19. Ларьков, А. Н. Совершенствование практики борьбы с хищениями, должностными преступлениями в новых условиях хозяйствования : метод. пособие / А. Н. Ларьков, Т. Д. Кривенко, Э. Д. Куранова ; ВНИИ проблем укрепления законности и правопорядка. – М., 1990. – 35 с.

20. Методика расследования коррупционных преступлений : науч.-практ. пособие / С. В. Войцеховская [и др.] ; под общ. ред. В. Х. Кадырова. – Минск, 2006. – 306 с.

21. Программа по криминалистике для юридических институтов / сост.: Е. У. Зицер, С. А. Голунский. – М. : Тип. высш. шк. пропагандистов им. Я. М. Свердлова при ЦК ВКП(б), 1937. – 28 с.

22. Программа по криминалистике (часть вторая) для юридических институтов и работников прокуратуры / под ред. А. Я. Вышинского. – М. : Юрид. изд-во НКЮ СССР, 1938. – 20 с.

23. Советская криминалистика. Методика расследования отдельных видов преступлений : учебник / В. П. Бахин [и др.] ; под ред. В. К. Лисиченко. – Київ : Вищ. шк., 1988. – 405 с.

24. Хилобок, М. П. Расследование должностных преступлений / М. П. Хилобок. – М., 1966. – 18 с.

25. Хлус, А. М. Криминалистический анализ структурных элементов злоупотребления властью или служебными полномочиями / А. М. Хлус, П. А. Кадуков // Концептуальные основы современной криминалистики: теория и практика : материалы Междунар. науч.-практ. конф., Минск, 25 окт. 2019 г. / учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь» ; редкол.: В. Б. Шабанов (отв. ред.) [и др.]. – Минск, 2019. – С. 132–139.

26. Хлус, А. М. Некоторые аспекты уголовно-правовой и криминалистической характеристики злоупотребления властью или служебными полномочиями / А. М. Хлус // Проблемы укрепления законности и правопорядка: наука, практика, тенденции : сб. науч. тр. / Науч.-практ. центр проблем укрепления законности и правопорядка Генер. прокуратуры Респ. Беларусь. – Вып. 11. – Минск, 2018. – С. 247–254.

27. Хлус, А. М. Теоретико-прикладные аспекты противодействия злоупотреблению властью или служебными полномочиями / А. М. Хлус // I Минские криминалистические чтения : материалы Междунар. науч.-практ. конф. (Минск, 20 дек. 2018 г.) : в 2 ч. / учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Минск, 2018. – Ч. 1. – С. 338–343.

28. Трегубов, С. Н. Основы уголовной техники: научно-технические приемы расследования преступлений / С. Н. Трегубов. – М. : ЛексЭст, 2002. – 336 с.

29. Шавер, Б. М. Криминалистика / Б. М. Шавер, А. И. Винберг. – М. : Юрид. изд-во НКЮ СССР, 1940. – 200 с.

30. Шавер, Б. М. Криминалистика / Б. М. Шавер, А. И. Винберг. – М. : Юрид. изд-во НКЮ СССР, 1945. – 205 с.

31. Шавер, Б. М. Криминалистика / Б. М. Шавер, А. И. Винберг. – М. : Гос. изд-во юрид. лит., 1949. – 272 с.

32. Шавер, Б. М. Руководство по расследованию преступлений : пособие / Б. М. Шавер, П. И. Тарасов-Родионов. – М. : Юрид. изд-во, 1941. – 190 с.

33. Шмонин, А. В. Актуальные проблемы криминалистической методики : учеб. пособие / А. В. Шмонин. – М. : Акад. упр. МВД России, 2010. – 208 с.

34. Шмонин, А. В. Формирование криминалистических знаний о расследовании коррупционных преступлений в сфере экономики / А. В. Шмонин, М. Г. Муссов // Тр. Акад. упр. МВД России. – 2012. – № 1. – С. 25–29.

Дата поступления в редакцию: 08.02.2022

УДК 343.985.7

***Л. Л. Мельник**, адъюнкт научно-педагогического факультета*
Академии Министерства внутренних дел Республики Беларусь
e-mail: l_melnik@sk.gov.by

О НЕКОТОРЫХ АСПЕКТАХ РАБОЧЕГО ЭТАПА ОБЫСКА ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ТОКЕНОВ И ЭЛЕКТРОННЫХ ДЕНЕГ

На основе обобщения практики расследования преступлений, совершенных с использованием токенов и электронных денег, приведены уголовно-процессуальные и криминалистические аспекты проведения обыска. Представлены новые подходы к реализации рабочего этапа его проведения, рассмотрена деятельность следователя по поиску, фиксации, копированию компьютерной информации, наложению ареста на электронные деньги и токены.

Ключевые слова: расследование преступлений, обыск, информационные технологии, токены, электронные деньги, компьютерная информация, арест, осмотр компьютерной информации.

***L. L. Melnik**, postgraduate student of the Scientific and Pedagogical Faculty*
of the Academy of the Ministry of Internal Affairs of the Republic of Belarus
e-mail: l_melnik@sk.gov.by

ON SOME ASPECTS OF THE WORKING STAGE OF THE SEARCH IN THE INVESTIGATION OF CRIMES COMMITTED WITH THE USE OF TOKENS AND ELECTRONIC MONEY

Based on the generalization of the practice of investigating crimes committed with the use of cryptocurrencies and electronic money, the article considers the criminal procedural and forensic aspects of conducting a search in this category of criminal cases. In the article, new approaches to the implementation of the working stage of the search, the activity of the investigator in the search, fixation, copying of computer information, seizure of electronic money and cryptocurrencies is considered.

Keywords: crime investigation, search, information technology, cryptocurrencies, electronic money, computer information, arrest, examination of computer information.

Существующие процессы информатизации в Республике Беларусь все больше затрагивают национальные экономические интересы [11], а также влияют на криминогенную обстановку, что сказывается на появлении новых способов совершения противоправных деяний [15]. По оценке экспертов, если не предпринять дополнительных мер, количество преступлений против компьютерной безопасности к 2025 г. может достигнуть 100 000 [2], что сопоставимо с общим количеством уголовных правонарушений, регистрируемых в последние годы. Относительно новыми общественными отношениями, подвергаемыми частым противоправным посягательствам, являются права владения, пользования и распоряжения токенами и электронными деньгами. Учитывая электронно-цифровую природу происхождения указанного имущества, высокую степень анонимности его пользователей, представители органов уголовного преследования часто испытывают сложности в раскрытии и расследовании таких преступлений. Одним из направлений по противодействию данной негативной тенденции является внедрение действенных рекомендаций по проведению отдельных следственных действий. Наиболее важным из них при расследовании уголовных дел этой категории является обыск.

Уголовно-процессуальным и криминалистическим проблемам проведения обыска при расследовании преступлений против компьютерной безопасности посвящено множество научных работ. Среди ученых, изучающих данный вопрос, можно выделить Л. Б. Краснову [7], В. А. Мещерякова [10], А. Н. Иванова [4], Д. А. Илюшина [5], М. В. Старичкова [16], Е. Г. Ларина [8], В. М. Логвина и Н. Н. Беломытцева [10]. Вместе с тем в научной литературе не представлены уголовно-процессуальные и криминалистические аспекты проведения рабочего этапа обыска при расследовании преступлений, совершенных с использованием токенов и электронных денег, что требует их дополнительного рассмотрения.

По мнению Р. С. Белкина, производство обыска состоит из четырех этапов: подготовительного, обзорного, детального и заключительного [1]. При этом другие ученые обзорный и детальный этапы обыска объединяют в рабочий, состоящий из обзорной и детальной (поисковой) стадии [3, 14].

Согласно традиционным рекомендациям на обзорной стадии рассматриваемого следственного действия первоначально производится обход помещений, ознакомление с обстановкой, принимается решение о порядке применения технических средств, последовательности поисковых действий. В целях совершенствования расследования преступлений с использованием токенов и электронных денег на рассматриваемой стадии рабочего этапа обыска целесообразно действовать в четырех направлениях.

Во-первых, ознакомиться с обстановкой по месту проведения обыска, в том числе: обеспечить сохранность первоначальной обстановки, электронных носителей информации с целью исключения риска повреждения или уничтожения важных источников доказательств, запретив сторонним лицам доступ к ним, а также к их источникам питания; идентифицировать носители информации, посредством которых можно осуществить доступ к электронным и криптокошелькам, их тип, подключение к сети Интернет, проверить их рабочее состояние; используя эффект неожиданности, выяснить у лиц, находящихся по месту производства обыска, реквизиты доступа к их носителям информации, электронным и криптокошелькам, наличие на данных носите-

лях зашифрованных сведений; ознакомиться с первоначальными пояснениями лица, у которого проводится обыск, и иных находящихся в помещении граждан относительно реализации прав владения, пользования и распоряжения интересующими электронными и криптокошельками.

Во-вторых, с учетом складывающейся следственной ситуации запланировать возможность приостановления обыска с целью проведения дополнительных следственных и процессуальных действий, направленных на осмотр и последующий арест токенов и электронных денег. Для этого изначально следует определить конкретные следственные ситуации, которые можно классифицировать по следующим обстоятельствам: рабочий/нерабочий режим функционирования электронных носителей информации, являющихся потенциальными источниками доказательств по делу; готовность/неготовность к сотрудничеству со следствием лица, обладающего доступом к указанным носителям, электронным и криптокошелькам; наличие/отсутствие паролей к электронным носителям информации, электронным и криптокошелькам.

Исходя из представленных обстоятельств можно выделить типичные следственные ситуации: электронные носители информации включены или выключены, лицо, у которого проводится обыск, готово предоставить реквизиты доступа к ним и своим электронным и криптокошелькам (первая следственная ситуация); электронные носители информации включены или выключены, лицо, у которого проводится обыск, отказывается предоставить какие-либо пароли, в том числе к электронным и криптошелькам, но у представителей органа уголовного преследования имеется возможность осуществить к ним доступ (вторая следственная ситуация); электронные носители информации включены или выключены, для доступа к ним требуется неустановленные пароли, лицо, у которого проводится обыск, их не предоставляет, орган уголовного преследования ими не располагает (третья следственная ситуация).

При наличии реквизитов доступа (как в первой и второй следственных ситуациях) следует принять решение о приостановлении обыска для проведения осмотра компьютерной информации по месту его проведения с целью последующего наложения ареста на электронные деньги и токены в соответствии с требованиями ст. 204, 204[1] и 132 УК.

Необходимость приостановления обыска обосновывается рядом причин и обстоятельств, которыми руководствуется следователь, чтобы сохранить сведения, имеющие значение по уголовному делу, обеспечить наложение ареста на токены и электронные деньги. К указанным причинам и обстоятельствам относятся: лицо, у которого производится обыск, категорически отрицает ранее достоверно установленные факты своей преступной деятельности или факты использования электронных и криптокошельков и их носителей; орган уголовного преследования располагает сведениями об иных соучастниках либо осведомленных лицах, имеющих возможность удаленно уничтожить электронную информацию, касающуюся фактов регистрации и использования электронных и криптокошельков, или заблокировать к ней доступ; в ходе внешнего осмотра включенных электронных носителей информации установлено, что их операционная система возможно зашифрована специальными программами (Veracrypt, Truecrypt и др.), а пароль доступа к ней не обнаружен (при выключении данных носителей имеется вероятность утраты доступа к зашифрованному объему памяти); необходимость проверки полученных реквизитов доступа по горячим следам, используя готовность интересуемого лица к сотрудничеству во время обыска.

В-третьих, рассмотрение необходимости применения научно-технических средств и устройств. Так, при наличии первой и второй вышеописанных следственных ситуаций необходимо подготовить к использованию: служебные адреса криптокошельков (аппаратных «холодных» криптокошельков) и электронных кошельков, предназначенных для дальнейшего обеспечения наложения ареста на токены и электронные деньги подозреваемого (обвиняемого) путем их перевода; ноутбук и мобильный принтер для составления протоколов обыска и осмотра компьютерной информации, постановления о наложении ареста; внешний жесткий диск для копирования информации из учетных записей удаленных интернет-ресурсов, включая регистрационные сведения электронных и криптокошельков, используемые IP-адреса при их посещении, историю транзакций токенов и электронных денег, интересуемые пароли, сведения о которых могут быть уничтожены или к ним ограничен доступ; специальное программное обеспечение Belkasoft [12] и (или) FTK Imager [13], среди прочего предназначенное для получения побитовой копии оперативной памяти исследуемого компьютера с целью фиксации реквизитов доступа,

в том числе к электронным и криптокошелькам (работающая компьютерная система в своей оперативной памяти может содержать сведения о паролях, ключах шифрования или дешифрованные приложения, последние сообщения).

В ходе реализации указанного направления надо использовать защитные перчатки, чтобы избежать уничтожения следов человека, обеспечить успешный сбор следов, пригодных для идентификации личности по следам рук и ДНК в случае необходимости по уголовному делу.

В-четвертых, определение последовательности поисковых действий, направленных на обнаружение и изъятие сведений, относящихся к владению, пользованию и распоряжению электронными и криптокошельками. Так, первоочередными объектами поиска являются носители информации, предоставляющие возможность доступа к управлению электронными и (или) криптокошельками, а также предметы и документы, содержащие сведения о их использовании. К таковым относятся: письменные пароли и другие рукописные заметки, бумажные кошельки для токенов, руководства по аппаратному и программному обеспечению, текстовые или графические распечатки, фотографии или информация о личных интересах, ежедневники и блокноты, банковские платежные карточки, сим-карты и слоты их крепления.

После обзорной стадии обыска следует его детальная стадия, в ходе которой следователь или иное процессуально уполномоченное лицо должны определиться с порядком копирования электронной информации и изъятием ее носителей. Данный порядок зависит от наличия вышеуказанных следственных ситуаций.

Далее рассмотрим порядок действий при первой и второй следственных ситуациях.

Учитывая необходимость фиксации и копирования электронной информации об использовании электронных и криптокошельков, наложения ареста на электронные деньги и токены, а также невозможность осуществления указанных действий непосредственно в ходе обыска, его необходимо приостановить, о чем сделать соответствующую отметку в протоколе. Далее, в соответствии с требованиями ст. 204^1 УК, требуется составить протокол осмотра компьютерной информации. Для проведения осмотра учетных записей требуется согласие лица, у которого они находятся в пользовании, или санкция прокурора. В случае отсутствия такого согласия и санкции при наличии у органа уголовного преследования реквизитов доступа к интересуемым учетным записям следователю необходимо вынести соответствующее постановление без санкции прокурора в связи с неотложностью проведения данного следственного действия с указанием идентификаторов учетных записей, которые будут осмотрены. После ознакомления с вышеуказанным постановлением лица, чьи учетные записи будут осмотрены, следователь непосредственно приступает к осмотру компьютерной информации, содержащейся на электронном носителе (это в большинстве случаев компьютерные системы – стационарные ПЭВМ и ноутбуки) и в учетных записях удаленных интернет-ресурсов. При копировании электронной информации следует придерживаться следующего алгоритма:

перед проведением копирования информации из работающей компьютерной системы предварительно подготовить внешний жесткий диск;

посредством USB-порта подключить внешний жесткий диск к целевой компьютерной системе;

определить наличие установленного программного обеспечения, указывающего на использование электронных и криптокошельков; при их идентификации осуществить в них вход (следует учитывать, что в большинстве случаев для входа потребуется мобильный телефон с симкартой, чей абонентский номер прикреплен к вышеуказанным кошелькам);

после входа зафиксировать остатки токенов и электронных денег на кошельках для последующего наложения на них ареста;

при принятии решения о последующем наложении ареста необходимо, используя служебные адреса криптокошельков и идентификаторов электронных кошельков, осуществить перевод токенов и электронных денег подозреваемого (обвиняемого) на них;

после того, когда токены и электронные деньги будут окончательно переведены (это может занять около двух часов), на переведенные суммы, исходя из наличия комиссий при переводах, наложить арест соответствующим постановлением;

определить потенциальные программные приложения для шифрования логических контейнеров или всего диска, обычно Veracrypt, Truecrypt, Bitlocker (в случае установления логического контейнерного шифрования, когда контейнер смонтирован (открыт), но к нему отсутству-

ют реквизиты доступа, надо скопировать интересующие файлы, хранящиеся в зашифрованном контейнере);

создать с использованием программы FTK Imager образ (побитовую копию) оперативной памяти электронного носителя информации;

после окончания копирования в соответствующем протоколе указать объем скопированной информации и ее контрольную сумму.

Учитывая порядок действий при наличии третьей следственной ситуации, а именно то обстоятельство, что получить доступ к электронной информации в режиме реального времени практически невозможно, следователю необходимо:

определить и отобразить в протоколе обыска элементы идентификации компьютерной системы, такие как тип, марка, модель, серийный номер, цвет, различные надписи, а также видимые недостатки и повреждения;

осуществить поиск объектов, которые могут указать на пароль к электронному носителю информации или электронному и криптокошельку;

использовать иные ранее установленные пароли в ходе расследования уголовного дела;

если не удалось получить пароль вышеуказанными способами, то можно попытаться снять образ оперативной памяти посредством подключения служебного компьютера к компьютеру подозреваемого с использованием самого обычного кабеля FireWire (данный способ подходит только в том случае, если имеется соответствующий порт на компьютере). На компьютере специалиста запускается программа, например, Inception или pyfw имеющаяся в открытом доступе [6], с помощью которой все содержимое оперативной памяти исследуемой машины копируется на служебный жесткий диск следователя;

в случае отсутствия возможности получить доступ к электронным носителям информации, отключить от них все подключенные периферийные устройства;

вынуть кабель питания из устройства, после чего записать время, когда это было сделано;

вынуть из стационарного компьютера серверы – устройства для хранения данных (например, накопители на жестких магнитных дисках), после чего поместить их в антистатические пузырчатые обертки.

Указанные мероприятия должны быть подробно описаны в соответствующих протоколах с отображением реального времени и каждого проведенного действия. Отметка о применении служебного носителя указывается в протоколе осмотра компьютерной информации, а изъятие служебного носителя с информацией производится в ходе обыска и оформляется протоколом обыска.

Представленный порядок действий следователя в ходе рабочего этапа обыска при расследовании преступлений, совершенных с использованием токенов и электронных денег, систематизирует имеющийся опыт в указанной области с учетом требований и нововведений законодательства Республики Беларусь, криминалистических и технических аспектов работы с потенциальными источниками доказательств, включая электронные носители информации и использования их в режиме реального времени. Обращение к вышеуказанной классификации следственных ситуаций позволяет определить направления и алгоритм работы с электронными носителями информации, токенами и электронными деньгами. Представленный комплекс следственных и процессуальных действий, которые необходимо планировать и готовить к осуществлению в ходе рабочего этапа обыска, позволит процессуально и тактически грамотно обнаруживать, фиксировать и изымать потенциальные источники доказательств по уголовным делам рассматриваемой категории, налагать в последующем арест на токены и электронные деньги.

Список использованных источников

1. Белкин, Р. С. Криминалистика : учеб. для вузов / Р. С. Белкин. – М. : Норма-ИНФРА-М, 2000. – 990 с.

2. Борьба с киберпреступностью [Электронный ресурс]. – Режим доступа: https://expert.belta.by/kiber. – Дата доступа: 12.09.2021.

3. Гаврилов, Б. Я. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей : учеб. пособие / Б. Я. Гаврилов. – М. : Проспект, 2017. – 171 с.

4. Иванов, А. Н. О новом виде обыска / А. Н. Иванов // Актуальные проблемы криминалистики на современном этапе : сб. науч. ст. : в 2 ч. / под ред. З. Д. Еникеева. – Уфа, 2003. – Ч. 1. – С. 105–109.

5. Илюшин, Д. А. Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг «Интернет» / Д. А. Илюшин // Вестн. Муницип. ин-та права и экономики.– Липецк : Интерлингва, 2004. – Вып. 1. – С. 77–86.

6. Криминалистические средства работы с оперативной памятью [Электронный ресурс]. – Режим доступа: https://xakep.ru/2013/11/16/forensic-ram-ringerprints. – Дата доступа: 16.09.2021.

7. Краснова, Л. Б. «Обыск-осмотр» средств компьютерной техники / Л. Б. Краснова // Воронежские криминалистические чтения : сб. науч. ст. / Воронеж. гос. ун-т ; редкол.: О. Я. Баева (гл. ред.) [и др.]. – Воронеж : ВГУ, 2000. – С. 106–110.

8. Ларин, Е. Г. Копирование информации с электронных носителей при производстве по уголовному делу / Е. Г. Ларин // Законодательство и практика. – Омск : Ом. акад. МВД России, 2012. – № 2. – С. 52–53.

9. Логвин, В. М. О некоторых особенностях тактики обыска в ходе расследования хищений, совершенных путем использования компьютерной техники / В. М. Логвин, Н. Н. Беломытцев // Вестн. Акад. МВД Респ. Беларусь. – 2020. – № 2. – С. 69–74.

10. Мещеряков, В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. ... д-ра юрид. наук : 12.00.09 / В. А. Мещеряков ; Воронеж. гос. ун-т. – Воронеж, 2001. – С. 39.

11. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2018 г., № 1 // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf. – Дата доступа: 22.08.2021.

12. Программное обеспечение Belkasoft [Электронный ресурс]. – Режим доступа: https://belkasoft.com/ru/news. – Дата доступа: 12.09.2021.

13. Программное обеспечение FTK Imager [Электронный ресурс]. – Режим доступа: https://accessdata.com/product-download. – Дата доступа: 12.09.2021.

14. Сапрунов, А. Г. Специфика производства обыска при проверке розыскных версий / А. Г. Сапрунов, Э. С. Данильян // О-во и право. – 2011. – № 3. – С. 274–279.

15. Состояние киберпреступности [Электронный ресурс]. – Режим доступа: https://www.belta.by/society/view/v-nachale-goda-chislo-kiberprestuplenij-v-belarusi-vyroslo-na-240-433123-2021. – Дата доступа: 12.08.2021.

16. Старичков, М. В. Тактика проведения обыска, связанного с изъятием носителей компьютерной информации / М. В. Старичков // Криминалистика: актуальные вопросы теории и практики : сб. тр. участников VII Всерос. науч.-практ. конф. Ростов-на-Дону, 20–21 мая 2010 г. / Рост. юрид. ин-т МВД России, Дон. юрид. ин-т ; редкол.: Г. Ф. Барковский (отв. ред.) [и др.]. – Ростов н/Д : Изд-во Дон. юрид. ин-та, 2010. – С. 167–169.

Дата поступления в редакцию: 14.12.2021

УДК 343.1

***Г. А. Павловец**, кандидат юридических наук, доцент, доцент кафедры уголовного процесса*
Академии Министерства внутренних дел Республики Беларусь
e-mail: pga241083@mail.ru;
***Р. Р. Алекперов**, преподаватель кафедры уголовного процесса*
Академии Министерства внутренних дел Республики Беларусь
e-mail: ruselalekperov@gmail.com

О ЛИБЕРАЛИЗАЦИИ ПРИМЕНЕНИЯ МЕРЫ ПРЕСЕЧЕНИЯ В ВИДЕ ЗАКЛЮЧЕНИЯ ПОД СТРАЖУ

В качестве одного из путей либерализации уголовно-процессуального законодательства обосновывается возможность закрепления в Уголовно-процессуальном кодексе Республики Беларусь обстоятельства, исключающего применение к подозреваемому, обвиняемому меры пресечения в виде заключения под стражу, – состояние здоровья лица. Предлагаются изменения в соответствующий нормативный правовой акт МВД Республики Беларусь и Министерства здравоохранения Республики Беларусь с целью практической реализации соответствующего положения и дальнейшего реформирования уголовно-процессуального закона.

Ключевые слова: заключение под стражу, мера пресечения, обвиняемый, обстоятельство, подозреваемый, права, состояние здоровья.