интернет-ресурсы, размещенные в свободном доступе: «2IP.UA», «WHOIS», «Dig», которые можно использовать для установления хостинг-провайдеров и IP-адресов; www.spravportal.ru, https://region-operator.ru/, https://codificator.ru/ – для определения операторов сотовой связи и региона, где был зарегистрирован номер абонента; xinit.ru – для примерного установления местонахождения абонента сотовой связи. Кроме того, при расследовании рассматриваемых преступлений не стоит пренебрегать разыскными и криминалистическими учетами, в частности учетом преступлений по способу их совершения.

3. Необходимо выразить солидарность с мнением В. О. Давыдова, И. В. Тишутиной о том, что повышению эффективности установления лиц, совершивших преступления, поспособствует систематизация в рамках единой базы данных информации о зарегистрированных мошенничествах, совершаемых с помощью Интернета, а также создание автоматизированных систем мониторинга сети Интернет, в том числе, значимых в криминалистическом аспекте информационных систем поиска по метаданным, что сегодня делают операторы сотовой связи и финансовый сектор.

4. В целях повышения мобильности и оперативности расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, включая хищения электронных денежных средств, особое внимание нужно уделить техническому оснащению рабочего места следователя. Полагаем, сегодня назрела необходимость создания специализированной цифровой экосистемы, которая будет объединять сервис межведомственного электронного документооборота, инструменты совместной работы (электронная почта), инструменты планирования (типа диаграммы Ганта) и обучающие площадки, что позволит осуществлять быстрый обмен информацией, визуализировать запланированные задачи и обеспечить своевременность их выполнения, проходить обучение и повышать квалификацию непосредственно на рабочем месте.

2.3. Тактика производства отдельных следственных действий первоначального этапа расследования хищений электронных денежных средств

Выдающийся русский философ И. А. Ильин писал: «… люди, не ведающие своих обязанностей, не в состоянии и блюсти их; люди, не знающие своих полномочий, произвольно превышают их или трусливо уступают силе; люди, не желающие признавать запретностей, легко забывают всякий удерж и дисциплину или оказываются обреченными на правовую невменяемость»[1]. Полагаем, что данные слова должны стать своеобразным наставлением для следователей в их деятельности в целом и производстве следственных действий в частности, поскольку здесь чрезвычайно важно соблюдение процессуальных правил, иначе следственные действия будут признаны незаконными, а доказательства, полученные таким образом, недопустимыми.

Общие правила производства следственных действий регламентированы ст. 164 УПК РФ[2], их главная цель заключается в получении или удостоверении информации об обстоятельствах, подлежащих доказыванию по уголовному делу.

Тактике производства следственных действий при расследовании киберпреступлений уделяли внимание Ю. В. Гаврилин, Г. А. Гундерич, Л. П. Зверянская, Т. П. Ишмаева, Е. П. Ищенко, В. В. Коломинов, Е. Г. Кравец, Н. В. Олиндер, А. А. Протасевич и др. Отдельный акцент нужно сделать на работах Г. З. Гаспаряна и Е. С. Шевченко. В диссертации первого рассматриваются невербальные следственные действия первоначального этапа расследования хищений денежных средств, совершенных с использованием информационных банковских технологий (осмотр места происшествия, обыск (выемка), осмотр предметов и документов)[3], вербальные следственные действия, в том числе допрос потерпевшего, не анализируются вовсе, что, на наш взгляд, не совсем верно, поскольку

[1] Ильин И. А. О сущности правосознания. М.: ТОО «Рарог», 1993. С. 21.

[2] См.: Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. URL: www.consultant.ru (дата обращения: 11.09.2021).

[3] См.: Гаспарян Г. З. Расследование хищений денежных средств, совершаемых с использованием информационных банковских технологий. С. 162–191.

иногда именно допрос потерпевшего приобретает здесь предопределяющее значение в связи с тем, что (ранее мы уже об этом говорили) способы совершения рассматриваемых преступлений не предполагают очевидцев, соответственно, потерпевший становится единственным источником информации. В свою очередь, внимание Е. С. Шевченко сосредоточено на тактике производства вербальных и невербальных следственных действий, а также следственных действий, направленных на получение виртуальной информации, при расследовании не только мошенничества, совершенного с использованием сети Интернет, но и преступлений, посягающих на авторские и смежные права; кибертерроризма; вымогательства, совершенного с использованием сети Интернет, и др.[1] Безусловно, работы названных авторов внесли существенный вклад в изучение криминалистического обеспечения расследования киберпреступлений, однако сегодня по-прежнему наблюдается дефицит научно обоснованных рекомендаций, связанных с тактикой производства отдельных следственных действий при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий, в том числе хищений электронных денежных средств.

В данном параграфе сделаем акцент на некоторых следственных действиях первоначального этапа расследования. Под ними понимается «подсистема ситуационного типа, которой наиболее оптимально начинать расследование определенных видов и групп преступлений, состоящая из относительно устойчивой совокупности процессуальных действий, эффективно выполняющих функции по безотлагательному поиску и выявлению источников (носителей) информации, получению доказательств, проверке типовых и некоторых первичных специфических версий, установлению и задержанию подозреваемых, предотвращению новых общественно опасных деяний, других вредных последствий и возмещению материального ущерба»[2]. В числе следственных действий первоначального этапа расследования хищений электронных денег необходимо назвать допрос потерпевшего и свидетелей, если таковые имеются, осмотр места происшествия, обыск, выемку, осмотр предметов и документов, назначение компьютерно-технических судебных экспертиз. Поговорим о них подробнее.

---

[1] См.: Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений. С. 77–163.

[2] Драпкин Л. Я., Карагодин В. Н. Криминалистика. С. 355.

Тактика производства допроса

Традиционно допрос определяется как следственное действие, цель которого заключается в получении от допрашиваемого лица доказательственной и ориентирующей информации об обстоятельствах преступления, его участниках, следах и иных сведений, имеющих значение для уголовного дела. Общие правила проведения допроса установлены в ст. 189 УПК РФ[1].

В рамках допроса обычно выделяют три этапа: подготовительный, основной и заключительный. Разумеется, каждый из них имеет свою специфику.

Подготовительный этап допроса во многом детерминирует его результативность. Здесь следователю стоит сделать акцент на информационном обеспечении данного следственного действия, изучении личности допрашиваемого лица и планировании. С точки зрения Е. С. Шевченко, «чем лучше информационное обеспечение у следователя, безупречное знание и владение им всем собранным по делу материалом и вспомогательной информацией, тем более подконтрольна будет ситуация, которая сложится на допросе. Кроме того, информационное обеспечение необходимо для исключения ошибки при квалификации совершенного киберпреступления. Для того чтобы верно квалифицировать киберпреступление, следователь должен понимать каким способом оно совершено, а также какие общественно опасные последствия принесло расследуемое преступление»[2].

Информационное обеспечение подразумевает под собой изучение специальной литературы (в первую очередь в сфере информационно-телекоммуникационных технологий) и консультирование со специалистами, которые могут разъяснить следователю некоторые термины, рассказать о возможных способах совершения рассматриваемых преступлений, а также «наметить очередность выясняемых технических вопросов и степень их конкретизации»[3].

---

[1] См.: Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. URL: www.consultant.ru (дата обращения: 11.09.2021).

[2] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений. С. 81.

[3] Там же. С. 84.

Не меньшее значение имеет анализ личности допрашиваемого лица. Если речь идет о потерпевшем, то следователю необходимо помнить о том, что граждане, ставшие жертвами телефонного или интернет-мошенничества, часто не спешат обращаться с заявлением о преступлении в правоохранительные органы, а в случае обращения могут утаивать некоторые его обстоятельства, чтобы не показаться невежественными. Как правило, такие лица сначала надеются вернуть похищенные деньги самостоятельно с помощью банка, оператора электронной платежной системы и т. д., которые, в свою очередь, обычно не отменяют произведенных транзакций. За данными действия может последовать обращение в суд с иском о возмещении кредитной организацией причиненного материального ущерба, что также в большинстве ситуаций не оканчивается успехом. Вполне естественно, после этого «у пострадавшего не возникает желания обращаться в другие инстанции для привлечения виновных… к ответственности»[1], а его психологическое состояние может быть как апатичным (если он смирился с утратой денежных средств и не верит в результативность деятельности органов внутренних дел), так и раздраженным (если ему кажется, что в возмещении причиненного ему материального ущерба заинтересован только он, а остальные бездействуют).

По мнению М. Н. Кузьмина, Н. В. Солонниковой, среди факторов, предопределяющих содержание тактического обеспечения производства допроса потерпевшего, нужно назвать:

– способ совершения преступления;

– позицию потерпевшего относительно расследования;

– его отношение к подозреваемому;

– этап расследования;

– личностные качества потерпевшего[2].

---

[1] Алексеева А. П., Ничуговская О. Н. Киберпреступность: основные черты и формы проявления // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2017. № 1. С. 31.

[2] См.: Кузьмин М. Н., Солонникова Н. В. Особенности тактики производства допроса потерпевшего в ходе расследования мошенничества в сфере компьютерной информации // Гуманитарные, социально-экономические и общественные науки. 2018. № 12. С. 112.

Все это поможет следователю установить соответствующий психологический контакт с потерпевшим и получить от него как можно больше важной информации по делу. Способ совершения преступления и личностные качества человека необходимо принимать во внимание и при подготовке к допросу свидетелей, если таковые имеются.

Составить некоторое представление о потерпевшем и свидетелях преступления можно в результате анализа их страниц в социальных сетях. Помочь в этом могут данные, указанные при регистрации (не только фамилия, имя и дата рождения, семейное положение, образование, но и предпочтения, статусы), фотографии, комментарии, размещаемый на странице контент, сообщества, в которых состоит пользователь, круг лиц, с кем он общается, подкасты и т. д. Однако не стоит забывать о том, что некоторая информация здесь может не соответствовать действительности.

Наконец еще одним значимым элементом подготовительной стадии допроса является его планирование: составление письменного плана, продумывание формулировки и очередности вопросов (здесь может помочь специалист, обладающий познаниями в соответствующей отрасли) и тактических приемов, которые будут применены при производстве следственного действия, выбор времени и места. Особый акцент следует сделать на формулировании вопросов. Чтобы избежать искажения информации допрашиваемым лицом, их нужно строить по аналогии с тестом СМИЛ (стандартизированный метод исследования личности): одно содержание, но разная формулировка (например, кому из Ваших знакомых известен пароль от Вашего устройства; все ли Ваши знакомые могут беспрепятственно воспользоваться Вашим устройством в своих целях; скрываете ли Вы информацию, хранящуюся на Вашем устройстве, от всех посторонних лиц, или кто-то все же имеет к ней доступ?). При этом задавать такие вопросы нужно не друг за другом, а спустя несколько иных.

Основной этап допроса включает в себя следующие обязательные стадии: выяснение необходимых данных о личности допрашиваемых, свободный рассказ допрашиваемого лица, стадию вопросов-ответов и заключительную стадию. При всей кажущейся простоте допрос является довольно сложным следственным действием, особенную трудность в нем представляет установление психологиче-

ского контакта с допрашиваемым лицом, умение варьировать тактические приемы и методы психологического воздействия исходя из ситуации.

Выяснение личности допрашиваемого лица сопровождается ознакомлением следователя с удостоверяющими личность документами, заполнением анкетной части протокола и разъяснением допрашиваемому лицу его прав и обязанностей. Именно здесь происходит установление психологического контакта. Важную роль на этом этапе играют правильно выбранный тон беседы, умение следователя расположить к себе, пробудить заинтересованность к даче правдивых показаний, а также его доброжелательность, корректность, готовность терпеливо выслушать и т. д. Чтобы установить контакт, можно задать допрашиваемому лицу несколько нейтральных вопросов (о месте его рождения, жительства и т. д.), а затем попросить его рассказать о случившемся, т. е. перейти к этапу свободного рассказа. В случае с хищениями электронных денежных средств он имеет большое значение, поскольку позволяет установить некоторые обстоятельства произошедшего, в частности способ и время совершения преступления. Допрашиваемого не нужно перебивать (вмешаться можно лишь при явном уклонении от предмета разговора), не стоит просить его умерить эмоции, необходимо терпеливо выслушать, в случае наличия уточняющих вопросов задать их по окончании рассказа.

Если имеется предположение, что потерпевший утаивает некоторые факты, чтобы не выглядеть несведущим, можно привести несколько примеров аналогичных преступлений, совершенных в отношении других лиц, где жертвы были откровенны, вспомнили детали события преступления и тем самым помогли изобличить виновных. Однако не стоит забывать о том, что искажение показаний возможно «в силу действия разнообразных психологических закономерностей, определяющих содержание будущих показаний от момента восприятия того или иного события до передачи информации о нем на допросе»[1]. Кроме того, по справедливому замечанию Е. С. Шевченко, при производстве допроса «следователю нужно учитывать,

[1] Тактика допроса и очной ставки. URL: https://be5-biz.turbopages.org/turbo/-be5.biz/s/pravo/k009/24.html#3-2 (дата обращения: 11.09.2021).

что киберпространство существенно меняет восприятие человеком действительности. В условиях киберпространства меняется психологическое содержание взаимосвязей: преступник – предмет преступления (потерпевший), – которые превращаются во взаимосвязь: преступник – электронное устройство (сети) – потерпевший (предмет преступления)»[1].

На этапе вопросов и ответов следователь в предельно четкой форме должен задавать уточняющие, дополняющие, конкретизирующие, контрольные вопросы, не допускать вопросов-подсказок. Так, если хищение электронных денег произошло с использованием приемов социальной инженерии, необходимо выяснить, каким устройством пользовался потерпевший, кто осуществил телефонный звонок, с какого номера, кем представился, что попросил сделать, какие данные были переданы звонившему лицу, в какое время, с каким оператором сотовой связи заключен договор; если имел место перевод электронных денег за товар, который так и не был доставлен, нужно уточнить, с какого устройства потерпевший заходил на сайт интернет-магазина или площадки с объявлениями, адрес сайта, имя продавца, вид товара или услуги, его стоимость, суть переписки с продавцом, сумму перевода денежных средств, время его осуществления, время предполагаемой доставки, реакцию продавца на требования выслать трек-номер отправления или товар, существует ли магазин в данный момент; если речь идет о краже электронных денег с использованием вредоносного программного обеспечения (в том числе программ удаленного доступа), следует выяснить, какими устройствами пользовался потерпевший, кто имел к ним доступ, кроме потерпевшего, как и в какое время потерпевший узнал о списании денежных средств, при каких обстоятельствах была установлена программа удаленного доступа, какие сайты посещал потерпевший, какие письма приходили ему на электронную почту, кто был их отправителем, открывал ли потерпевший эти письма, переходил ли по ссылкам, содержащимся в этих письмах или рекламе на интернет-сайтах, какие SMS-сообщения поступали на телефон, с каких номеров, какими знаниями в сфере информационно-телекоммуникационных технологий обладает потер-

[1] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений. С. 92.

певший; наконец, если была совершена кража электронных денег без использования вредоносного программного обеспечения нужно установить, с помощью какого устройства потерпевший осуществляет доступ к своему электронному кошельку, имеется ли на устройстве пароль, кому известен этот пароль, кто, кроме потерпевшего имеет доступ к его устройству, оставлял ли потерпевший устройство без присмотра и на какое время, кто имел доступ к устройству в это время, кому известен пароль от электронного кошелька, какова сумма причиненного ущерба, как и в какое время потерпевший узнал о списании денежных средств. Перечень вопросов не является исчерпывающим и зависит от конкретной следственной ситуации.

При допросе следователю может помочь криминалистический профайлинг, под которым понимается комплекс психологических методов и приемов, включающий в себя определение характера, темперамента, интеллекта и, как результат, прогноз поведения человека, а также характеристику внешности, вербальное и невербальное поведение, оперативную психодиагностику[1]. При производстве допроса особое внимание нужно обращать на мимику, позы и жесты допрашиваемого лица, чтобы выявить признаки лжи в ходе вербального общения по невербальным коммуникациям, а также на конгруэнтность – соответствие лингвистической информации невербальным коммуникациям (слов действиям). Конечно, большое значение криминалистический профайлинг приобретает при допросе подозреваемого (поговорим об этом в параграфе 3.1), однако отдельные его методики могут применяться и по отношении к потерпевшему и свидетелям.

Заключительная стадия допроса представляет собой фиксацию хода и результатов следственного действия, составление протокола в конечной форме, каждая страница которого подписывается допрашиваемым лицом.

Тактика производства осмотра места происшествия

В криминалистической литературе местом происшествия называется помещение или участок местности, в пределах которого обнаружены следы совершенного преступления. Л. В. Пинчук отмечает,

[1] См.: Бурмистрова Н. С., Бертовский Л. В. Особенности применения криминалистического профайлинга в период сбора релевантной информации в ходе расследования преступления // Пробелы в российском законодательстве. 2018. № 6. С. 266.

что в качестве такового можно рассматривать «любые места, где выявлены следы и объекты, относящиеся к расследуемому преступлению»[1]. Полагаем, что в случае совершения хищений электронных денежных средств особенно путем обмана или злоупотребления доверием ими являются местонахождение заявителя в момент перевода денег и киберпространство. По мнению Е. С. Шевченко, именно киберпространство, точнее, необходимость распознавания виртуальных следов, образованных средствами вычислительной техники, доступным сегментом локальной вычислительной сети, глобальной сети Интернет и цифровыми носителями информации, вызывает наибольшие трудности при производстве рассматриваемого следственного действия[2].

Согласно ст. 176 УПК РФ цель осмотра места происшествия состоит в обнаружении следов преступления, выяснении других обстоятельств, имеющих значение для уголовного дела[3], т. е. нужно установить механизм преступления (ответить на вопросы, что и как произошло). Задачи данного следственного действия заключаются в своевременном выявлении, изучении, фиксации, изъятии и предварительном исследовании в соответствии с законом необходимой информации и следов (материальных, идеальных, цифровых).

Осмотр места происшествия объединяет в себе три этапа: подготовительный, рабочий и заключительный. Первый охватывает время до выезда следственно-оперативной группы (СОГ) на место происшествия и сразу по прибытии сюда. Как правило, в рамках данного этапа на основе сбора и анализа ориентирующей информации устанавливаются обстоятельства произошедшего (способ, место и время); определяются цель и конкретные задачи следственного действия, а также состав СОГ, проводится ее инструктаж. По мнению Д. А. Илюшина, в случае совершения преступления с использованием возможностей сети Интернет она должна быть укомплектована следователем – руководителем СОГ, сотрудником отдела «К» БСТМ МВД России, оперуполномоченным уголовного розыска и специалистом-

[1] Пинчук Л. В. К вопросу о понятии осмотра места происшествия // Вестник Московского университета МВД России. 2018. № 5. С. 230.

[2] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений. С. 102–103.

[3] См.: Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. URL: www.consultant.ru (дата обращения: 11.09.2021).

криминалистом[1]. Однако нам ближе точка зрения А. Н. Яковлева, Н. В. Олиндер, согласно которой основные функции участников СОГ успешно выполняют следователь и привлеченный к осмотру места происшествия специалист, оказывающий как консультативное, так и доказательственное содействие первому. В случае когда привлечь специалиста не представляется возможным, стоит прибегнуть к помощи разных лиц, обладающих необходимым опытом и объемом знаний[2]. Кроме того, до выезда СОГ на место происшествия принимается решение о целесообразности, а иногда об обязательности использования при осмотре программно-аппаратных средств работы с электронной информацией («Мобильный криминалист», Elcomsoft Mobile Forensic Bundle, Cellebrite UFED и др.).

По прибытии на место происшествия следователь должен организовать его охрану, позаботиться о сохранности следов и обстановки преступления, оставить все объекты в том состоянии, в каком они находились на момент начала осмотра, определить круг участников следственного действия.

Рабочий этап осмотра места происшествия состоит из двух стадий: обзорной и детальной. Первая предполагает установление границ места, подлежащего осмотру; фиксацию обстановки на момент начала производства следственного действия; выдвижение типичных общих и частных версий, определение оптимальных методов поиска. Многие ученые[3] сходятся во мнении, что при расследовании киберпреступлений осмотр места происшествия должен проходить в направлении «от центра – к периферии», чаще всего таким «центром» является устройство, откуда был осуществлен вход в Интернет и перевод денежных средств. Однако в случае неявной локализации носителей информации осмотр может проводиться по методу «закручивающейся спирали»: от периферии к центру.

---

[1] См.: Илюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: дис. … канд. юрид. наук. Волгоград, 2008. С. 118.

[2] См.: Яковлев А. Н., Олиндер Н. В. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем: науч.-практ. пособие. М., 2012. С. 100.

[3] См., например: Илюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет. С. 126; Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений. С. 105 и др.

С точки зрения Г. З. Гаспаряна, при расследовании хищений денежных средств, совершенных с использованием дистанционных банковских технологий, также возможно применение фронтального (линейного) метода осмотра: линия делится на равные отрезки, каждый из которых осматривается от одного до другого края[1].

В рамках детальной стадии осмотра места происшествия проводится тщательное изучение структуры места в целом и каждого ее элемента в частности, обнаружение и изъятие криминалистически значимой информации. Здесь важно использовать помощь и знания специалиста, который должен быть предельно внимателен и аккуратен, поскольку, как справедливо отмечает В. Ю. Ткач, «осмотр места происшествия – это самая сложная проводимая в необычных (полевых) условиях „экспертиза“, к тому же во многом предопределяющая возможности не только производства экспертиз в лабораторных условиях по отдельным следам, но и формирование в целом доказательственной базы по уголовным делам»[2].

Сначала выявляются материальные следы преступления, чаще всего они имеют место, когда речь идет о краже электронных денег, которой предшествовал непосредственный контакт преступника с устройством потерпевшего (следы пальцев рук, следы обуви, следы биологического происхождения, устройства, документы, данные банковских карт и др.). Затем следователь и специалист переходят к осмотру устройства и киберпространства, т. е. к поиску цифровых следов. Необходимо помнить о том, что, если на момент начала осмотра устройство находилось в выключенном состоянии, нужно оставить его в таком же, чтобы не потерять важной информации, если было включено, в первую очередь стоит обратить внимание на изображение на экране дисплея, далее выяснить, какая операционная система установлена на компьютере, какие используются протоколы связи, службы доступа к файлам и сети[3]. Именно здесь могут быть выявлены цифровые следы преступления. Важно подчеркнуть,

[1] См.: Гаспарян Г. З. Расследование хищений денежных средств, совершаемых с использованием информационных банковских технологий. С. 174.

[2] Ткач В. Ю. Место происшествия – объект осмотра и криминалистического исследования // Известия Тульского государственного университета. Экономические и юридические науки. 2012. № 1-2. С. 299.

[3] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений. С. 140.

что такие следы «имеют высокую скорость трансформации, легко уничтожаются и модифицируются, могут быть представлены бесконечным количеством копий, легко распространяются в компьютерных сетях и доступны в любой точке, где имеется подключение к сети Интернет… цифровой или электронный след может состоять из большого количества отдельных информационных элементов, которые могут быть записаны как на одном, так и на нескольких электронных носителях информации, подключенных как к одному, так и к нескольким компьютерам, объединенным в информационную систему или информационно-телекоммуникационную сеть»[1]. Цифровыми следами могут быть следы вывода и ввода денег, хранящиеся на серверах онлайн-банков или платежных систем, следы, связанные с регистрацией доменного имени сайта, IP-адрес и т. д.

В завершение обнаруженные следы, электронные документы и иная значимая для дела информация фиксируется и изымается, при необходимости может быть изъят весь компьютер или системный блок либо сотовый телефон. В качестве иной информации могут выступать, например, документы. Так, согласно материалам уголовного дела по обвинению Д. в совершении преступления, предусмотренного п. «в» ч. 2 ст. 158 Уголовного кодекса Российской Федерации, у потерпевшей Р. были изъяты документы, свидетельствующие о несанкционированном списании со счета №, открытого в банке «название» денежных средств в сумме 17 000 руб., принадлежащих ей, справка банка «название» и минивыписка по карте банка «название», а также сотовый телефон «Honor» IMEI 1 <…> IMEI 2 <…>, содержащий SMS-сообщения о списании денежных средств.

На заключительном этапе осмотра места происшествия изъятые объекты упаковываются, принимаются меры к охране объектов, которые невозможно изъять с места происшествия, делается запись об ознакомлении с протоколом всех участников следственного действия, учитываются их замечания.

[1] Давыдов В. О., Тишутина И. В. Цифровые следы в расследовании дистанционного мошенничества // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 3. С. 22.

Тактика производства обыска и выемки

Обыском и выемкой называются следственные действия, производимые в целях получения объектов, которые могут иметь значение для правильного разрешения уголовного дела. Именно общая цель позволяет рассматривать их совместно.

Под обыском понимается принудительное обследование помещений, участков местности, а также физических лиц для обнаружения и изъятия орудий преступления, предметов и ценностей, которые могут иметь значение для уголовного дела, а также трупов и разыскиваемых лиц. Под выемкой – изъятие в заранее известном месте и у конкретного лица предметов и документов, обладающих индивидуально-определенными признаками и имеющих значение для уголовного дела. Основания и порядок производства обыска и выемки установлены в ст. 182–183 УПК РФ[1].

При расследовании хищений электронных денежных средств производство обыска и выемки имеет свою специфику, прежде всего обусловленную тем, что сам предмет преступления не имеет материального выражения. Главная цель здесь состоит в обнаружении и изъятии компьютерной техники, на которой могли остаться следы совершенного преступления; компьютерной информации, касающейся как самого преступления, так и лиц, его совершивших; предметов, являющихся средством совершения преступления (вредоносное программное обеспечение); документов, содержащих информацию о преступлении (выписки с карт и счетов, квитанции о переводе денежных средств).

Как правило, выделяют четыре стадии производства обыска: предварительную, обзорную, детальную и завершающую. На первой необходимо собрать информацию о месте производства данного следственного действия (точный адрес, характеристику строения, наличие телефонной связи, наличие локальной и глобальной сети, месторасположения электропитания, место прокладки телекоммуникационных кабелей); определить вид и содержание информации, которая может храниться у преступника, предположить, на какой технике и каких носителях она может содержаться, какие документы и предметы, имеющие значение для уголовного дела, могут нахо-

[1] См.: Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. URL: www.consultant.ru (дата обращения: 11.09.2021).

диться на месте обыска; изучить личность обыскиваемого лица, особое внимание уделить его образованию, навыкам работы с информационно-коммуникационными технологиями, платежными системами, финансовыми документами; принять решение о целесообразности использования программно-аппаратных средств работы с электронной информацией («Мобильный криминалист», Cellebrite UFED и др.); очертить круг участников следственного действия (обязательно участие специалиста и понятых). Затем необходимо незамедлительно приступить к его производству.

По прибытии на место обыска следователю надлежит ознакомить обыскиваемое лицо с постановлением и судебным решением о его производстве и предложить добровольно выдать искомые предметы. Если обыскиваемый отказывается это делать, нужно собрать всех лиц, находящихся здесь, в одном месте и запретить им доступ к устройствам (компьютеру, телефону, планшету и т. д.) и телекоммуникационным сетям.

На обзорной стадии обыска в первую очередь нужно провести осмотр всего помещения, вместе с тем сделать акцент на компьютерной технике, находящейся здесь, ее расположении и состоянии, состоянии телекоммуникационных сетей, «произвести поиск портативных запоминающих устройств (флэш-карты, внешний жесткий диск), а также замаскированных высокотехнологичных продуктов маленького размера, которые тоже могут являться носителями компьютерной информации (например, кулон, часы, серьги)»[1]. Для этого стоит использовать приборы нелинейной локации («Онега», «Обь-3»), реагирующие на индуцирующие объекты. Кроме того, необходимо обращать внимание на конверты и документы, которые могут свидетельствовать о получении банковских карт, куда могли переводиться похищенные деньги. Отметим, что непосредственно в поиске следователь не участвует, он наблюдает за поведением обыскиваемого и в случае необходимости оказывает на него воздействие. Обыск производится от двери по часовой стрелке вдоль стен, в завершение обыскивается центр.

Детальная стадия обыска предполагает работу с устройством, на котором может храниться имеющая для уголовного дела информация. Если нет угрозы потери данных, осматриваются жесткий диск и оперативная память. В случае нахождения искомой информа-

[1] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений. С. 145.

ции нужно определить, где именно она находится. Затем устройство выключается, упаковывается и изымается. Если компьютер находится в выключенном состоянии, необходимо зафиксировать его местоположение, его соединение с телекоммуникационными сетями, периферийными устройствами, разъединить их, упаковать и изъять.

В работе с мобильным телефоном существенную помощь может оказать программно-аппаратный комплекс «Мобильный криминалист», предназначенный для извлечения данных с мобильных устройств, из облачных хранилищ, выстраивания связей между контактами пользователя, нахождения геолокации, построения маршрутов, выполнения поиска по ключевым словам, выражениям, набора хешей, номерам телефонов и т. д.[1] Если исследовать мобильное устройство на месте обыска не представляется возможным, то принимается решение о его изъятии.

В завершение следственного проверяется правильность упаковки изъятых предметов, они опечатываются, составляется протокол и опись к нему.

Тактика производства осмотра предметов и документов

Целью осмотра предметов и документов является обнаружение следов преступления и выяснение других обстоятельств, имеющих значение для уголовного дела. По уголовным делам о хищениях электронных денег предметами осмотра обычно выступают устройства, откуда был осуществлен вход в Интернет, перевод денежных средств; устройства, с которых была запущена вредоносная программа; флэш-накопители; внешние жесткие диски; оптические диски; служебные журналы системных и прикладных программ, применяемые для осуществления транзакций; информация, полученная в результате проведения отделом «К» БСТМ МВД России оперативно-разыскного мероприятия «Снятие информации с технических каналов связи»; банковские карты; sim-карты и пластиковые держатели для них и др. Документами – документы, подтверждающие причинение материального ущербы потерпевшему; документы, подтверждающие получение банковских карт, с которых и на которые осуществлялся перевод денежных средств; документы, свидетельствующие о несанкционированном списании денежных средств со счета; выписки о движении денежных средств и т. д.

[1] См.: Программно-аппаратный комплекс «Мобильный криминалист-эксперт». URL: https://www.oxygensoftware.ru/ru/products/mk (дата обращения: 12.09.2021).

Осмотр предметов и документов включает в себя три этапа: подготовительный, рабочий и завершающий.

На подготовительном этапе нужно проанализировать имеющуюся в уголовном деле информацию, организовать участие специалиста, понятых (в их отсутствие решить вопрос о применение средств фиксации). Г. З. Гаспарян отмечает, что «непродолжительные осмотры… предметов целесообразно проводить с участием понятых, которым необходимо в процессе разъяснять суть производимых манипуляций, и знакомить с результатами следственных действий в целях дальнейшего получения полных и объективных показаний от них в подтверждение объективности и законности проведенного с их участием следственного действия. Допуская возможность производства продолжительного осмотра изъятых электронных носителей информации… возможно применение видеофиксации хода и результатов следственного действия, что полностью соответствует ч. 1.1 ст. 170 УПК РФ»[1].

На рабочем этапе производства осмотра устройств в первую очередь важно обеспечить неизменность, подлинность и сохранность источника информации (не завершать запущенные ранее программы и не закрывать приложения, не отключать функции «авиарежим», «блокировка экрана», не допускать самостоятельного совершения действий, результат которых неизвестен); тщательно изучить предмет осмотра (для этого могут быть использованы названные аппаратно-программные комплексы). Большое значение здесь приобретает участие специалиста. При решении вопроса о его вызове следователь, по справедливому замечанию В. А. Снеткова, П. Т. Скорченко, должен иметь представление о категории доказательств, какие он надеется получить в ходе осмотра, наличии у специалиста необходимой профессиональной подготовки, соответствующей задачам следственного действия, и технико-криминалистических средств, от которых зависит эффективность его работы[2]. Именно с помощью таких средств можно получить доступ к переписке, страницам в социаль-

[1] Гаспарян Г. З. Расследование хищений денежных средств, совершаемых с использованием информационных банковских технологий. С. 186–187.

[2] См.: Снетков В. А. Основы деятельности специалиста экспертно-криминалистических подразделений органов внутренних дел: учеб. пособие. М.: ГУ ЭКЦ МВД России, 2001. С. 30–31, 56; Скорченко П. Т. Криминалистика. Технико-криминалистическое обеспечение расследования преступлений: учеб. пособие. М.: Былина, 1999. С. 51–57.

ных сетях, резервным копиям, облачным хранилищам, особенно если на устройстве активирована функция «авиарежим». Кроме того, необходимо удостоверить подлинность обнаруженной информации: отображаемая на устройствах информация должна быть зафиксирована с помощью функции скриншот и отражена в фототаблице с соответствующими пояснительными записями. Г. З. Гаспарян рекомендует также формировать по особым алгоритмам контрольные суммы (хэш-суммы) изъятой в процессе следственного действия информации, обеспечивающей достоверность доказательств на основе сопоставления параметров изъятой и исследуемой в дальнейшем информации[1].

На завершающем этапе оформляется протокол осмотра, предметы упаковываются в материал, исключающий возможность доступа к содержимому и дистанционного считывания информации, ее модификации или уничтожения.

Назначение судебных компьютерно-технических экспертиз

Обычно судебная компьютерно-техническая экспертиза назначается следователем после того, как произведены осмотр места происшествия, обыск и выемка, но информации для дальнейшего расследования недостаточно. По мнению Е. Р. Россинской, Е. И. Галяшиной, «судебные компьютерно-технические экспертизы производятся в целях определения статуса объекта как компьютерного средства, выявления и изучения его роли в расследуемом преступлении а также получения доступа к информации на носителях данных с последующим всесторонним ее исследованием»[2]. В. Р. Гайнельзянова отмечает, что экспертное исследование таких объектов, как информация, зафиксированная в электронной форме, программное обеспечение, средства компьютерной техники и сетевые технологии, «позволяет предоставить в распоряжение следователя сведения, отражающие механизм совершенного преступления, дает возможность определить параметры средств компьютерной техники, их отношения к обнаруженной информации и друг другу»[3].

---

[1] См.: Гаспарян Г. З. Расследование хищений денежных средств, совершаемых с использованием информационных банковских технологий. С. 189.

[2] Россинская Е. Р., Галяшина Е. И. Настольная книга судьи: судебная экспертиза. М.: Проспект, 2010. С. 378.

[3] Гайнельзянова В. Р. Возможности судебной компьютерно-технической экспертизы при расследовании преступлений в сфере компьютерной информации // Вестник Уфимского юридического института МВД России. 2021. № 1 (91). С. 146.

Сразу сделаем оговорку, что в России назначение судебных компьютерно-технических экспертиз сопряжено с такими трудностями, как недостаточное количество экспертов, имеющих допуск к их производству, длительность производства, высокая стоимость в негосударственных учреждениях. Кроме того, наблюдается отсутствие единого подхода к производству этих экспертиз в рамках МВД России и Минюста России, «еще более свободны в своих действиях негосударственные частные эксперты, чьи специальные знания в последнее время востребованы правоохранительной и судебной системой в случаях, когда требуется исследовать как компьютерную информацию, так и аппаратную часть цифровых устройств»[1].

Первой трудностью, с которой сталкивается следователь при назначении судебной компьютерно-технической экспертизы, является выбор ее вида. Сегодня различают несколько видов судебной компьютерно-технической экспертизы:

– аппаратно-компьютерную экспертизу;

– программно-компьютерную экспертизу;

– информационно-компьютерную экспертизу (данных);

– компьютерно-сетевую экспертизу.

В случае с хищениями электронных денежных средств наиболее востребованы программно-компьютерная и информационно-компьютерная экспертизы. Родовым объектом судебной программно-компьютерной экспертизы выступают «исполняемые модули, пакеты, алгоритмы и исходные тексты программ»[2], родовым объектом судебной информационно-компьютерной экспертизы – файлы компьютерной системы, не являющиеся исполняемыми модулями и подготовленные пользователем или самой системой. При производстве данной экспертизы возможно исследование не только существующих файлов, но и тех, что были удалены.

Чтобы правильно выбрать вид экспертизы, перед оформлением соответствующего постановления необходимо получить консультацию у эксперта. После этого требуется определить экспертную задачу (идентификационную, т. е. установить единый источник происхождения исследуемого объекта, и диагностическую, т. е. установить тех-

[1] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений. С. 154.

[2] Семикаленова А. И. Особенности определения объекта судебной программно-компьютерной экспертизы // Вестник университета имени О. Е. Кутафина. 2015. № 12. С. 73.

нические характеристики исследуемого объекта) и сформулировать связанные с ней вопросы, разрешить которые призван эксперт. Важно помнить о том, что вопросы должны быть корректными, техническими (в том числе вопросы, предполагающие разъяснение терминов), не должны затрагивать правовой стороны и стоимости объекта. Приведем пример.

В неустановленное время, но не позднее 13 января 2018 г., находясь по адресу фактического проживания <адрес>, Д., будучи активным пользователем сети Интернет, вступил в состав организованной группы в целях совершения хищения денежных средств пользователей услуг дистанционного банковского обслуживания путем заражения устройств под управлением операционной системы «Android» вредоносным программным обеспечением и перехвата личной информации.

В ходе обыска у Д. был изъят компьютерный системный блок в корпусе серого цвета с накопителем на жестких магнитных дисках «Toshiba» модель <название> серийный номер <номер> емкостью 1 Тб и флеш-накопителем «Kingston DTSE9» емкостью 8 Гб, а также накопитель на жестких магнитных дисках «Seagate» модель <название> серийный номер <номер> емкостью 250 Гб.

В целях установления наличия на указанных цифровых носителях документов и информации, имеющих значение для уголовного дела, была назначена судебная компьютерно-техническая экспертиза, на разрешение эксперта поставлены следующие вопросы:

1. Какие сведения о посещении интернет-ресурсов, имеются на цифровых носителях информации, представленных на исследование?

2. Имеется ли электронная переписка на цифровых носителях информации, представленных на исследование? Если имеется, то предоставить данные сведения в удобном для ознакомления виде, включая сведения об аккаунтах. Имеется ли электронная переписка посредством программных средств, поддерживающих передачу данных по протоколу XMPP? Если имеется, то осуществить запись данной переписки на оптический диск.

3. Имеются ли на цифровых носителях информации, представленных на исследование, компьютерные программы либо иная компьютерная информация, в том числе для операционной системы Android, определяемые антивирусным программным обеспечением как «вредоносные»?

4. Имеются ли на представленных на исследование носителях информации аутентификационные данные для доступа к веб-ресурсам?

5. Имеются ли на цифровых носителях информации, представленных на исследование, сведения об использовании протокола RDP?

6. Имеются ли на цифровых носителях информации, представленных на исследование, файлы, содержащие сведения о банковских картах, расчетных счетах, денежных переводах, электронных кошельках и криптовалютных кошельках?[1]

Как видим, в приведенном перечне все вопросы корректны, понятны, заданы по существу дела, не затрагивают правовой стороны и иных обстоятельств, исследовать которые эксперт не уполномочен. Корректной и конкретной должна быть и резолютивная часть постановления о назначении экспертизы. По мнению Д. А. Илюшина, современные средства вычислительной техники имеют большие объемы постоянной памяти в виде жестких дисков, в связи с этим эксперт физически не сможет исследовать содержание всего машинного носителя информации за отведенное на экспертизу время. Исходя из сказанного, интересующие следователя вопросы и данные эксперту задания должны быть краткими и информативными[2].

Кроме вопросов, следователь должен позаботится об объектах, которые будут представлены на экспертизу: проверить и оценить их достаточность, оформить их для дальнейшей передачи в судебно-экспертное учреждение. Особое внимание нужно уделить их упаковке: если объектом является внешний носитель информации, его необходимо упаковать и опечатать по местам вскрытия упаковки, когда речь идет о внутреннем, который представляет собой часть технического устройства, его надлежит отделить от устройства, если это возможно, упаковать и опечатать или же передать на экспертизу вместе с устройством, которое также следует упаковать и опечатать[3].

Таким образом, в завершение параграфа заключим, что главные задачи первоначального этапа расследования состоят в поиске и выявлении источников доказательственной информации, проверке

[1] По данным ГУ МВД России по Волгоградской области.

[2] См.: Илюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет С. 167.

[3] См.: Семикаленова А. И. Судебная программно-компьютерная экспертиза по уголовным делам: дис. … канд. юрид. наук. М., 2005. С. 97.

следственных версий, установлении и задержании подозреваемых. В случае совершения хищений электронных денег решить эти задачи можно путем производства таких следственных действий, как допрос потерпевшего, который часто является единственным источником информации, осмотр места происшествия (местонахождения потерпевшего, киберпространства), обыск и выемка (если установлено местонахождение подозреваемого), осмотр предметов и документов, назначение судебной компьютерно-технической экспертизы.

ГЛАВА 3 ПОСЛЕДУЮЩИЙ И ЗАВЕРШАЮЩИЙ ЭТАПЫ РАССЛЕДОВАНИЯ ХИЩЕНИЙ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

3.1. Специфика последующего этапа расследования хищений электронных денежных средств

Цель последующего этапа расследования преступлений заключается в сборе доказательств, достаточных для принятия решения об окончании предварительного следствия. По мнению М. В. Кардашевской, Е. С. Шипиловой, основными задачами данного этапа являются:

«1. Раскрытие преступления, если это не было сделано на первоначальном этапе.

2. Сбор, анализ и оценка всех необходимых доказательств, подтверждающих или опровергающих вину подозреваемого лица в совершении преступления.

3. Розыск скрывшегося обвиняемого.

4. Установление соучастников, если это не было сделано на первоначальном этапе, дополнительных эпизодов преступной деятельности, местонахождения похищенного.

5. Изучение личности обвиняемого»[1].

Продолжительность последующего этапа, как и первоначального, обратно пропорциональна информационной составляющей: первая больше, если вторая меньше. Его основная направленность непосредственно зависит от проведенных следственных действий и оперативно-разыскных мероприятий, следственной ситуации, сложившейся на момент окончания первоначального этапа расследования. Кроме того, как отмечает Н. Г. Шурухнов, здесь необходимо принимать во внимание позиции подозреваемых, уровень и интенсивность их противодействия расследованию[2]. Исходя из этого, на последующем этапе возможны такие следственные ситуации, как:

---

[1] Кардашевская М. В., Шипилова Е. С. Этап процесса расследования и их характеристика. С. 11.

[2] См.: Шурухнов Н. Г. Тактические и технологические основы проведения следственных действий при разрешении следственных ситуаций последующего этапа расследования фальшивомонетничества // Вестник Восточно-Сибирского института МВД России. 2013. № 2 (65). С. 18.

– лицо, совершившее преступление установлено, но не признает себя виновным и отказывается от дачи показаний;

– лицо, совершившее преступление, частично признает себя виновным;

– лицо, совершившее преступление, полностью признает себя виновным и сотрудничает со следствием.

Самой сложной следственной ситуацией, естественно, является первая. В целях ее разрешения некоторые авторы рекомендуют выполнить приведенный далее алгоритм действий:

– преодолеть отказ от дачи показаний, принять меры по недопущению противодействия расследованию;

– оценить имеющиеся по делу доказательства;

– выявить новые следы, свидетельствующие о совершении преступления[1].

Для этого нужно провести допрос подозреваемого, эксперта, дополнительный допрос потерпевшего, в случае с хищениями электронных денег также следует допросить сотрудников кредитных организаций, оператора электронной платежной системы, интернет-провайдера в случае необходимости провести проверку показаний на месте и следственный эксперимент. Кроме того, надлежит дать поручение оперативному подразделению о проведении оперативно-разыскных мероприятий, направленных на получение дополнительной информации по уголовному делу.

Сделаем акцент на допросе подозреваемого. По мнению Е. С. Шевченко, во время подготовки к нему особое внимание нужно уделить личности допрашиваемого лица. При этом важными источниками получения данных будут «анализ учебной и (или) трудовой деятельности лица; назначение судебно-психологических или судебно-психиатрических экспертиз и учет их заключений; непосредственное наблюдение за человеком (эмоции, речь, особенности коммуникации). Результаты анализа учебной и (или) трудовой деятельности лица, соответствующих страниц в социальных сетях… помогут следователю узнать, каким уровнем знаний в области информационных технологий обладает преступник, с чем было сопряжено преступление…»[2]. Безусловно, проанализировать учебную и трудовую деятельность

[1] См.: Гаспарян Г. З. Расследование хищений денежных средств, совершаемых с использованием информационных банковских технологий. С. 209.

[2] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений. С. 88.

подозреваемого, его активность в Интернете (социальные сети, мессенджеры, посещаемые страницы и т. д.) нужно, однако необходимо помнить о том, что, как мы указывали ранее, в случае с хищением электронных денег только 4 % преступников имели специальные знания в области информационных технологий, остальные же приобрели навыки пользования платежными системами, инструментами сокрытия своих действий в сети Интернет и т. д. самостоятельно. Кроме того, лишь 4 % преступников имели психическое расстройство личности, что говорит об умышленном и спланированном характере большинства совершаемых преступлений.

С учетом сказанного полагаем, что ведущую роль при подготовке к допросу подозреваемого и во время его производства стоит отвести наблюдению и основанным на нем криминалистическому профайлингу и верификации. Первый сегодня связывают, прежде всего, с безынструментальной детекцией лжи: он базируется на понимании того, что человек чувствует дискомфорт, когда говорит неправду. «Обманщик прекрасно осознает, что может быть разоблачен и наказан. И скрывать свои истинные чувства тем сложнее, чем масштабнее обман»[1]. Однако это не совсем верно: выявление лжи, сокрытия и искажения информации – задача верификации (от лат. verus – «истинный» и facere – «делать»). Профайлинг же – это «совокупность психологических методов и методик оценки и прогнозирования поведения человека на основе анализа наиболее информативных частных признаков, характеристик внешности, невербального и вербального поведения»[2]. Он может быть полезным тогда, «когда требуется быстрая оценка личности и ее основных характеристик для прикладного использования этих знаний в целях построения эффективной коммуникации»[3].

При производстве следственных действий ключевыми задачами профайлинга и верификации являются:

– осуществление психологической диагностики;

---

[1] См.: Обмани меня: профайлер о шокирующей практике, мифах и тонкостях профессии. URL: https://news.rambler.ru/other/44770099-obmani-menya-profayler-o-shokiruyuschey-praktike-mifah-i-tonkostyah-professii/ (дата обращения: 22.09.2021).

[2] Васильева Н. Ю., Мадянов А. В., Болховитина С. Н. Использование методов профайлинга и верификации в ходе предварительного расследования. URL: https://www.b17.ru/article/98851/ (дата обращения: 22.09.2021).

[3] См.: Филатов А. Профайлинг. Как научиться разбираться в людях и прогнозировать их поведение. М.: Перо, 2016. С. 10.

– диагностика ложных показаний;
– побуждение к даче правдивых показаний;
– реализация приемов правомерного психологического воздействия;
– прогнозирование дальнейшего поведения.

Н. Ю. Васильева, А. В. Мадянов и С. Н. Болховитина отмечают, что возможность использования при допросе подозреваемого методик верификации и профайлинга детерминирована «наличием в мозге человека нейронных популяций, которые различно реагируют на правильное и ошибочное выполнение деятельности, будь то в связи с дефектом восприятия (ранняя реакция) или с дефектом реализации (поздняя реакция). Данный феномен в психологии обозначен как „детектор ошибок“, который активизируется при рассогласовании деятельности с ее планом, точнее, с хранящейся в мозге матрицей»[1]. Из этого следует, что лицо, оказывающее противодействие сотрудникам правоохранительных органов либо занимающее «нейтрально-пассивную позицию стороннего наблюдателя»[2], создает для себя ложный образ события, часто находится в состоянии эмоционального напряжения и тревоги, что затрудняет адекватную оценку происходящего и контроль собственного поведения. Соответственно, «приближение сотрудника правоохранительных органов к так называемой „опасной зоне“ потенциального преступника… будь то значимая тема в ходе допроса, место хранения предметов в ходе обыска, место преступления в ходе осмотра и/или проверки показаний… приводит к активизации в мозгу тех очагов, которые связаны с событием преступления и его последствиями, и это обстоятельство не может не сказаться на поведении человека так же, как и удаление от „опасной зоны“»[3]. Именно методы профайлинга и верификации позволяют определить такие «опасные зоны». Для этого важно обращать внимание на мимику (проявление эмоций на лице человека), жесты (активная жестикуляция, ее отсутствие, открытые жесты (ладони вверх), закрытые (пальцы сжаты, ладони вниз) и т. д.), позу (открытая, закрытая), речь (быстрая, медленная,

[1] Васильева Н. Ю., Мадянов А. В., Болховитина С. Н. Использование методов профайлинга и верификации в ходе предварительного расследования. URL: https://www.b17.ru/article/98851/ (дата обращения: 22.09.2021).
[2] Там же.
[3] Там же.

сбивчивая, нелогичная, с хезитациями – речевыми колебаниями, которые возникают во время спонтанной речи при подборе слов, грамматических конструкций (звуки типа «ммм», «ээээ», «нууу») и т. д.), а также на признаки и состояния, не контролируемые сознанием и зависящие от активности вегетативной нервной системы (покраснение и побледнение кожных покровов, потливость, учащенное дыхание и сердцебиение, облизывание губ, связанное с сухостью во рту, изменение тембра, покашливание, моргание и т. д.). Кроме того, стоит следить за тем, чтобы допрашиваемый не уходил от темы, предмета разговора, если он пытается отвлечь от них внимание, это тоже может быть свидетельством приближения к «опасным зонам».

Анализ речи, мимики, жестов, стиля мышления, поведения и внешнего облика человека в целом позволяет построить его психологический профиль, на основе которого можно сформировать представление о личностных качествах, характере и темпераменте, привычных стратегиях лжи и сокрытия информации, поведении в конфликтных ситуациях, об эмоциональной сфере и убеждениях, что, в свою очередь, поможет спрогнозировать вероятное поведение субъекта в той или иной ситуации, а также понять, каким образом оказать на него правомерное эмоциональное воздействие. С точки зрения Р. Л. Ахмедшина «областями воздействия на личность преступника… будут являться:

– сфера ценностей личности (то, что представляет для человека интерес во внешнем мире);

– сфера отношений личности (то, чем руководствуется человек для достижения своего интереса);

– сфера притязаний личности (то, каким способом человек реализует свой интерес)»[1].

Первая из них во многом обусловливает мотивы действий и поступков личности, вторая свидетельствует о влиянии на нее различных обстоятельств, интересов, третья говорит о самооценке человека (завышенной, адекватной, заниженной), т. е. о том, как он относится к собственным возможностям и способностям. Знание этих сфер поможет повысить эффективность тактических приемов,

[1] Ахмедшин Р. Л. Криминалистическая характеристика личности преступника» и «воздействие»: содержательная взаимосвязь // Вестник Томского государственного университета. 2006. № 292-1. С. 66.

применяемых следователями во время допроса подозреваемого, в частности стимулирования положительных качеств допрашиваемого и использования его слабых мест (пристрастие, привязанность, тщеславие и др.). Именно они, по мнению Е. В. Чернышевой, наряду с приемами искаженного представления об осведомленности, уверенности в раскрытии преступления и предъявления допрашиваемому изобличающих доказательств наиболее популярны среди следователей[1].

В целях повышения эффективности допроса подозреваемого могут использоваться такие методики, как опросник Н. Гордона или интервью судебной оценки – структурированная беседа, по результатам которой по определенному алгоритму оценивается содержательная составляющая ответов и невербальное поведение лица, на основе чего делаются выводы о его вероятной причастности либо непричастности к совершенному преступлению[2]; когнитивное интервью – метод получения достоверной информации, базирующийся на психологических процессах (социальная динамика, память, сознание, коммуникация) и способствующий «активизации памяти у подозреваемого, ориентированного на достоверную информацию, у подозреваемого, сообщающего ложные сведения, наблюдается обратный эффект»[3]. Полагаем, данные методики стоит применять тогда, когда речь идет о «профессиональных» мошенниках (в нашем случае это создатели фейковых интернет-магазинов, ложных объявлений в социальных сетях и на торговых площадках, а также злоумышленники, осуществляющие телефонные звонки от имени кредитных организаций и оказывающие псевдопомощь на рынке брокерских услуг), поскольку их отличают изобретательность, циничность, самоуверенность, знание психологии, умения легко коммуницировать и втираться в доверие и т. д. Л. А. Сухомлинова пишет:

---

[1] Чернышева Е. В. Эффективность психологических тактик взаимодействия с допрашиваемым лицом при расследовании преступлений // Прикладная юридическая психология. 2018. № 4 (45). С. 74–75.

[2] См.: В профайлинге и верификации лжи существует довольно много стандартов проведения интервью. URL: https://proprofiling.com/faint_inerview (дата обращения: 22.09.2021).

[3] Холевчук А. Г. Использование тактики когнитивного интервью в целях получения достоверной информации о запланированных действиях допрашиваемого: современные зарубежные подходы // Международный научный журнал «Инновационная наука». 2015. № 11. С. 193.

«Говоря о психических качествах личности, занимающейся мошенничеством, необходимо выделить определенную стойкость характера. Как правило, это люди, представляющие характер организации и реализации правоохранительной деятельности; опытные, знающие, в чем их могут уличить и какие доказательства могут быть против них собраны»[1], соответственно, уровень их противодействия расследованию будет выше, чем у тех, кто совершил преступление, например, в состоянии алкогольного опьянения, воспользовавшись свободным доступом к электронному кошельку потерпевшего.

Существенную пользу профайлинг и верификация могут принести и при производстве проверки показаний на месте и следственного эксперимента.

В соответствии с ч. 2 ст. 194 УПК РФ «проверка показаний на месте заключается в том, что ранее допрошенное лицо воспроизводит на месте обстановку и обстоятельства исследуемого события, указывает на предметы, документы, следы, имеющие значение для уголовного дела, демонстрирует определенные действия. Какое-либо постороннее вмешательство в ход проверки и наводящие вопросы недопустимы»[2]. Во время этого следственного действия следователь проводит сравнение нескольких информационных потоков: показаний, данных подозреваемым на допросе, результатов иных следственных действий и показаний, получаемых непосредственно во время проведения проверки.

Отметим, что в случаях совершения хищений электронных денежных средств проверка показаний на месте может производиться, когда речь идет об их краже при непосредственном контакте с устройством потерпевшего.

Рассматриваемое следственное действие складывается из трех этапов: подготовительного, рабочего и заключительного. В рамках первого выделяют стадию допроса, где проверяемому лицу предлагают повторить свои предыдущие показания, ответить на уточняющие вопросы и продемонстрировать некоторые действия, не требующие выезда на место проверки; стадию планирования и подго-

---

[1] Сухомлинова Л. А. Технико-криминалистические и организационные основы выявления и расследования мошенничества в сфере обязательного страхования гражданской ответственности владельцев транспортных средств: дис. …канд. юрид. наук. Волгоград, 2008. С. 93.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. URL: www.consultant.ru (дата обращения: 11.09.2021).

товки иных элементов (выбор времени производства следственного действия, определение круга его участников (не менее двух понятых), подготовка технико-криминалистических средств, изучение личности допрашиваемого, обеспечение участников транспортом и т. д.). Кроме того, как отмечает П. А. Картавский, перед выездом подозреваемому целесообразно предложить собственноручно нарисовать схему, отражающую расположение места проверяемого события, подходы к нему, обстановку. Это будет свидетельствовать о добровольности его действий и осведомленности о деталях проверяемых событий[1].

Рабочий этап проверки показаний на месте включает в себя движение к исходному пункту, по опорным пунктам и к конечному пункту. Начинать производство следственного действия необходимо со сбора и инструктажа его участников (это можно сделать в кабинете следователя). Им надлежит разъяснить их права и обязанности, описать порядок и условия проведения проверки. После этого только при наличии добровольного согласия подозреваемого осуществляется выезд на место следственного действия. Маршрут движения определяет следователь.

На месте проведения проверки необходимо расположить ее участников так, чтобы не сковывать действий подозреваемого, исключить возможность его побега, причинения им вреда кому-либо из находящихся здесь, обеспечить условия для фото- или видеофиксации хода и результатов следственного действия, после этого предоставить инициативу подозреваемому. Он должен рассказать об обстановке совершения преступления, показать предметы, продемонстрировать некоторые действия: например, в случае кражи электронных денег пояснить, где находилось устройство потерпевшего, с помощью которого был осуществлен перевод денежных средств; если потерпевший был в том же помещении, указать, где именно располагался он, почему не мог видеть действий подозреваемого, и т. д. Затем необходимо перейти к другому опорному пункту, если таковой имеется. В нашем случае это может быть место встречи с соучастником для передачи банковской карты или банкомат, где произошло снятие похищенных денег. Во время движения к нему подозреваемый должен идти чуть впереди остальных. По прибытии он снова дает пояснения и демонстрирует определенные действия.

[1] См.: Картавский П. А. Некоторые приемы тактики проверки показаний на месте // Научный компонент. 2019. № 2 (2). С. 26.

Далее за подозреваемым все переходят к конечному пункту, которым может быть и последний опорный пункт.

Нужно помнить о том, что в рассказ проверяемого лица никто не должен вмешиваться, задавать наводящие вопросы, иначе возникнут сомнения в достоверности следственного действия, а его результаты потеряют доказательственное значение. Согласимся с точкой зрения Т. В. Вагабова, согласно которой проверка показаний на месте эффективна лишь тогда, когда в ходе ее производства «подозреваемый… не только дает новые или повторяет ранее данные им показания, но и самостоятельно и четко указывает место совершенного преступления; демонстрирует осведомленность об обстановке места совершения преступления… и обстоятельствах его совершения; указывает на соответствующие происшедшему следы, преступления, сокрытые орудия и средства совершения преступного деяния… иные предметы и документы, в том числе ранее не выявленные следствием; самостоятельно, четко и детально воспроизводит на месте происшествия механизм… действий в момент совершения преступления..; делает соответствующие ранее данным показаниям их дополнения и уточнения на месте происшествия…»[1]. Важным аспектом следственного действия также является наблюдение за подозреваемым (его мимикой, жестами, речью и т. д.) в целях выявления «опасных зон» и лжи.

Заключительный этап проверки показаний на месте предполагает составление протокола, плана места проведения проверки, схемы маршрута движения; процессуальное оформление и упаковку обнаруженных предметов; завершение фото- или видеосъемки; ее просмотр всеми участниками следственного действия; фиксацию их замечаний; занесение в протокол пометки о просмотре.

Кроме того, «в целях проверки и уточнения данных, имеющих значение для уголовного дела, следователь вправе произвести следственный эксперимент путем воспроизведения действий, а также обстановки или иных обстоятельств проверяемого события»[2].

---

[1] Вагабов Т. М. Тактические особенности проведения проверки показаний на месте в системе мер преодоления лжи со стороны подозреваемого (обвиняемого) // Известия Тульского государственного университета. Экономические и юридические науки. 2014. № 2-2. С. 53.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. URL: www.consultant.ru (дата обращения: 11.09.2021).

Следственный эксперимент состоит их трех этапов: подготовительного, экспериментального и заключительного. Первый охватывает время до выезда на место эксперимента и непосредственно на месте. В рамках этого этапа следователю необходимо:

– предварительно ознакомиться с обстановкой совершения преступления, особенностями эксплуатации технических средств, которые использовал злоумышленник;

– воссоздать условия совершения преступления. В случаях с хищениями электронных денег наибольшее внимание должно быть уделено именно устройствам (надлежит выяснить характеристики компьютерной системы, компьютерной сети, установить вид программного обеспечения, периферийное оборудование и т. д.). *При производстве следственного эксперимента важно использовать подлинные или аналогичные технические устройства*;

– с помощью специалиста продумать содержание опытных действий;

– определить время проведения эксперимента и круг его участников (понятые (в идеале должны иметь навыки пользования информационно-телекоммуникационными технологиями), специалист и др.), обеспечить их явку;

– составить план проведения следственного эксперимента;

– подготовить средства фото- или видеофиксации хода и результатов следственного действия, транспорт и т. д.

На месте эксперимента нужно зафиксировать обстановку, провести инструктаж участников, организовать охрану.

Экспериментальный этап предполагает проведение опытных действий и их неоднократное повторение. Отметим, что при расследовании киберпреступлений, в том числе хищений электронных денежных средств, различают такие виды следственного эксперимента, как «по проверке возможности подключения компьютерной техники и совершения действий с использованием определенной криминальной (компьютерной) технологии; по проверке подбора паролей, идентификационных кодов и установлению периода… для данного подбора; по проверке возможности подключения к компьютерной сети и использования криминальной (компьютерной) технологии; по проверке возможности электромагнитного перехвата; по установлению периода… необходимого на отключение технических средств защиты информации; по установлению промежутка времени, необходимого для модификации, копирования компьютерной информации; по про-

верке возможности совершения определенных действий в киберпространстве в одиночку и др.»[1]. Совершать экспериментальные действия нужно поэтапно. Это позволяет наблюдать их во всех стадиях, облегчает их восприятие и фиксацию.

Большую роль в производстве следственного эксперимента при расследовании хищений электронных денег играет специалист, поскольку здесь необходимы специальные знания в области информационно-телекоммуникационных технологий, особенно если была совершена кража с использованием вредоносного программного обеспечения. Именно он может помочь следователю воссоздать обстановку совершения преступления, подобрать нужные технические средства, определить порядок, условия и содержание опытных действий, зафиксировать полученные результаты.

Как и при проведении проверки показаний на месте, во время следственного эксперимента важно осуществлять постоянное наблюдение за подозреваемым в целях выявления лжи, искажения или сокрытия информации.

На заключительном этапе оформляется протокол следственного действия, учитываются замечания его участников, делается отметка о составленных планах и схемах, фото- или видеосъемке, об ознакомлении всех участников с протоколом.

Скажем несколько слов о других следственных ситуациях последующего этапа расследования хищений электронных денег. Так, если лицо, совершившее преступление, частично признает себя виновным, рекомендуется повторно допросить его, эксперта, провести дополнительные допросы потерпевшего и свидетелей в целях уточнения и детализации показаний, выявить дополнительные следы преступления, провести комплекс следственных и процессуальных действий, способствующих формированию доказательственной базы (очная ставка, проверка показаний на месте, следственный эксперимент, назначение экспертизы). Если лицо, совершившее преступление, полностью признает себя виновным и сотрудничает со следствием, необходимо проанализировать имеющуюся в уголовном деле информацию, исключить самооговор, собрать факты, доказывающие вину именно этого лица.

[1] Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений. С. 148.

В завершение параграфа отметим, что последующий этап расследования хищений электронных денежных средств, как и первоначальный, носит поисково-разведывательный характер. Его главная цель состоит в сборе доказательств, достаточных для принятия решения об окончании предварительного следствия. Достижение данной цели предполагает решение комплекса задач, в числе которых стоит назвать и преодоление противодействия расследованию. Для этого можно использовать методики верификации и профайлинга, направленные на выявление признаков лжи, сокрытия и искажения информации, а также на установление психологического контакта с лицом, прогнозирование его поведения на основе анализа невербального и вербального поведения, внешности в целом. Указанные методики могут применяться при производстве таких следственных действий, как допрос подозреваемого, проверка показаний на месте, обыск, следственный эксперимент.

3.2. Криминалистические проблемы расследования хищений электронных денежных средств на завершающем этапе

В связи с тем что основу завершающего этапа расследования преступлений составляют не следственные, а процессуальные действия, он редко анализируется в научных работах по криминалистике и «практически не находит освещения в видовых методиках»[1]. Однако, как пишут М. В. Кардашевская, Е. С. Шипилова, этот этап играет важную роль в процессе расследования, имеет значительную криминалистическую специфику, а от работы следователя здесь зависят результаты рассмотрения уголовного дела в суде[2].

Основными задачами завершающего этапа расследования являются подведение его итогов и составление обвинительного заключения. Соответственно, содержание этапа складывается из организационных и организационно-технических мероприятий, необходимых для завершения расследования, и аналитической работы следователя при составлении обвинительного заключения[3]. При этом к пер-

[1] Кардашевская М. В., Шипилова Е. С. Этап процесса расследования и их характеристика. С. 12.
[2] Там же.
[3] Там же.

вым относится «нейтрализация возможных вредных для расследования последствий, вызванных ознакомлением обвиняемых и адвокатов с материалами дела, а также ряд технических вопросов»[1].

На завершающем этапе расследования преступления следователь должен:

– ознакомить обвиняемого и иных участников уголовного процесса с материалами уголовного дела;

– рассмотреть заявленные ходатайства (о дополнительном допросе свидетелей, проведении дополнительных экспертиз, приобщении дополнительного характеризующего материала и т. д.) и принять по ним обоснованные решения;

– в случае необходимости провести дополнительные следственные действия;

– ознакомить стороны с дополнительными материалами уголовного дела, если таковые имеются;

– составить обвинительное заключение.

По справедливому замечанию Л. Я. Драпкина, В. Н. Карагодина, именно дополнительные следственные действия «могут привести к коренному изменению традиционного характера этого этапа и возникновению ситуаций, типичных не только для последующего, но и для первоначального этапов расследования. Однако… производство заключительных действий параллельно с последующими и первоначальными следственными действиями в большинстве случаев практически невозможно. Поэтому при возникновении ситуаций, типичных для первоначального или последующего этапов, процесс расследования должен быть „возвращен“ на соответствующий этап, вновь приобретая его отличительные черты и качества»[2].

На завершающем этапе расследования преступлений отдельное внимание нужно уделить доказательствам. Так, при составлении обвинительного заключения следователю надлежит проанализировать и оценить их в совокупности. При этом «нужно логически сопоставить каждое отдельное доказательство с его источником, выяснить, подкрепляется ли оно или, напротив, опровергается другими доказательствами… Доказательства должны иметь достоверные, проверенные источ-

[1] Кардашевская М. В., Шипилова Е. С. Этап процесса расследования и их характеристика. С. 12.

[2] Драпкин Л. Я., Карагодин В. Н. Криминалистика. С. 362.

ники и выстраиваться в единую логическую цепь, быть прямо или косвенно связанными с преступлением»[1]. Некоторые авторы отмечают, что расследование преступлений, совершенных с использованием возможностей сети Интернет, в том числе хищений электронных денежных средств, сопряжено с трудностями доказывания, и задают вопросы «Чего полученные доказательства будут стоить в суде? А главное – будут ли они признаны и поняты судом?»[2]. Действительно, проблемы вызывает приобщение к материалам уголовного дела в качестве доказательств электронной переписки и информации, содержащейся на интернет-сайтах. Еще труднее предоставить доказательства принадлежности страницы в социальной сети и подтвердить подлинность лог-файлов.

В соответствии с процессуальным законодательством Российской Федерации доказательства оцениваются с точки зрения их допустимости, достоверности и достаточности. Согласно ч. 2 ст. 74 УПК РФ в качестве доказательств допускаются показания подозреваемого, обвиняемого, потерпевшего, свидетеля; заключение и показания эксперта; заключение и показания специалиста; вещественные доказательства; протоколы следственных и судебных действий; иные документы, если изложенные в них сведения имеют значение для установления некоторых обстоятельств дела (ст. 84 УПК РФ). Такие документы могут содержать информацию, зафиксированную в письменном или другом виде[3]. Мы не будем вступать в дискуссию о том, быть или не быть электронным доказательствам в уголовном процессе, укажем лишь некоторые факты, на которые стоит обратить внимание следователю при составлении обвинительного заключения.

Так, важно помнить о том, что доказательства могут быть получены только уполномоченными лицами путем производства следственных и процессуальных действий, предусмотренных УПК РФ, т. е., если речь идет, например, о переписке в электронной почте, мессенджерах, социальных сетях, журналах логов и т. д., они должны

[1] Кардашевская М. В., Шипилова Е. С. Этап процесса расследования и их характеристика. С. 12.

[2] См.: Почему так сложно преследовать киберпреступников? URL: https://www.securitylab.ru/blog/personal/bezmaly/344477.php (дата обращения: 14.09.2021).

[3] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. URL: www.consultant.ru (дата обращения: 22.09.2021).

быть получены в ходе обыска, следственного эксперимента, выемки электронной информации с компьютеров поставщиков услуг. Следователю надлежит проанализировать реквизиты сообщений: отправитель, получатель, тема, если она есть, время отправки, содержание сообщения (источник получения доказательства не должен быть анонимным), – и назначить экспертизу в целях установления подлинности электронной переписки. Однако здесь нужно подчеркнуть, что эксперт может подтвердить только отсутствие каких-либо вмешательств в нее.

В идеале оценка всех электронных доказательств должна производиться с участием специалиста, кроме того, при осмотре места происшествия и изъятии электронных документов должны присутствовать достаточно компетентные понятые, которые бы понимали смысл действий следователя и специалиста[1] и могли подтвердить их законность. Особую актуальность это приобретает при изъятии лог-файлов, поскольку их подлинность всегда вызывает сомнения. Применительно к ним защитники обычно задают следующие вопросы: как мы можем быть уверены, что файл журнала логов не был изменен; кто имел доступ к файлу; вы уверены в том, что метки даты и времени точны; как мы узнаем, что ваша компьютерная система точно обнаружила исходный IP-адрес, не могут ли быть подменены IP-адреса; какова цепочка хранения этого файла журнала с момента его создания до сих пор; каков опыт работы специалиста и следователя в получении юридических доказательств и др.[2]

Необходимо помнить о том, что доказательством может служить только корректный и неизменный журнал логов, в связи с этим при анализе лога следователю нужно работать исключительно с копиями, чтобы не повредить оригинал.

В рамках уголовного дела различают три категории логов:

– принадлежащие потерпевшему;

– принадлежащие подозреваемому (обвиняемому);

– принадлежащие третьим лицам (интернет-провайдеру, хостинговой компании).

---

[1] О доказательственном значении лог-файлов. URL: https://www.securitylab.ru/analytics/216291.php (дата обращения: 24.09.2021).

[2] См.: Почему так сложно преследовать киберпреступников? URL: https://www.securitylab.ru/blog/personal/bezmaly/344477.php (дата обращения: 14.09.2021).

Поскольку лог-файлы довольно легко изменить, первые две категории имеют наименьшую доказательственную силу. Подтвердить их неизменность может только экспертиза.

В случае с информацией, размещенной на интернет-сайтах, и электронной перепиской нужно подтвердить их допустимость. Для этого недостаточно сделать простой скриншот страницы и предоставить его суду. Необходимо доказать, что именно на этом сайте или странице в социальной сети в определенную дату была размещена соответствующая информация, а также что данный сайт или страница принадлежат именно этому лицу. Для выяснения указанных обстоятельств стоит обратиться к регистратору доменных имен, а в случае его отказа дать нужные сведения, – в суд.

На завершающем этапе расследования следователю надлежит обратить внимание и на показания потерпевшего, свидетелей и обвиняемого. М. В. Кардашевская, Е. С. Шипилова отмечают, что «показания свидетелей и обвиняемых лишь в редких случаях полностью согласуются между собой и складываются вместе с другими доказательствами в единую систему доказательств, подтверждающих предъявленное обвинение. В ситуациях, когда принятыми мерами противоречия в показаниях свидетелей и обвиняемых устранить не удалось, следователь должен по своему внутреннему убеждению выбрать именно те показания, которые в большей степени отвечают требованиям достоверности, допустимости и достаточности»[1]. Если допрашиваемые лица неоднократно меняли свои показания, их оценка происходит на основании того, насколько полно были сообщены обстоятельства совершенного деяния. Здесь стоит указать, что, в случае с потерпевшим и свидетелями, как правило, наиболее достоверными являются первоначальные показания, поскольку событие преступления еще сохраняется в их памяти в деталях.

После оценки доказательств, ознакомления всех участников с материалами уголовного дела следователь составляет обвинительное заключение – процессуальный документ, которым завершается предварительное следствие. Основанием для этого выступает необходимая и достаточная совокупность доказательств, достоверно

[1] Кардашевская М. В., Шипилова Е. С. Этап процесса расследования и их характеристика. С. 13.

устанавливающая все обстоятельства, подлежащие доказыванию, сформированная в результате всестороннего, полного и объективного их исследования и оценки[1]. Обвинительное заключение должно отвечать всем требованиям, указанным в ст. 220 УПК РФ[2], иначе будет исключена возможность постановления судом приговора и уголовное дело будет возвращено прокурору.

Резюмируя сказанное, еще раз отметим, что завершающий этап расследования преступлений складывается из процессуальных действий, необходимых для завершения расследования, некоторых организационно-технических мероприятий и аналитической работы следователя при составлении обвинительного заключения. При расследовании хищений электронных денежных средств на данном этапе особое внимание нужно обратить на допустимость, достоверность и достаточность электронных доказательств (электронной переписки, информации, содержащейся на интернет-сайтах, журналов логов).

[1] Гумеров Т. А. Обвинительное заключение: правовая природа, содержание, процессуальные последствия: моногр. М.: Юрлитинформ, 2011. 216 с.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. URL: www.consultant.ru (дата обращения: 22.09.2021).

ЗАКЛЮЧЕНИЕ

Пандемия коронавирусной инфекции COVID-19 в очередной раз подтвердила, что сегодня Интернет является одной из самых популярных и удобных площадок для ведения бизнеса, работы, получения образования, торговли и т. д., а электронная коммерция открывает новые возможности для покупателей и продавцов. Естественно, подобные условия требуют особой системы расчетов – безналичными или электронными денежными средствами, доля которых в торговом розничном обороте растет с каждым годом[1].

Электронные деньги представляют собой валюту, эквивалентную наличным деньгам, существующую в виде цифровой записи и не требующую открытия банковского счета. Их назначение состоит в создании универсальной платежной среды, способной объединить покупателя и продавца[2]. В настоящее время электронными денежными средствами пользуются примерно 42 % россиян в основном для оплаты счетов и онлайн-покупок[3].

Популярность электронных денег обусловила рост числа криминальных посягательств, совершаемых в отношении них, – краж и так называемых «дистанционных» мошенничеств, что, в свою очередь, диктует необходимость совершенствования существующей методики их расследования. Особую важность здесь приобретает повышение эффективности взаимодействия между правоохранительными органами, кредитными организациями, операторами сотовой связи, операторами платежных систем и интернет-провайдерами, что может быть достигнуто путем заключения соглашений об обмене информацией в электронном виде, где будут четко прописаны сроки исполнения требований первых.

---

[1] См.: ЦБ: Доля безналичных платежей вырастет до 75 % за 3–5 лет. URL: https://finance-rambler-ru.turbopages.org/turbo/finance.rambler.ru/s/money/46030635-tsb-dolya-beznalichnyh-platezhey-vyrastet-do-75-za-3-5-let/ (дата обращения: 23.09.2021).

[2] См: Казимагомедова З. А., Атемова А. З. Электронные деньги в современном мире. С. 36.

[3] См.: Почти половина россиян предпочитает электронные деньги. URL: https://rg-ru.turbopages.org/rg.ru/s/2020/07/15/pochti-polovina-rossiian-predpochitaet-elektronnye-dengi.html (дата обращения: 23.09.2021).

Полагаем, стоит сделать акцент и на сотрудничестве органов внутренних дел с IT-компаниями. Благодаря ему можно получить доступ к программам и модулям, ориентированным на выявление и, что не менее значимо, предупреждение преступлений в сети Интернет, в частности спаминга, мошенничества с использованием технологий социальной инженерии и вредоносного софта и др. Это позволит полиции действовать не реактивно – в ходе расследования совершенного преступления, а проактивно, т. е. предупреждать его, что в случае с кибермошенничествами особенно важно с учетом сложностей их раскрытия и расследования, обусловленных, в том числе, транснациональным характером киберпреступности.

В завершение отметим, что большую роль в противодействии хищениям электронных денежных средств играют не только правоохранители, но и сами граждане: пока вторые не начнут проявлять осторожность в общении с незнакомцами по телефону и в Интернете, бережно относиться к своим личным данным, соблюдать элементарные правила «цифровой гигиены» и продолжат руководствоваться логикой «Деда Мороза», т. е. логикой не тезиса и доказательства, а легенды и вовлеченности в нее, усилия первых будут тщетны.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативные правовые акты и материалы судебной практики

1. Конституция Российской Федерации : текст с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. : [принята всенародным голосованием 12 декабря 1993 г.]. – Текст : электронный // КонсультантПлюс [сайт]. – URL: www.consultant.ru (дата обращения: 10.08.2021).

2. Директива 2000/46/ЕС Европейского Парламента и Совета Европейского Союза от 18 сентября 2000 г. об учреждении и деятельности организаций, эмитирующих электронные деньги, и о пруденциальном надзоре за их деятельностью (отменена). – Текст : электронный // ГАРАНТ.РУ [сайт]. – URL: https://base.garant.ru/2569190 (дата обращения: 02.02.2021).

3. Директива 2009/110/ЕС Европейского Парламента и Совета Европейского Союза от 16 сентября 2009 г. об организации, деятельности и пруденциальном надзоре за деятельностью учреждений электронных денег, вносящая изменения в директивы 2005/60/ЕС и 2006/48/ЕС и отменяющая Директиву 2000/46/ЕС (распространяется на Европейскую экономическую зону). – Текст : электронный // ГАРАНТ.РУ [сайт]. – URL: https://base.garant.ru/71312234 (дата обращения: 02.02.2021).

4. Report of Electronic Money // European Central Bank. – Frankfurt am Main. – August, 1998. – 47 p.

5. Survey of Electronic Money Developments // Bank for International Settlements. Committee on Payment and Settlement Systems. – Basel, Switzerland. – May, 2000. – 104 p.

6. The EU's Cybersecurity Strategy for the Digital Decade (Brussels, 16th December 2020). – Текст : электронный // European Commission [сайт]. – URL: ec.europa.eu (дата обращения: 03.03.2021).

7. Уголовно-процессуальный кодекс Российской Федерации : УПК РФ : текст с изменениями от 23 сентября 2021 г. : [принят Государственной Думой 22 ноября 2001 г. : одобрен Советом Федерации 5 декабря 2001]. – Текст : электронный // КонсультантПлюс [сайт]. – URL: www.consultant.ru (дата обращения: 22.09.2021).

8. Уголовный кодекс Российской Федерации : УК РФ : текст с изменениями от 11 июня 2021 г. : [принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г.]. – Текст : электронный // КонсультантПлюс [сайт]. – URL: www.consultant.ru (дата обращения: 21.06.2021).

9. О банках и банковской деятельности : Федеральный закон № 395-1 : [принят 2 декабря 1990 г.]. – Текст : электронный // ГАРАНТ.РУ [сайт]. – URL: https://base.garant.ru/10105800 (дата обращения: 12.08.2021).

10. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : Федеральный закон № 115-ФЗ : [принят Государственной Думой 13 июля 2001 г. : одобрен Советом Федерации 20 июля 2001 г]. – Текст : электронный // КонсультантПлюс [сайт]. – URL: www.consultant.ru (дата обращения: 27.07.2021).

11. О полиции : Федеральный закон № 3-ФЗ : [принят Государственной Думой 28 января 2011 г. : одобрен Советом Федерации 2 февраля 2011 г]. – Текст : электронный // КонсультантПлюс [сайт]. – URL: www.consultant.ru (дата обращения: 11.08.2021).

12. О национальной платежной системе : Федеральный закон № 161-ФЗ : [принят Государственной Думой 14 июня 2011 г. : одобрен Советом Федерации 22 июня 2011 г.]. – Текст : электронный // КонсультантПлюс [сайт]. – URL: www.consultant.ru. (дата обращения: 02.02.2021).

13. О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон № 111-ФЗ : [принят Государственной Думой 10 апреля 2018 г. : одобрен Советом Федерации 18 апреля 2018 г]. – Текст : электронный // ГАРАНТ.РУ [сайт]. – URL: https://base.garant.ru/71929752/ (дата обращения: 22.07.2021).

14. О внесении изменений в Федеральный закон «О национальной платежной системе» и отдельные законодательные акты Российской Федерации : Федеральный закон № 173-ФЗ : [принят Государственной Думой 25 июня 2019 г. : одобрен Советом Федерации 26 июня 2019 г.] // Российская газета. – 2019. – № 145 (7903).

15. О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений : приказ МВД России от 3 апреля 2018 г. № 196. – Текст : электронный // Управление на транспорте МВД России по Южному федеральному округу [сайт]. – URL: https://43.xn--b1aew.xn--p1ai/Moni/item/13373340 (дата обращения: 10.08.2021).

16. Памятка «Об электронных денежных средствах» : приложение к письму Банка России «О предоставлении клиентам – физическим лицам информации об особенностях оказания услуг по переводу электронных денежных средств» от 11 марта 2016 г. № ИН-017-45/12. – Текст : электронный // ГАРАНТ.РУ [сайт]. – URL: https://base.garant.ru/70576142/53f89421bbdaf741eb2d1ecc4ddb4c33 (дата обращения: 03.04.2020).

17. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. № 51 (утратило силу). – Текст : электронный // ГАРАНТ.РУ [сайт]. – URL: https://base.garant.ru/products/ipo/prime/doc/1685377/ (дата обращения: 10.08.2021)

18. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48. – Текст : электронный // ГАРАНТ.РУ [сайт]. – URL: https://base.garant.ru/71823288 (дата обращения: 21.07.2021).

19. Приговор Центрального районного суда г. Оренбурга № 1-395/2019 от 24 сентября 2019 г. по делу № 1-395/2019. – Текст : электронный // Судебные и нормативные акты РФ [сайт]. – URL: https://sudact.ru/regular/doc/vmW1hq3bpkH/&page...80%D0%B5%D0%B4%D1%8 (дата обращения: 12.08.2021).

20. Приговор Собинского городского суда Владимирской области № 1-1-25/2020 1-1-252/2019 от 28 января 2020 г. по делу № 1-1-25/2020. – Текст : электронный // Судебные и нормативные акты РФ [сайт]. –URL: https://sudact.ru/regular/doc/WVxRhfsp0Hgn..._pos=-3542#snippet (дата обращения: 28.07.2021).

21. Приговор Ленинского районного суда г. Махачкалы № 1-281/2019 от 11 июня 2019 г. по делу № 1-281/2019. – Текст : электронный // Судебные и нормативные акты РФ [сайт]. – URL: https://sudact.ru/regular/doc/u64vRKWrBYVL/ (дата обращения: 21.04.2020).

22. Приговор Мотовилихинского районного суда г. Перми № 1-72/2019 от 20 февраля 2019 г. по делу № 1-72/2019. – Текст : электронный // Судебные и нормативные акты РФ [сайт]. – URL: https://sudact.ru/regular/doc/kgD0AP0FckUW/ (дата обращения: 21.04.2020).

23. Постановление Ленинского районного суда г. Омска № 1-300/-2019 от 24 июня 2019 г. по делу № 1-300/2019. – Текст : электронный // Судебные и нормативные акты РФ [сайт]. – URL: https://sudact.ru/regular/doc/r3Gy6n1iafHw/ (дата обращения: 26.07.2021).

24. Приговор Волжского городского суда (Волгоградская область) № 1-998/2016 по делу № 1-998/2016. – Текст : электронный // Судебные и нормативные акты РФ [сайт]. – URL: https://sudact.ru/regular/-doc/IwoDKKQidEUn/ (дата обращения: 12.08.2021).

25. Приговор Советского районного суда г. Томска № 1-25/2019 1-377/2018 от 9 декабря 2019 г. по делу № 1-275/2018. – Текст : электронный // Судебные и нормативные акты РФ [сайт]. – URL: https://sudact.ru/regular/doc/hktokOrwZgbO/&regular...D1%82%D0%B5%D1%80 (дата обращения: 09.09.2021).

Научная, учебная и справочная литература

1. Балашов, Д. Н. Криминалистика : учебник / Д. Н. Балашов, Н. М. Балашов, С. В. Маликов. – Москва : ИНФРА-М, 2005. – 503 с. – ISBN 5-16-002200-7.

2. Белкин, Р. С. Криминалистика. Краткая энциклопедия / Р. С. Белкин. – Москва : Большая российская энциклопедия, 1993. – 111 с. – ISBN 5-85270-088-6.

3. Белкин, Р. С. Криминалистическая энциклопедия / Р. С. Белкин. – 2-е изд., доп. – Москва : Мегатрон XXI, 2000. – 334 с. – ISBN 5-901391-01-2.

4. Белкин, Р. С. Курс криминалистики : в 3 т. Т. 3. Криминалистические средства, приемы и рекомендации / Р. С. Белкин. – Москва : Юристъ, 1997. – Т. 3. – 480 с.

5. Белкин, Р. С. Курс криминалистики : учеб. пособие / Р. С. Белкин. – 3-е изд, доп. Москва : ЮНИТИ-ДАНА ; Закон и право, 2001. – 867 с. – ISBN 5-238-00198-3.

6. Ведерников, Н. Т. Криминалистическое изучение личности / Н. Т. Ведерников // Криминалистика : учебник / под ред А. Ф. Волынского, В. П. Лаврова. – 2-е изд., перераб. и доп. – Москва : Юнити-Дана ; Закон и право, 2008. – С. 104–123. – ISBN 978-5-238-01398-5.

7. Великородный, П. Г. Идентификационное исследование способа совершения преступлений в целях поиска преступника : монография / П. Г. Великородный. – 2-е изд, испр. и доп. – Москва : Юрлитинформ, 2013. – 138 с. – ISBN 978-5-4396-0474-6.

8. Вехов, В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки : монография / В. Б. Вехов. – Волгоград : Волгоградская академия МВД России, 2008. – 404 с. – ISBN 978-5-7899-0550-0.

9. Викторова, Л. Н. Фактор времени и его значение для раскрытия и расследования преступлений : учеб. пособие / Л. Н. Викторова. – Москва : Изд-во ВНИИ МВД СССР, 1983. – 34 с.

10. Возгрин, И. А. Научные основы криминалистической методики расследования преступлений : курс лекций / И. А. Возгрин. – Санкт-Петербург : Санкт-Петербургский юрид. ин-т МВД России, 1993. – Ч. IV. – 79 с.

11. Волчецкая, Т. С. Современные проблемы моделирования в криминалистике и следственной практике : учеб. пособие / Т. С. Волчецкая. – Калининград : Калининградский гос. ун-т, 1997. – 95 с. – ISBN 5-88874-083-7.

12. Гаврилин, Ю. В. Криминалистическая тактика и методика расследования отдельных видов преступлений : учеб. пособие / Ю. В. Гаврилин. – Москва : Книжный мир, 2004. – 332 с. – ISBN 5-8041-0253-4.

13. Гаврилин, Ю. В. Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы : монография / Ю. В. Гаврилин. – Тула : Левша, 2009. – 361 с. – ISBN 5-86269-214-2.

14. Глоссарий по информационному обществу / под ред. Ю. Е. Хохлова. – Москва : Ин-т развития информационного общества, 2009. – 162 с. – ISBN 978-5-901907-20-7.

15. Гумеров, Т. А. Обвинительное заключение: правовая природа, содержание, процессуальные последствия : монография / Т. А. Гумеров. – Москва : Юрлитинформ, 2011. – 216 с. – ISBN 978-5-93295-927-5.

16. Деньги. Кредит. Банки : учебник / под ред. М. С. Марамыгина, Е. Н. Прокофьевой. – Екатеринбург : Изд-во Уральского ун-та, 2019. – 384 с. – ISBN 978-5-7996-2741-6.

17. Драпкин, Л. Я. Криминалистика : учебник / Л. Я. Драпкин, В. Н. Канрагодин. – 2-е изд., перераб. и доп. – Москва : Проспект, 2016. – 768 с. – ISBN 978-5-392-19433-9.

18. Егоров, Н. Н. Руководство по производству следственных действий : учеб.-практ. пособие / Н. Н. Егоров, Е. П. Ищенко. – Москва : ООО «Проспект», 2017. – 145 с. – ISBN 978-5-392-21124-1.

19. Зуев, Е. И. Криминалистическая характеристика преступлений / Е. И. Зуев, Н. Г. Шурухнов // Криминалистика (актуальные проблемы). – Москва : Академия МВД СССР, 1988.

20. Зуйков, Г. Г. Поиск преступников по признакам способов совершения преступлений : учеб. пособие / Г. Г. Зуйков. – Москва : ВШ МВД СССР, 1970. – 189 с.

21. Ильин, И. А. О сущности правосознания / И. А. Ильин. – Москва : ТОО «Рарог», 1993. – 234 с. – ISBN 5-87372-005-6.

22. Исходные следственные ситуации и криминалистические методы их разрешения : сб. науч. тр. / отв. ред. В. П. Лавров. – Москва : Высшая юрид. заоч. школа, 1991. – 152 с.

23. Ищенко, Е. П. Криминалистика в вопросах и ответах : учеб. пособие / Е. П. Ищенко. – Москва : ООО «Проспект», 2020. – 304 с. – ISBN 978-5-392-30255-0.

24. Ищенко, Е. П. Криминалистика : учебник и практикум / Е. П. Ищенко, Н. Н. Егоров. – Москва : Юрайт, 2020. – 545 с. – ISBN 978-5-9916-7469-0.

25. Колесниченко, А. Н. Криминалистическая характеристика преступлений / А. Н. Колесниченко, В. Е. Коновалова. – Харьков : Юрид. ин-т, 1985. – 93 с.

26. Кон, И. С. Социологическая психология / И. С. Кон. – Москва : Психолого-социальный ун-т ; Воронеж : МОДЭК, 1999. – 554 с. – ISBN 5-89395-106-9.

27. Кочергин, Д. А. Электронные деньги : учебник / Д. А. Кочергин. – Москва : Маркет ДС, 2011. – 422 с. – ISBN 978-5-94416-126-0.

28. Криминалистика : учебник / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская ; под ред. Р. С. Белкина. – Москва : НОРМА (НОРМА–ИНФРА М), 2001. – 990 с. – ISBN 5-89123-302-9 (НОРМА); ISBN 5-86225-949-X (ИНФРА М).

29. Криминалистика : учебник / под ред. А. Н. Васильева. – Москва : Изд-во Московского ун-та, 1971. – 564 с.

30. Криминалистика : учебник / под ред. А. Ф. Волынского, В. П. Лаврова. – 2-е изд., перераб. и доп. – Москва : Юнити-Дана : Закон и право, 2013. – 943 с. – ISBN 978-5-238-01398-5.

31. Криминалистическая методика расследования отдельных видов и групп преступлений : учеб. пособие / В. Д. Зеленский, Г. М. Меретуков, А. В. Гусев, С. А. Данильян. – Краснодар : Кубанский гос. аграр. ун-т, 2013. – 355 с.

32. Криминалистическое изучение личности : науч.-практ. пособие / отв. ред. Я. В. Комиссарова. – Москва : Проспект, 2019. – ISBN 978-5-392-30024-2.

33. Криминология : учебник / отв. ред. В. К. Звирбуль, Н. Ф. Кузнецова, Г. М. Миньковский. – Москва : Юрид. лит., 1979. – 304 с.

34. Кустов, А. М. Криминалистика и механизм преступления. Цикл лекций : учеб.-метод. пособие / А. М. Кустов. – Москва : Московский псих.-социал. ун-т ; Воронеж : МОДЕК, 2002. – 301 с. – ISBN 5-89502-338-X.

35. Лавров, В. П. Криминалистика / В. П. Лавров. – Москва : Норма, 1999.

36. Лаврухин, С. В. Поведение преступника как объект криминалистического моделирования : монография / С. В. Лаврухин. – Саратов : Саратовская государственная академия права, 2005. – 386 с. – ISBN 5-7924-0433-X.

37. Лебедев, В. М. Уголовно-процессуальное право : учебник / В. М. Лебедев. – Москва : Юрайт, 2012. – 403 с.

38. Лихолетов, А. А. Особенности квалификации и расследования преступлений, связанных с хищением денежных средств с использованием платежных карт (ст. 159.3 Уголовного кодекса Российской Федерации) : учеб. пособие / А. А. Лихолетов, П. Е. Кулешов. – Волгоград : Волгоградская академия МВД России, 2018. – 64 с. – ISBN 978-5-7899-1109-9.

39. Лубин, А. Ф. Механизм преступной деятельности / А. Ф. Лубин. – Нижний Новгород : Нижегородский юрид. ин-т, 1997. – 334 с. – ISBN 5-88840-012-2.

40. Маркс, К. Капитал. Т. 1. Критика политической экономии. Кн. 1. Процесс производства капитала / К. Маркс ; пер. И. И. Степанова-Скворцова. – Москва : Гос. изд-во полит. лит., 1952. – 797 с.

41. Образцов В. А. О некоторых перспективах интеграции и дифференциации знаний в криминалистике // Актуальные проблемы советской криминалистики. М.: Изд-во Всесоюзного ин-та по изучению причин и разработке мер предупреждения преступности, 1979. – 103 с.

42. Овчинский, В. С. Технологии будущего против криминала / В. С. Овчинский. – Москва : Книжный мир, 2017. – 288 с. – ISBN: 978-5-9500726-4-2.

43. Олиндер, Н. В. Преступления, совершенные с использованием электронных платежных средств и систем: криминалистический аспект : монография / Н. В. Олиндер. – Москва : ООО «Юстиция», 2016. – 122 с. – ISBN 978-5-4365-1489-5.

44. Осипенко, А. Л. Сетевая компьютерная преступность: теория и практика борьбы : монография / А. Л. Осипенко. – Омск : Омская академия МВД России, 2009. – 480 с. – ISBN 978-5-88651-445-2.

45. Познышев, С. В. Криминальная психология. Преступные типы. О психологическом исследовании личности как субъекта поведения вообще и об изучении личности преступника в частности / С. В. Познышев. – Москва : Инфра-М, 2010. – 300 с. – ISBN 978-5-16-002934-4.

46. Россинская, Е. Р. Настольная книга судьи: судебная экспертиза / Е. Р. Россинская, Е. И. Галяшина. – Москва : Проспект, 2010. – 464 с. – ISBN 978-5-392-01270-1.

47. Савельева, М. В. Криминалистика : учебник / М. В. Савельева, А. Б. Смушкин. – Москва : Издат. дом «Дашков и К», 2009. –608 с. – ISBN 978-5-91131-836-9.

48. Сергеев, Л. А. Криминалистика / Л. А. Сергеев. – Москва : Изд-во МГУ, 1971. – 425 с.

49. Скорченко, П. Т. Криминалистика. Технико-криминалистическое обеспечение расследования преступлений : учеб. пособие / П. Т. Скорченко. – Москва : Былина, 1999. – 270 с. – ISBN 5-93384-002-5.

50. Снетков, В. А. Основы деятельности специалиста экспертно-криминалистических подразделений органов внутренних дел : учеб. пособие / В. А. Снетков. – Москва : ГУ ЭКЦ МВД России, 2001. –72 с.

51. Стельмах, В. Ю. Производство следственных действий, направленных на получение и использование компьютерной информации : монография / В. Ю. Стельмах, О. М. Ефремова, В. Ф. Васюков ; под общ. ред. А. Г. Волеводза. – Москва : Проспект, 2021. – 480 с. – ISBN 978-5-392-33469-8.

52. Типовые модели и алгоритмы криминалистического исследования : учеб. пособие / под ред. В. Я. Колдина. – Москва : Изд-во Московского ун-та, 1989. – 184 с. – ISBN 5-211-01217-8.

53. Уголовный процесс : в 3 ч. Ч. 2. Досудебное производство по уголовным делам : учебник / под ред. В. Г. Глебова, Е. А. Зайцевой. – 5-е изд., перераб. и доп. – Волгоград : ВА МВД России, 2017. 260 с. – ISBN 978-5-7899-1061-0; ISBN 978-5-7899-1063-4.

54. Усоскин, В. М. Теории денег / В. М. Усоскин. – Москва : Мысль, 1976. – 228 с.

55. Филатов, А. Профайлинг. Как научиться разбираться в людях и прогнозировать их поведение / А. Филатов. – Москва : Перо, 2016. – 417 с. – ISBN 978-5-906862-66-2.

56. Филиппов, М. Н. Особенности расследования краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов : монография / М. Н. Филиппов. – Москва : Юрлитинформ, 2014. – 157 с. – ISBN 978-5-4396-0540-8.

57. Яблоков, Н. П. Криминалистика : учебник / Н. П. Яблоков. – 2-е изд., перераб. и доп. – Москва : Норма, 2009. – 288 с.

58. Яблоков, Н. П. Криминалистическая характеристика отражаемой преступлением информации / Н. П. Яблоков // Криминалистика : учебник / под ред. А. И. Бастрыкина. – Москва : Экзамен, 2014. – Т. 1. – 511 с.

59. Яковлев, А. Н. Особенности расследования преступлений, совершаемых с использованием электронных платежных средств и систем : науч.-практ. пособие / А. Н. Яковлев, Н. В. Олиндер. – Москва, 2012. – 182 с.

Диссертации и авторефераты диссертаций

60. Атаманов, Р. С. Основы методики расследования мошенничества в сети «Интернет» : автореф. дис. … канд. юрид. наук : 12.00.00 / Атаманов Руслан Сергеевич. – Москва, 2012. – 28 с.

61. Вражнов, А. С. Криминалистический риск при расследовании неправомерного доступа к компьютерной информации : дис. … канд. юрид. наук : 12.00.12 / Вражнов Алексей Сергеевич. – Москва, 2015. – 218 с.

62. Гаврилин, Ю. В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы : автореф. дис. … д-ра юрид. наук : 12.00.09 / Гаврилин Юрий Викторович. – Москва, 2009. – 55 с.

63. Гаспарян, Г. З. Расследование хищений денежных средств, совершенных использованием информационных банковских технологий : автореф. дис. … канд. юрид. наук : 12.00.12 / Гаспарян Гурген Зорикович. – Москва, 2020. – 31 с.

64. Гаспарян, Г. З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : дис. … канд. юрид. наук : 12.00.12 / Гаспарян Гурген Зорикович. – Москва, 2020. – 300 с.

65. Денисова, А. С. Уголовно-правовое значение орудий и средств совершения преступления : автореф. дис. … канд. юрид. наук : 12.00.08 / Денисова Александрина Сергеевна. –Москва, 2005. – 26 с.

66. Дикова, Н. В. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем : автореф. дис. … канд. юрид. наук : 12.00.09 / Дикова Нина Владимировна. – Воронеж, 2011. – 23 с.

67. Ильин, А. Н. Тактика предварительной проверки сообщения о преступлении : автореф. дис. … канд. юрид. наук : 12.00.09 / Ильин Алексей Николаевич. – Москва, 2009. – 24 с.

68. Илюшин, Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет : дис. … канд. юрид. наук : 12.00.09 / Илюшин Денис Анатольевич. – Волгоград, 2008. – 233 с.

69. Имаева, Ю. Б. Особенности расследования хищений, совершенных с использованием кредитных и расчетных карт : дис. … канд. юрид. наук : 12.00.12 / Имаева Юлия Борисовна. – Уфа, 2015. – 233 с.

70. Ким, Д. В. Проблемы теории и практики разрешения криминалистических ситуаций в процессе раскрытия, предварительного расследования и судебного рассмотрения уголовных дел : дис. … д-ра юрид. наук : 12.00.09 / Ким Дмитрий Владимирович. – Барнаул, 2009. – 428 с.

71. Колесниченко, А. Н. Научные и правовые основы расследования отдельных видов преступлений : автореф. дис. … д-ра юрид. наук : 12.00.00 / Колесниченко Алексей Никофорович. – Харьков, 1967. – 28 с.

72. Коломинов, В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа : дис. … канд. юрид. наук : 12.00.12 / Коломинов Вячеслав Валентинович. – Краснодар, 2017. – 211 с.

73. Мазуров, И. Е. Методика расследования хищений, совершенных с использованием интернет-технологий : дис. … канд. юрид. наук : 12.00.12 / Мазуров Игорь Евгеньевич. – Казань, 2017. – 188 с.

74. Мещеряков, В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. … д-ра юрид наук : 12.00.09 / Мещеряков Владимир Алексеевич. – Воронеж, 2001. – 39 с.

75. Семикаленова, А. И. Судебная программно-компьютерная экспертиза по уголовным делам : дис. … канд. юрид. наук : 12.00.09 / Семикаленова Анастасия Игоревна. – Москва, 2005. – 228 с.

76. Сухомлинова, Л. А. Технико-криминалистические и организационные основы выявления и расследования мошенничества в сфере обязательного страхования гражданской ответственности владельцев транспортных средств : дис. …канд. юрид. наук : 12.00.09 / Сухомлинова Людмила Александровна. – Волгоград, 2008. – 197 с.

77. Уткин, М. С. Особенности расследования и предупреждения хищений в потребительской кооперации : автореф. дис. … канд. юрид. наук : 12.00.09 / Уткин Михаил Семенович. – Свердловск, 1975. –21 с.

78. Шевченко, Е. С. Тактика производства отдельных следственных действия при расследовании киберпреступлений : дис. … канд. юрид. наук : 12.00.12 / Шевченко Елизавета Сергеевна. – Москва, 2016. – 249 с.

Статьи в журналах и иных изданиях

79. Алейникова, Ю. В. Цифровая экосистема. Анализ применения искусственного интеллекта / Ю. В. Алейникова, В. В. Матвеев // Здоровье – основа человеческого потенциала: проблемы и пути их решения. – 2020. – Т. 15. – № 3. – С. 1480–1487. – ISSN 2076-4618.

80. Алексеева, А. П. Киберпреступность: основные черты и формы проявления / А. П. Алексеева, О. Н. Ничуговская // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2017. – № 1. – С. 27–34.

81. Алескеров, В. И. Некоторые способы хищения денежных средств, совершаемых в системе дистанционного банковского обслуживания / В. И. Алескеров, В. В. Баранов // Академическая мысль. – 2020. – № 2 (11). – С. 12–16. – eISSN 2588-0020.

82. Аллаханов, С. Ю. Электронные деньги: эпоха к совершенству / С. Ю. Аллаханов // Экономика, статистика и информатика. – 2013. – № 3. – С. 6–10. – ISSN 1994-7844.

83. Анапольская, А. И. Типичные следственные ситуации и версии первоначального этапа расследования мошенничеств с электронными счетами / А. И. Анапольская // Вестник Тамбовского государственного университета. Серия: Гуманитарные науки. – 2015. – Вып. 8 (148). – С. 133–139. – ISSN 1810-0201.

84. Андреева, О. И. О необходимости стадии возбуждения уголовного дела в современном уголовном процессе России / О. И. Андреева // Вестник Томского государственного университета. – 2012. № 356. – С. 109–112. – ISSN 1561-7793.

85. Ахмедшин, Р. Л. «Криминалистическая характеристика личности преступника» и «воздействие»: содержательная взаимосвязь / Р. Л. Ахмедшин // Вестник Томского государственного университета. – 2006. – № 292-1. – С. 64–68. – ISSN 1561-7793.

86. Баринов, С. В. Типовые механизмы преступных нарушений неприкосновенности частной жизни / С. В. Баринов // Вестник Удмуртского университета. Серия: Экономика и право. – 2019. – Т. 29. – Вып. 5. – С. 638–643. – ISSN 2412-9593.

87. Бегма, Ю. С. «Электронные деньги – деньги?». Еще раз к вопросу об интерпретации электронных денег / Ю. С. Бегма // Вестник РГГУ. Серия: Экономика. Управление. Право. – 2013. – № 15 (116). – С. 201–206. – ISSN 2073-6304.

88. Березина, М. П. Деньги в современной интерпретации / М. П. Березина // Бизнес и банки. – 2002. – № 22. – С. 1–8.

89. Бессонов, А. А. О некоторых возможностях современной криминалистики в работе с электронными следами / А. А. Бессонов // Вестник университета имени О. Е. Кутафина. – 2018. – № 3. – С. 46–52. – ISSN 2311-5998.

90. Бессонов, А. А. Способ преступления как элемент его криминалистической характеристики / А. А. Бессонов // Пробелы в российском законодательстве. – 2014. – № 4. – С. 171–173. – ISSN 2072-3164.

91. Бессонов, А. А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности / А. А. Бессонов // Академическая мысль. – 2020. – № 4 (13). – С. 58–61. – eISSN 2588-0020.

92. Бурмистрова, Н. С. Особенности применения криминалистического профайлинга в период сбора релевантной информации в ходе расследования преступления / Н. С. Бурмистрова, Л. В. Бертовский // Пробелы в российском законодательстве. –2018. – № 6. – С. 265–272. – ISSN 2072-3164.

93. Вагабов, Т. М. Тактические особенности проведения проверки показаний на месте в системе мер преодоления лжи со стороны подозреваемого (обвиняемого) / Т. М. Вагабов // Известия Тульского государственного университета. Экономические и юридические науки. – 2014. – № 2-2. – С. 50–56. – ISSN 2071-6184.

94. Ведерников, Н. Т. О проблеме предела изучения личности преступника в криминалистике / Н. Т. Ведерников // Вестник Томского государственного университета. – 2014. – № 385. – С. 135–138. – ISSN 1561-7793.

95. Вехов, В. Б. Электронные следы в системе криминалистики / В. Б. Вехов, С. А. Ковалев, Б. П. Смагоринский // Судебная экспертиза. – 2016. – № 2 (46). – С. 10–19. – ISSN 1813-4327.

96. Гаврилин, Ю. В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации / Ю. В. Гаврилин, В. В. Шипилов // Российский следователь. – 2013. – № 23. – С. 2–6. – ISSN 1812-3783.

97. Гайнельзянова, В. Р. Возможности судебной компьютерно-технической экспертизы при расследовании преступлений в сфере компьютерной информации / В. Р. Гайнельзянова // Вестник Уфимского юридического института МВД России. – 2021. – № 1 (91). – С. 144–149. – ISSN 1729-9187.

98. Гайфутдинов, Р. Р. Типы компьютерных преступников / Р. Р. Гайфутдинов // Вестник экономики, права и социологии. – 2017. – № 2. – С. 54–58. – ISSN 1998-5533.

99. Головин, А. Ю. К вопросу межэлементных связей в криминалистической характеристике преступления / А. Ю. Головин // Деятельность правоохранительных органов в современных условиях : сб. материалов междунар. науч.-практ. конф. (Иркутск, 24–25 мая 2018 г.). – Иркутск : Восточно-Сибирский ин-т МВД России, 2018. С. 31–35. – ISBN 978-5-9538-0070-9.

100. Давыдов, В. О. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий / В. О. Давыдов, И. В. Тишутина // Криминалистика: вчера, сегодня, завтра. – 2020. – № 2 (14). – С. 81–91. – ISSN 2587-9820.

101. Давыдов, В. О. Цифровые следы в расследовании дистанционного мошенничества / В. О. Давыдов, И. В. Тишутина // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 3. – С. 20–27. – ISSN 2071-6184.

102. Дорофеев, К. И. Особенности организации расследования мошенничеств, совершенных дистанционным способом / К. И. Дорофеев // Академическая мысль. – 2019. – № 4 (9). – С. 55–61. – eISSN 2588-0020.

103. Дронова, О. Б. Интернет-ресурсы, используемые в процессе информационного обеспечения раскрытия и расследования мошенничеств, совершенных с использованием средств мобильной связи и сети Интернет / О. Б. Дронова, К. В. Проваторова, А. А. Сапухин // Вестник Волгоградской академии МВД России. – 2021. – № 3 (58). – С. 134–142. – ISSN 2074-8183.

104. Дяблова, Ю. Л. Понятие и структура личности в криминалистике / Ю. Л. Дяблова // Известия Тульского государственного университета. – Серия : Экономические и юридические науки. – 2016. – № 2-2. – С. 99–110. – ISSN 2071-6184.

105. Евдокимов, Д. А. Безопасность мобильного банка: защита от «краж по воздуху» / Д. А. Евдокимов // Банковское дело. – 2014. – № 8. – С. 70-73. – ISSN 2071-4904.

106. Егерева, О. А. Некоторые вопросы методики расследования киберпреступлений / О. А. Егерева, В. В. Коломинов, М. С. Сизова // Сибирские уголовно-процессуальные и криминалистические чтения. – 2018. – № 4 (22). – С. 24–32. – ISSN 2411-6122.

107. Жулева, Е. С. Хищение электронных денег / Е. С. Жулева, В. К. Кулев // Труды международного симпозиума «Надежность и качество». – 2011. – Т. 1. – С. 177–178. – ISSN 2220-6418.

108. Зарубина, Е. Получить ответ непросто / Е. Зарубина, Н. Ивлиева // Полиция России. – 2021. – № 1. – С. 40–43.

109. Зверянская, Л. П. Современные проблемы исследования криминалистических особенностей киберпреступлений / Л. П. Зверянская // Приоритетные научные направления: от теории к практике. – 2015. – № 15. – С. 127–132.

110. Зуйков, Г. Г. Развитие криминалистического учения о способе совершения преступления и проблема способа сокрытия преступления / Г. Г. Зуйков // Повышение эффективности расследования преступлений : сб. науч. тр. – Иркутск : Изд-во ИГУ, 1986.

111. Ибрагимова, Л. Г. Проблемы внедрения электронных денег в денежный оборот Российской Федерации / Л. Г. Ибрагимова // Бизнес в законе. – 2012. – № 5. – С. 89–90.

112. Иванова, Е. В. Типичные механизмы преступлений, связанных с опасными для здоровья веществами / Е. В. Иванова // Научные ведомости Белгородского государственного университета. Серия: Философия. Социология. Право. – 2012. – № 20 (139). – Вып. 22. – С. 201–211. – ISSN 2075-4574.

113. Ищенко, Е. П. О криминалистическом обеспечении раскрытия и расследования киберпреступлений / Е. П. Ищенко // Деятельность правоохранительных органов в современных условиях : сб. материалов 20-й междунар. науч.-практ. конф. : в 2 т. – Иркутск : ВСИ МВД России, 2015. – С. 336–341.

114. Казимагомедова, З. А. Электронные деньги в современном мире / З. А. Казимагомедова, А. З. Атемова // Экономические исследования и разработки. – 2020. – № 4. – С. 36–42. – eISSN 2542-0208.

115. Калентьева, Т. А. Киберпространство как место совершения преступления / Т. А. Калентьева, А. О. Кузьмина // Актуальные проблемы правоведения. – 2019. – № 1 (61). – С. 31–37. – ISSN 2070-1039.

116. Кангезов, М. Р. Проблемы доказывания на стадии возбуждения уголовного дела / М. Р. Кангезов // Пробелы в российском законодательстве. – 2018. – № 4. – С. 323–325. – ISSN 2072-3164.

117. Кардашевская, М. В. Этапы расследования преступлений и их характеристика / М. В. Кардашевская, Е. С. Шипилова // Таврический научный обозреватель. – 2015. – № 2. – С. 8–14. – eISSN 2412-9356.

118. Картавский, П. А. Некоторые приемы тактики проверки показаний на месте / П. А. Картавский // Научный компонент. – 2019. – № 2 (2). – С. 23–32. – eISSN 2686-939X.

119. Ковалев, С. А. Использование криминалистического компьютерного моделирования при планировании расследования преступлений / С. А. Ковалев, Б. П. Смагоринский // Юридическая наука и правоохранительная практика. – 2013. – № 4 (26). – С. 111–123. – ISSN 1998-6963.

120. Ковалев, С. А. Использование метода криминалистического компьютерного моделирования в расследовании преступлений / С. А. Ковалев // Российский следователь. – 2021. – № 4. – С. 35–37. – ISSN 1812-3783.

121. Копыткин, С. А. О соотношении категорий «криминалистическая характеристика преступления» и «механизм преступления» / С. А. Копыткин // Вестник Самарского юридического института. – 2010. – № 2 (2). – С. 77–79. – ISSN 2307-6852.

122. Кочергин, Д. А. Интерпретация электронных денег и оценка их влияния на денежно-кредитную систему / Д. А. Кочергин // Финансы и кредит. – 2005. – № 13 (181). – С. 29–39. – ISSN 2071-4688.

123. Кругова, Е. Ю. Понятие электронных денег: функциональные особенности / Е. Ю. Кругова // Социально-экономические явления и процессы. – 2012. – № 7-8 (041-042). – С. 91–97. – ISSN 1819-8813.

124. Кузьмин, М. Н. Особенности тактики производства допроса потерпевшего в ходе расследования мошенничества в сфере компьютерной информации / М. Н. Кузьмин, Н. В. Солонникова // Гуманитарные, социально-экономические и общественные науки. – 2018. – № 12. – С. 111–113. – ISSN 2220-2404.

125. Кургузкина, Е. Б. Место совершения компьютерных преступлений / Е. Б. Кургузкина, Н. Д. Ратникова // Вестник Воронежского института ФСИН России. – 2016. – № 1. – С. 79–87. – ISSN 2223-3873.

126. Кустов, А. М. Криминалистическая концепция механизма преступления / А. М. Кустов // Вестник Московского финансово-юридического университета. – 2016. – № 2. – С. 164–169. – ISSN 2224-669X.

127. Лавров, В. П. Проблемы предварительной проверки сообщений о преступлениях в современных российских условиях / В. П. Лавров // Труды Академии управления МВД России. – 2017. – № 4 (44). – С. 111–114. – ISSN 2072-9391.

128. Лелетова, М. В. Особенности возбуждения уголовного дела и первоначального этапа расследования хищений электронных денежных средств / М. В. Лелетова, Д. В. Климов // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2014. – № 3 (27). – С. 123–126. – ISSN 2078-5356.

129. Любан, В. Г. Распространенные способы мошенничеств в сфере информационно-телекоммуникационных технологий / В. Г. Любан, А. Ю. Молянов, Е. Н. Хазов // Вестник Московского университета МВД России. – 2019. – № 1. – С. 190–194. – ISSN 2073-0454.

130. Маилян, А. В. Криминалистические аспекты изучения хищений, совершенных с использованием электронных средств платежа / А. В. Маилян // Вестник Уфимского юридического института МВД России. – 2020. – № 3 (89). – С. 110–115. – ISSN 1729-9187.

131. Маилян, А. В. Общие положения криминалистической характеристики хищений, совершенных с банковского счета, в отношении электронных денежных средств и/или с помощью электронных средств платежа / А. В. Маилян // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 3. – С. 120–126. – ISSN 2071-6184.

132. Маилян, А. В. Особенности проведения допроса при расследовании хищений, совершаемых с использованием электронных средств платежа / А. В. Маилян // Криминалистика: вчера, сегодня, завтра. – 2020. – № 3 (15). – С. 78–84. – ISSN 2587-9820.

133. Малыхина, Н. И. Алгоритм действий следователя в типовых ситуациях расследования мошенничеств, совершенных с использованием сети Интернет / Н. И. Малыхина, С. В. Кузьмина // Вестник Томского государственного университета. – 2021. – № 462. – С. 238–247. – ISSN 1561-7793.

134. Мантарджиев, М. В. Отдельные проблемы доказывания в стадии возбуждения уголовного дела / М. В. Мантарджиев // Вопросы российского и международного права. – 2018. – Т. 8. – № 4. – С. 141–149. – ISSN 2222-5129.

135. Марамыгин, М. С. Сущность электронных денег, преимущества и недостатки / М. С. Марамыгин, Е. Н. Прокофьева, А. А. Маркова // Вестник Омского университета. Серия: Экономика. – 2016. – № 1. – С. 60–65. – ISSN 1812-3988.

136. Михайленко, И. А. К вопросу о способах мошенничества в сети Интернет / И. А. Михайленко // Сибирские уголовно-процессуальные и криминалистические чтения. – 2016. – № 5 (13). – С. 98–104. – ISSN 2411-6122.

137. Мусалаева, С. А. Электронные деньги и платежные системы / С. А. Мусалаева // Проблемы современной экономики. – 2010. – № 4 (36). – С. 206–208. – ISSN 1818-3395.

138. Науменко, О. А. Проблемы в расследовании уголовных дел о мошенничестве, совершенном с использованием информационно-телекоммуникационной среды / О. А. Науменко // Вестник Краснодарского университета МВД России. – 2019. – № 3 (45). – С. 60–64. – ISSN 2073-1078.

139. Нестерович, С. А. Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов / С. А. Нестерович // Вестник науки и образования. – 2018. – Т. 2. – № 8 (44). – С. 46–49. – ISSN 2312-8089.

140. Неупокоева, И. А. Осмотр зашифрованных файлов. Тактические особенности и криминалистические рекомендации / И. А. Неупокоева // Закон и право. – 2020. – № 8. – С. 142–144. – ISSN 2073-3313.

141. Овсейко, С. Юридическая природа электронных денег / С. Овсейко // Юрист. – 2007. – № 9. – С. 30–37. – ISSN 1812-3929.

142. Олиндер, Н. В. Криминалистическая характеристика электронных платежных средств и систем / Н. В. Олиндер // Lex Russica. – 2015. – № 10. – Т. CVII. – С, 128–138. – ISSN 1729-5920.

143. Олиндер, Н. В. О назначении экспертиз при расследовании преступлений, совершенных с использованием электронных платежных средств и систем / Н. В. Олиндер // Судебная власть и уголовный процесс. – 2016. – № 1. – С. 82–87. – ISSN 2310-4813.

144. Парасоцкая, Н. Н. Электронные деньги: проблемы и перспективы / Н. Н. Парасоцкая, М. А. Архипова // Бухгалтерский учет в бюджетных и некоммерческих организациях. – 2014. – № 14 (350). – С. 38–42. – ISSN 2079-6714.

145. Переверзева, Е. С. Виртуальные и цифровые следы: новый подход в понимании / Е. С. Переверзева, А. В. Комов // Вестник Санкт-Петербургского университета МВД России. – 2021. – № 1 (89). – С. 172–178. – ISSN 2071-8284.

146. Пинчук, Л. В. К вопросу о понятии осмотра места происшествия / Л. В. Пинчук // Вестник Московского университета МВД России. –2018. – № 5. – 227–231. – ISSN 2073-0454.

147. Поддубный, И. В. К вопросу об использовании злоумышленниками программ удаленного доступа и вредоносного ПО как средств совершения хищений с банковских карт граждан / И. В. Поддубный // Криминалистика: вчера, сегодня, завтра. – 2020. – № 3 (15). – С. 99–105. – ISSN 2587-9820.

148. Поляков, В. В. Особенности личности компьютерных преступников / В. В. Поляков, Л. А. Попов // Известия Алтайского государственного университета. – 2018. – № 6 (104). – С. 256–259. – ISSN 1561-9443.

149. Протасевич, А. А. Криминалистическая характеристика компьютерных преступлений / А. А. Протасевич, Л. П. Зверянская // Российский следователь. – 2013. – № 11. – С. 45–47. – ISSN 1812-3783.

150. Расторопова, Д. С. К вопросу об определении родового и видового объекта преступления, предусмотренного ст. 185.6 УК РФ / Д. С. Расторопова // Пробелы в российском законодательстве. – 2018. – № 6. – С. 216–219. – ISSN 2071-3164.

151. Ревякин, С. В. Проблемы раскрытия хищений, совершаемых посредством современных электронных средств коммуникации / С. В. Ревякин // Правопорядок: история, теория, практика. – 2018. – № 3 (18). – С 27–32. – ISSN 2311-696X.

152. Россинская, Е. Р. Концепция вредоносных программ как способов совершений компьютерных преступлений: классификации и технологии противоправного использования / Е. Р. Россинская, И. А. Рядовский // Всероссийский криминологический журнал. – 2020. – Т. 14. – № 5. – С. 699–709. – ISSN 2500-4255.

153. Россинская Е. Р. Концепция цифровых следов в криминалистике / Е. Р. Россинская, И. А. Рядовский // Аубакировские чтения : материалы междунар. науч.-практ. конф. (19 февраля 2019 г.). – Алматы : Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2019. – С. 6–8. – ISBN 978-601-7599-44-9.

154. Россинская, Е. Р. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров / Е. Р. Россинская, Т. А. Сааков // Криминалистика: вчера, сегодня, завтра. – 2020. – № 3 (15). – С. 106–123. – ISSN 2587-9820.

155. Россинская, Е. Р. Современные способы компьютерных преступлений и закономерности их реализации / Е. Р. Россинская, И. А. Рядовский // Lex Russica. – 2019. – № 3 (148). – С. 87–99. – ISSN 1729-5920.

156. Самойлов, А. В. Понятие способа совершения преступления и его роль в системе механизма совершения преступления / А. В. Самойлов // Журнал научных публикаций аспирантов и докторантов. – 2010. – № 10 (52). – С. 49–50. – ISSN 1991-3087.

157. Самойлов, П. А. К вопросу об основаниях для направления по территориальности материалов доследственных проверок на примере мошенничеств с использованием средств сотовой связи и Интернета / П. А. Самойлов // Вектор науки ТГУ. Серия: Юридические науки. – 2017. – № 3 (30). – С. 47–51. – ISSN 2220-7457.

158. Семикаленова, А. И. Особенности определения объекта судебной программно-компьютерной экспертизы / А. И. Семикаленова // Вестник университета имени О. Е. Кутафина. – 2015. – № 12. – С. 72–74. – ISSN 2311-5998.

159. Семикаленова, А. И. Проблема определения объекта и задач судебной программно-компьютерной экспертизы / А. И. Семикаленова // Теория и практика судебной экспертизы в современных ус-

ловиях : сб. тр. конф. (Москва, 22–23 января 2015 г.). – Москва : Проспект, 2015. – С. 438–442.

160. Сергеев, А. Б. Стадия возбуждения уголовного дела – «атавизм» уголовного процесса? / А. Б. Сергеев, Э. А. Хохрякова // Вестник Челябинского государственного университета. – 2015. – № 17 (372). – Вып. 43. – С. 163–170. – ISSN 2618-8236.

161. Сидорова, К. С. Способы установления IP-адреса и сведений о нем при расследовании уголовных дел / К. С. Сидорова // Вестник Сибирского института бизнеса и информационных технологий. – 2018. – № 2 (26). – С. 88–92. – ISSN 2225-8264.

162. Смагоринский, Б. П. Новые способы совершения мошенничеств, связанных с распространением коронавирусной инфекции / Б. П. Смагоринский, А. В. Сычева // Вестник Волгоградской академии МВД России. – 2020. – № 2 (53). – С. 111–117. – ISSN 2074-8183.

163. Солуянов, А. А. Использование электронных денег в международных расчетах и контроль со стороны государства / А. А. Солуянов // Мир новой экономики. – 2017. – № 1. – С. 60–63. – ISSN 2220-6469.

164. Степанова, М. А. Проблемы определения места совершения хищения денежных средств с использованием информационно-телекоммуникационных технологий / М. А. Степанова, Е. В. Царев // Вестник Белгородского юридического института МВД России. – 2021. – № 1. – С. 12–16. –ISSN 2313-5646.

165. Суходолов, А. П. Математические методы и цифровые технологии в современной криминологии / А. П. Суходолов, А. М. Бычкова // Всероссийский криминологический журнал. – 2018. – Т. 12. – № 6. – С. 753–766. – ISSN 2500-4255.

166. Сыпачев, А. Ю. Основные способы хищений с использованием сети Интернет / А. Ю. Сыпачев // Научно-методический электронный журнал Концепт. – 2015. – № 10. – С. 71–75. – eISSN 2304-120X.

167. Сысенко, А. Р. Особенности осмотра места происшествия при расследовании компьютерных преступлений / А. Р. Сысенко // Закон и право. – 2020. – № 12. – С. 216–218. – ISSN 2073-3313.

168. Сысенко, А. Р. Проблемы назначения и производства судебной компьютерно-технической экспертизы / А. Р. Сысенко, И. С. Смирнова, С. Е. Тимошенко // Сибирское юридическое обозрение. – 2020. – Т. 17. – № 4. – С. 523–532. – ISSN 2658-7602.

169. Тепляков, С. П. Социальная инженерия. Анализ и методы защиты / С. П. Тепляков, А. С. Тимохович // Academy. – 2018. – № 7 (34). – С. 26–27. – ISSN 2412-8236.

170. Ткач, В. Ю. Место происшествия – объект осмотра и криминалистического исследования / В. Ю. Ткач // Известия Тульского государственного университета. Экономические и юридические науки. – 2012. – № 1-2. – С. 296–304. – ISSN 2071-6184.

171. Третьякова, Е. И. Правовые проблемы расследования мошенничества с использованием электронных средств платежа / Е. И. Третьякова, О. В. Трубкина // Криминалистика: вчера, сегодня, завтра. – 2020 – № 2 (14). – С. 195–200. – ISSN 2587-9820.

172. Харина, Э. Н. Киберпреступления: уголовно-правовой и криминалистический аспект / Э. Н. Харина // Вестник университета имени О. Е. Кутафина. – 2017. – № 5. – С. 164–171. – ISSN 2311-5998.

173. Холевчук, А. Г. Использование тактики когнитивного интервью в целях получения достоверной информации о запланированных действиях допрашиваемого: современные зарубежные подходы / А. Г. Холевчук // Международный научный журнал «Инновационная наука». – 2015. – № 11. – С. 191–195. – ISSN 2410-6070.

174. Хомякова, Л. И. Обеспечение экономической безопасности в сфере оборота электронных денег в странах ЕАЭС в 2019–2021 годах / Л. И. Хомякова // Экономика. Налоги. Право. – 2019. – № 1. – С. 37–46. – ISSN 1999-849X.

175. Чекунов, И. Г. Понятие и отличительные особенности киберпреступности / И. Г. Чекунов // Российский следователь. – 2014. – № 18. – С. 53–56. – ISSN 1812-3783.

176. Чернышева, Е. В. Эффективность психологических тактик взаимодействия с допрашиваемым лицом при расследовании преступлений / Е. В. Чернышева // Прикладная юридическая психология. – 2018. – № 4 (45). – С. 71–81. – ISSN 2072-8336.

177. Шавалеев, Б. Э. Особенности мошенничества с использованием электронных средств платежа в структуре современной Российской преступности / Б. Э. Шавалеев // Ученые записки Казанского юридического института МВД России. – 2020. – Т. 5. – № 1 (9). – С. 36–39. – eISSN 2541-8262.

178. Шаталов, А. С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции / А. С. Шаталов // Вестник Сибирского юридического института МВД России. – 2018. – № 3 (32). – С. 7–15. – ISSN 2542-1735.

179. Шишова, Н. Е. Моделирование механизма преступлений, связанных с жестоким обращением с детьми / Н. Е. Шишова // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2016. – № 1. – С. 119–124. – eISSN 2224-0209.

180. Шурухнов, Н. Г. Тактические и технологические основы проведения следственных действий при разрешении следственных ситуаций последующего этапа расследования фальшивомонетничества / Н. Г. Шурухнов // Вестник Восточно-Сибирского института МВД России. – 2013. – № 2 (65). – С. 16–24. – ISSN 2312-3184.

181. Яковлев, М. М. К вопросу о понятии и значении стадии возбуждения уголовного дела в уголовном процессе России / М. М. Яковлев, И. К. Федоров // Проблемы науки. – 2018. – № 11 (35). – С. 22–25. – ISSN 2413-2101.

182. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK / D. Buil-Gil, F. Miró-Llinares. A. Moneva, S. Kemp, N Díaz-Castaño // European Societies. – 2020. – P. 1–13.

183. Understanding Internet Fraud: Denial of Risk Theory Perspective / M. Offei, F. K. Andoh-Baidoo, E. Ayaburi, D. Asamoah // ICT Unbounded, Social Impact of Bright ICT Adoption, IFIP WG 8.6 International Conference on Transfer and Diffusion of IT, TDIT 2019. – Accra, Ghana, June 21–22, 2019. – P. 415–424.

Электронные ресурсы

184. Абрамовский, А. Электронные деньги – валюта будущего? / А. Абрамовский. – URL: readli.net. (дата обращения: 23.02.2021). – Текст : электронный.

185. Алиев, А. Т. Деньги. Кредит. Банки : учеб. пособие / А. Т. Алиев. – URL: https://thelib.ru/books/adik_tagirovich_aliev/dengi_kredit_banki_uchebnoe-posobie-read-2.html (дата обращения: 19.05.2021). – Текст : электронный.

186. Антонян, Ю. М. Психология преступника и расследование преступлений / Ю. М. Антонян, М. И. Еникеев, В. Е. Эминов. – URL: http://yurpsy.com/files/ucheb/anton/04.htm (дата обращения: 23.06.2020). – Текст : электронный.

187. Банкиры и операторы начинают обмен мошенниками. В России запускается несколько новых антифрод-платформ. – URL: https://www.rbc.ru/newspaper/2020/12/09/5fce307f9a7947fa67b4bcfc (дата обращения: 10.08.2021). – Текст : электронный.

188. Бессонов, А. А. Учение о криминалистической характеристике преступлений / А. А. Бессонов. – URL: https://izron.ru/articles/problemy-i-perspektivy-razvitiya-sovremennoy-yurisprudentsii-sbornik-nauchnykh-trudov-po-itogam-mezh/sektsiya-7-ugolovnyy-protsess-kriminalistika-operativno-rozysknaya-deyatelnost-spetsialnost-12-00-09/uchenie-o-kriminalisticheskoypkharakteristike-prestupleniy/ (дата обращения: 14.07.2021). – Текст : электронный.

189. Бозов, А. А. Методические рекомендации: использование возможностей сотовой связи при раскрытии и расследовании преступлений / А. А. Бозов. – URL: https://alexboz.pravorub.ru/personal/30734.html (дата обращения: 09.09. 2021). – Текст : электронный.

190. Большие данные против большого мошенничества. – URL: https://www.kaspersky.ru/blog/bolshie-dannye-protiv-bolshogo-moshennichestva/14902/ (дата обращения: 10.08.2021). – Текст : электронный.

191. В Коми осужден программист, похитивший деньг с расчетного счета предпринимателя. – URL: https://komiinform.ru/news/64150 (дата обращения: 17.04.2021). – Текст : электронный.

192. В профайлинге и верификации лжи существует довольно много стандартов проведения интервью. – URL: https://proprofiling.com/faint_inerview (дата обращения: 22.09.2021). – Текст : электронный.

193. Васильева, Н. Ю. Использование методов профайлинга и верификации в ходе предварительного расследования / Н. Ю. Васильева, А. В. Мадянов, С. Н. Болховитина. URL: https://www.b17.ru/article/98851/ (дата обращения: 22.09.2021). – Текст : электронный.

194. Виртуальные деньги: что это такое, плюсы и минусы электронной валюты. – URL: https://elgreloo.com/business-and-finances/internet-money (дата обращения: 16.03.2021). – Текст : электронный.

195. Возбуждение уголовного дела. – URL: https://yandex.ru/turbo/be5.biz/s/pravo/u034/10.html (дата обращения: 10.08.2021). – Текст : электронный.

196. Где проводить расследование при хищении с банковского счета. – URL: https://ugpr-ru.turbopages.org/ugpr.ru/s/article/1589-qqe-17-m2-22-02-2017-podsledstvennost-pri-hishchenii-deneg-s-bankovskogo-scheta (дата обращения: 10.08.2021). – Текст : электронный.

197. Генезис-архивы: ecash Дэвида Чаума и рождение мечты шифропанков. – URL: forklog.com (дата обращения: 18.03.2021). – Текст : электронный.

198. Информационная безопасность: лекции (контент по дисциплине). – URL: eos.ibi.spb.ru (дата обращения: 18.03.2021). – Текст : электронный.

199. Вехов, В. Б. Особенности проведения доследственной проверки по делам о преступлениях в сфере компьютерной информации / В. Б. Вехов. – URL: https://wiselawyer-ru/turbopages.org...-477969-709906072657 (дата обращения: 10.08.2021). – Текст : электронный.

200. Евсеева, Е. ЦБ: объем мошеннических операций в 2020 году в России вырос на 32 % – до 2,5 млрд рублей / Е. Евсеева. – URL: https://vc.ru/finance/192576-cb-obem-moshennicheskih-operaciy-v-2020-godu-v-rossii-vyros-na-32-do-2-5-mlrd-rubley (дата обращения: 07.04.2021). – Текст : электронный.

201. Жур, Я. Встревают в беседу и поглощают сотни тысяч рублей: вид мошенничества из 80-х принял новую форму. «Человек посередине» вернулся / Я. Жур. – URL: https://sb-by.turbopages.org/turbo/sb.by/s/articles/chelovek-poseredine-vernulsya.html (дата обращения: 17.04.2021). – Текст : электронный.

202. Забейда, А. Исключить ст. 159.6 УК. Вопросы цифрового хищения в новом постановлении Пленума ВС о судебной практике по делам о мошенничестве / А. Забейда, Д. Данилов. – URL: https://www.advgazeta.ru/mneniya/isklyuchit-st-159-6-uk/ (дата обращения: 21.07.2021). – Текст : электронный.

203. Закурдаев, М. Количество «удаленщиков» за пандемию выросло в 100 раз в России / М. Закурдаев. – URL: https://osnmedia-ru.turbopages.org/turbo/osnmedia.ru/s/ekonomika/kolichestvo-udalenshhikov-za-pandemiyu-vyroslo-v-100-ras-v-rossii/ (дата обращения: 07.04.2021). – Текст : электронный.

204. «Игра в прятки»: немного о технологиях анонимности в Интернете. – URL: https://habr.com/ru/company/cloud_mts/blog/312032 (дата обращения: 27.07.2021). – Текст : электронный.

205. Интересные факты об электронных деньгах. Чем так любопытна цифровая валюта. – URL: https://yandex.ru/turbo/finansy.-name/s/upravlenie/fakty-ob-jelektronnyh-dengah.html (дата обращения: 19.05.2021). – Текст : электронный.

206. Интернет-торговля в России 2020. – URL: https://datainsight.ru/DI-eCommerce2020 (дата обращения: 20.06.2021). – Текст : электронный.

207. История возникновения пластиковых карт. – URL: https://abium24.ru/istoriya-vozniknoveniya-plastikovykh-kart (дата обращения: 18.03.2021). – Текст : электронный.

208. Как пандемия изменила рынок фриланса: исследование FL.ru и Нетологии. – URL: https://netology.ru/blog/04-2021-pandemiya-i-frilans (дата обращения: 07.04.2021). – Текст : электронный.

209. Как узнать IP-адрес чужого компьютера и есть ли в этом смысл. – URL: https://compconfig.ru/net/kak-uznat-ip-adres-chuzhogo-kompyutera.html (дата обращения: 12.08.2021). – Текст : электронный.

210. Как это работает: координаты базовых станций. – URL: https://xinit.ru/ (дата обращения: 09.09.2021). – Текст : электронный.

211. Какие виды лог-файлов бывают. – URL: https://ru.hostings.info/termins/log-fayly.html (дата обращения: 27.07.2021). – Текст : электронный.

212. Колдин, В. Я. Типовая информационная модель или криминалистическая характеристика преступления? / В. Я. Колдин, Е. П. Ищенко, О. А. Крестовников. – URL: http://koldin-msu.ru/science/modeling (дата обращения: 28.07.2021). – Текст : электронный.

213. Кошельки уходят в Интернет. Bain подготовила доклад о настоящем и будущем рынка платежей. – URL: https://yandex.ru/turbo/kommersant.ru/s/doc/4096264 (дата обращения: 25.03.2021). – Текст : электронный.

214. Кокош Г. Электронные деньги / Г. Кокош. – URL: https://bankspravka.ru/bankovskiy-slovar/elektronnyie-dengi.html (дата обращения: 09.04.2021). – Текст : электронный.

215. Краткая история электронных платежных технологий. – URL: smart-lab.ru (дата обращения: 16.03.2021). – Текст : электронный.

216. Криптография для хакеров. Основы алгоритмов шифрования. – URL: https://hacker-basement.ru/2019/08/23/kryptografia-dlya-hakerov-algorytmy-shifrovaniy/ (дата обращения: 27.07.2021). – Текст : электронный.

217. Либерман, К. Что такое «электронные деньги»? / К. Либерман // Российский бухгалтер. 2011. № 12. – URL: http://docs.cntd.ru/document/902318750 (дата обращения: 31.03.2021). – Текст : электронный.

218. МВД добавит в приложение «МВД России» модуль «Антимошенник», который будет иметь доступ к контактам пользователей. – URL: https://m.habr.com/ru/news/t/541092/ (дата обращения: 10.05.2021). – Текст : электронный.

219. Механизм преступной деятельности. – URL: https://be5-biz/turbopages.org/be5.biz/s/pravo/k044/...-prod-8080-BAL-1804&trb-src=wb (дата обращения: 28.07.2021). – Текст : электронный.

220. Могут ли правоохранительные органы действительно отследить кого-то по IP-адресу. – URL: https://guidepc-ru/turbopages.org/turbo/guidepc.ru/s/articles/mogut-li-pravoohranitelnye-organy-dejstvitelno-otsledit-kogo-to-po-ip-adresu/ (дата обращения: 09.09.2021). – Текст : электронный.

221. Моделирование механизма совершения преступления. – URL: https://scicenter/online/kniga-kriminalistika-scicenter/modelirovanie-mehanizma-sovershenіya.html (дата обращения: 28.07.2021). – Текст : электронный.

222. Мы твердо убеждены, что национальная безопасность может быть обеспечена без нарушения конфиденциальности. – URL: https://www.apple.com/ru/privacy/government-information-requests/ (дата обращения: 09.09.2021). – Текст : электронный.

223. Немцева, М. «Их слишком много»: почему киберпреступления остаются нераскрытыми / М. Немцева. – URL: https://iz-ru.turbopages.org/iz.ru/s/1166840/mariia-nemtceva/ikh-slishkom-mnogo-pochemu-kiberprestupleniia-ostaiutsia-neraskrytymi (дата обращения: 11.08.2021). – Текст : электронный.

224. О доказательственном значении лог-файлов. – URL: https://www.securitylab.ru/analytics/216291.php (дата обращения: 24.09.2021). – Текст : электронный.

225. Отслеживание людей по MAC-адресу их гаджетов. – URL: https://camslider.ru/otslezhivanie-ljudej-po-mac-adresu-ih-gadzhetov/ (дата обращения: 09.09.2021). – Текст : электронный.

226. Пандемия и цифровое невежество: эксперты назвали причины роста киберпреступности в России. – URL: https://online47-ru.turbo-pages.org/ (дата обращения: 20.06.2021). – Текст : электронный.

227. Почему так сложно преследовать киберпреступников? – URL: https://www.securitylab.ru/blog/personal/bezmaly/344477.php (дата обращения: 14.09.2021). – Текст : электронный.

228. Почти половина россиян предпочитает электронные деньги. – URL: https://rg-ru.turbopages.org/rg.ru/s/2020/07/15/pochti-polovina-rossian-predpochitaet-elektronnye-dengi.html (дата обращения: 23.09.2021). – Текст : электронный.

229. Природа электронных денег. – URL: https://vuzlit.ru/1241419/priroda_elektronnyh_deneg (дата обращения: 09.04.2021). – Текст : электронный.

230. Про электронные деньги: история появления. – URL: http://niceforex.ru/2016/03/pro-electronnye-dengi-istoriya-poyavleniya/ (дата обращения: 18.03.2021). – Текст : электронный.

231. Ревенков, П. В. Электронные деньги: международный опыт регулирования в области ПОД/ФТ / П. В. Ревенков. – URL: http://lexandbusiness.ru/view-article.php?id=3910 (дата обращения: 09.04.2021). – Текст : электронный.

232. Рештей, Д. История появления электронных денежных средств / Д. Рештей. – URL: http://richinvest.biz/eps/istoriya-poyavleniya--electronnyx-denezhnyx-sredstv (дата обращения: 18.03.2021). – Текст : электронный.

233. Самойлов, А. В. Понятие механизма совершения преступления как научной категории криминалистики / А. В. Самойлов. – URL: http://www.rusnauka.com/16_PN_2016/Pravo/11_211242.doc.htm (дата обращения 28.07.2021). – Текст : электронный.

234. Самойлов, А. В. Понятие способа совершение преступления и его роль в механизме совершения преступления / А. В. Самойлов. – URL: jurnal.org/articles/2010/uri64.html (дата обращения: 28.07.2021). – Текст : электронный.

235. Сапожникова, М. Свобода по выбору: настоящее и будущее фриланса в России / М. Сапожникова. – URL: https://trends-rbc-ru.turbo-pages.org/turbo/trends.rbc.ru/s/trends/social/60c8e3139a79472ba64fde35 (дата обращения: 07.04.2021). – Текст : электронный.

236. Сергей Лебедев: в виртуальном мире не выстроены барьеры для преступников. – URL: https://ria.ru/20210820/kibermoshennichestvo-1746425415.html (дата обращения: 01.09.2021). – Текст : электронный.

237. Тактика допроса и очной ставки. – URL: https://be5-biz.turbopages.org/turbo/be5.biz/s/pravo/k009/24.html#3-2 (дата обращения: 11.09.2021). – Текст : электронный.

238. Титова, О. К. Значение электронных денег на современном этапе развития / О. К. Титова. – URL: rep.polessu.by›bitstream/-123456789/2760/1/171.pdf (дата обращения: 09.04.2021). – Текст : электронный.

239. Трегубова, Е. И хочется, и колется. Насколько безопасны электронные кошельки? / Е. И. Трегубова. – URL: https://aif.ru/-money/mymoney/42997 (дата обращения: 14.07.2021). – Текст : электронный.

240. Финансовая империя Alibaba Group: от одного платежного сервиса до гиганта китайского рынка. – URL: https://vc.ru/story/24990-ant-financial-story (дата обращения: 22.03.2021). – Текст : электронный.

241. Царев, Е. О. Судебная компьютерно-техническая экспертиза, виды, вопросы / Е. О. Царев. – URL: rtmtech.ru (дата обращения: 01.03.2021). – Текст : электронный.

242. ЦБ: Доля безналичных платежей вырастет до 75 % за 3–5 лет. – URL: https://finance-rambler-ru.turbopages.org/turbo/finance.rambler.ru/s/-money/46030635-tsb-dolya-beznalichnyh-platezhey-vyrastet-do-75-za-3-5-let/ (дата обращения: 23.09.2021). – Текст : электронный.

243. Эксперты назвали самый популярный способ мошенничества в Интернете. – URL: https://www.rbc.ru/technology_and_media/09/02/-2021/602184e19a794726a2165b6b (дата обращения: 09.09.2021). – Текст : электронный.

244. Электронная почта. Ремейлер. – URL: https://google--info-org.turbopages.org...-balancer-8080-BAL-7957&trb (дата обращения: 26.07.2021). – Текст : электронный.

245. Электронные деньги. – URL: https://www.tadviser.ru/index.php (дата обращения: 18.03.2021). – Текст : электронный.

246. Электронные деньги. – URL: http://www.incore.me/informacionnyye-texnologii/elektronnye-dengi/ (дата обращения: 03.04.2021). – Текст : электронный.

247. Электронные деньги вчера, сегодня, завтра – их плюсы и минусы. – URL: https://business-poisk.com/elektronnye-dengi.html#-chto-takoe-elektronnye-dengi (дата обращения: 23.02.2021). – Текст : электронный.

248. Этапы процесса расследования преступлений. – URL: https://crimlib.info/%D0%AD...%D0%BD%D0%B8%D0%B9 (дата обращения: 17.08.2021). – Текст : электронный.

249. «Этот год стал серьезным тестом для всех отраслей, и интернет-отрасль этот тест прошла»: эксперты подвели итоги года Рунета. – URL: https://raec.ru/live/branch/12132 (дата обращения: 20.06.2021). – Текст : электронный.

250. China Mobile привлек к борьбе с мошенничеством ИИ-технологии и Big Data. – URL: https://nag.ru/news/newsline/102103/-china-mobile-privlek-k-borbe-s-moshennichestvom-ii-tehnologii-i-big-data (дата обращения: 09.05.2021). – Текст : электронный.

251. Ecash. – URL: https://www.tadviser.ru/index.php/%D0%-9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:ECash (дата обращения: 18.03.2021). – Текст : электронный.

252. Frequently Asked Questions: the new European Cybercrime Centre. – URL: https://ec.europa.eu/commission/presscorner/detail/en/-MEMO_12_221 (дата обращения: 05.10.2020). – Текст : электронный.

253. IBM получила патент на новую технологию борьбы с интернет-мошенничеством. – URL: https://m/habr.com/ru/company/ibm/-blog/225933 (дата обращения: 10.05.2021). – Текст : электронный.

254. Praxxis: как устроен анонимный цифровой «кэш» от Дэвида Чаума. – URL: decenter.org (дата обращения: 22.03.2021). – Текст : электронный.

Научное издание

Голятина Светлана Михайловна

КРИМИНАЛИСТИЧЕСКАЯ ТЕОРИЯ
И ПРАКТИКА РАССЛЕДОВАНИЯ ХИЩЕНИЙ
ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

Монография

Под научной редакцией А. П. Алексеевой

При дизайне обложки использовались материалы сайта:
https://vesti-nesvetay.ru, https://images.izi.ua, https://sun9-43.userapi.com

Редактор *М. В. Остертак*
Компьютерная верстка *Н. А. Доненко*
Дизайн обложки *А. Н. Улизко*

Волгоградская академия МВД России.
400075, Волгоград, ул. Историческая, 130.

Редакционно-издательский отдел.
400005, Волгоград, ул. Коммунистическая, 36.

Подписано в печать 02.12.2021. Формат 60Х84/16. Бумага офсетная.
Гарнитура Times New Roman. Физ. печ. л. 11,5. Усл. печ. л. 10,7.
Тираж 50 экз. Заказ 53.

ОПиОП РИО ВА МВД России. 400005, Волгоград, ул. Коммунистическая, 36.