

Дата поступления рукописи в редакцию: 05.07.2026 г.

Дата принятия рукописи в печать: 23.08.2026 г.

ГОНЧАР Владимир Владимирович,

доцент кафедры информационных технологий и
организации расследования киберпреступлений
Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева,
e-mail: vg0778@bk.ru

ПАСЮКОВ Сергей Эдуардович,

сотрудник УВД по САО г. Москвы,
e-mail: spasukov2@yandex.ru

ОСОБЕННОСТИ ПОЛУЧЕНИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ ПРИ ПРОТИВОДЕЙСТВИИ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ В ПСЕВДОДОМЕННЫХ ЗОНАХ СЕТИ ИНТЕРНЕТ

Аннотация. В данной статье рассматриваются отдельные направления получения доказательственной информации при расследовании преступлений совершаемых с использованием анонимных торговых площадок.

Ключевые слова: анонимные торговые площадки, сбор доказательств, получение доказательственной информации, псевдодоменная зона, зона .onion, сеть Tor, классификация анонимных торговых площадок, темный Интернет.

GONCHAR Vladimir Vladimirovich,

Associate Professor, Department of Information Technologies
and Organization of Cybercrime Investigations,
A.Ya. Sukharev Moscow Academy of the
Investigative Committee of the Russian Federation

PASYUKOV Sergey Eduardovich,

Officer, Directorate of Internal Affairs for the
Northern Administrative District of Moscow

FEATURES OF OBTAINING EVIDENTIAL INFORMATION IN COUNTERING CRIMES COMMITTED IN PSEUDODOMAIN ZONES OF THE INTERNET

Annotation. This article examines certain approaches to obtaining evidentiary information in the investigation of crimes committed using anonymous marketplaces.

Key words: anonymous trading platforms, evidence collection, obtaining evidentiary information, pseudo-domain zone, .onion zone, Tor network, classification of anonymous trading platforms, the dark web.

Работа с материальными объектами и цифровыми носителями - это один из самых важных и ответственных этапов расследования. Именно на нём вся информация, собранная во время цифровой разведки - IP-адреса, никнеймы, хеши транзакций. Такая информация перестаёт быть просто оперативными данными и становится настоящими вещественными доказательствами.

Теперь их можно полноценно исследовать и предъявлять в суде. Здесь цена ошибки очень высока: одна мелкая оплошность при изъятии или обработке может полностью уничтожить ценность материалов или привести к тому, что суд их не примет.

Подготовка к изъятию начинается с вниматель-

ного изучения всех имеющихся разведданных.

Нужно примерно понимать, какое оборудование ожидать у подозреваемого. Если это администратор площадки, то скорее всего там будут серверы, маршрутизаторы с туннелями Tor и аппаратные криптокошельки. У рядового продавца внимание в первую очередь обращают на обычные компьютеры, мобильные телефоны и всё, что связано с упаковкой товара.

Один из главных рисков при работе с цифровыми носителями - удалённое уничтожение информации. Вредоносные программы и скрипты часто настроены на срабатывание, если владелец не подаст контрольный сигнал (dead man's switch) или если

кто-то попытается получить доступ извне.

После проникновения на объект всю технику нужно срочно отрезать от внешних сетей: отключить кабель, выключить Wi-Fi и обязательно убрать телефоны в экранирующие пакеты Faraday bags, которые полностью глушат радиосигнал.

Осмотр места происшествия и изъятие техники - две разные вещи.

Осмотр нужен, чтобы зафиксировать обстановку и найти носители.

Изъятие же делается для того, чтобы сохранить данные в том виде, в каком они были. Перед изъятием обязательно оценивают состояние устройств: включены они, выключены, зашифрованы ли диски, запущены ли виртуальные машины. От этого зависит, как действовать дальше - проводить криминалистические манипуляции на месте или забирать оборудование выключенным.

Решение об отключении питания принимают прямо на месте. Если компьютер работает и на экране видно открытые мессенджеры, браузер с авторизацией на площадке или идёт копирование файлов, то сначала снимают дампы оперативной памяти (RAM). Там могут быть ключи шифрования, пароли и последние действия пользователя. После выключения всё это пропадёт безвозвратно. Для дампа используют специальные утилиты с внешней флешки. Образ сохраняют на отдельный диск, и только потом компьютер выключают штатно. Выдергивать шнур из розетки нельзя - это ломает файловую систему и сильно усложняет последующий анализ.

Если компьютер уже выключен, его забирают как есть. Включать для проверки запрещено: автозагрузка изменит временные метки файлов и может запустить механизмы самоуничтожения. Всю изъятую технику упаковывают в антистатические пакеты и перевозят в жёстких кейсах, чтобы ничего не повредить по дороге.

Особое внимание уделяют аппаратным криптокошелькам и бумажным носителям с seed-фразами. Без PIN-кода или фразы восстановления доступ к средствам легко потерять. Поэтому во время обыска параллельно ищут любые записки с паролями, блокноты с мнемоническими фразами, фотографии экранов и другие носители с доступами.

Когда носители доставили в лабораторию, начинают создавать криминалистические копии. Обычное копирование файлов здесь не годится - при этом теряются удалённые данные и меняются атрибуты. Нужно делать полный побитовый образ всего физического диска. Чтобы случайно ничего не изменить, используют аппаратные блокираторы записи, которые физически разрешают только чтение. Без них операционная система может сама внести изменения, и образ станет бесполезным для суда.

Весь процесс подробно описывают в протоколе: модель диска, серийный номер, объём, способ подключения. Программы типа EnCase, FTK Imager или X-Ways считывают диск сектор за сектором, включая неразмеченное пространство, и формируют файл-образ. После копирования проверяют

хеш-суммы по MD5 и SHA-256. Если они совпали — копия идентична оригиналу.

Делают два образа: один идёт в работу как рабочий, второй хранят опечатанным как контрольный. После этого оригинальный носитель больше не трогают и отправляют на хранение.

Анализ цифрового образа - один из самых тяжёлых этапов. Его проводят только на рабочей копии. Сначала определяют файловую систему и монтируют образ в изолированную среду. Программа сканирует диск, восстанавливает папки, индексирует содержимое и ищет известные сигнатуры файлов. Даже удалённые файлы часто оставляют свои фрагменты на диске. Восстановление помогает найти переписку, которую пытались стереть. Анализ реестра Windows или plist-файлов macOS показывает, какие устройства подключались, когда и какие документы открывались.

Отдельно изучают данные браузеров. Даже при Tor Browser в системе могут остаться следы: временные файлы, журналы DNS, ярлыки запуска.

Если подозреваемый выходил в обычный интернет для обмена валюты, история обычного браузера покажет посещения бирж и обменников.

С зашифрованными контейнерами (Veracrypt, TrueCrypt, BitLocker) работают отдельно. Если пароль не нашли при обыске, применяют криптоанализ.

На практике люди часто ошибаются: хранят пароли в браузере, оставляют их в текстовых файлах на рабочем столе или используют один и тот же пароль для разных сервисов.

Помимо цифровых носителей, тщательно изучают материальные объекты. Упаковочные материалы (пакеты, скотч, весы) проверяют на микрочастицы, отпечатки пальцев и ДНК. Если упаковка у подозреваемого похожа на ту, что изъяли у покупателей, или есть характерный способ склеивания - это уже хороший признак конкретного продавца.

Черновые записи и блокноты часто содержат то, что человек не хочет держать в компьютере: адреса закладок, координаты встреч, расчёты, схемы логистики. Почерковедческая экспертиза устанавливает автора, химический анализ - время создания записей. Даже обрывки бумаги из мусорного ведра после восстановления иногда оказываются полезными.

Анализ движения наличных денег нужен, чтобы связать их с операциями в блокчейне [1]. Если сумма и время изъятия совпадают с выводом средств из кошелька — это косвенное доказательство таких операций. Состав купюр, серийные номера и следы веществ на банкнотах тоже имеют значение.

Когда цифровые данные и материальные объекты объединяют, вырисовывается полная картина. Переписка и фотографии товара на компьютере подкрепляются самим товаром и весами, найденными дома. Если в телефоне есть сообщения о продаже партии на определённую дату, а дома лежит точно такой же товар - цепочка доказательств становится крепкой. Цифровые следы объясняют, откуда взялись вещи, а вещи подтверждают, что цифровые планы были реальными.

Анализ метаданных фотографий и видео (EXIF) может показать модель камеры, дату и время съёмки, а иногда и координаты. Это помогает привязать человека к конкретному месту.

Сравнение временных меток - времени создания файлов, отправки сообщений и изъятия товара - позволяет восстановить последовательность действий всей группы [2].

Всё завершается правильным процессуальным оформлением. Каждое действие фиксируют в протоколах и экспертных заключениях. В протоколе выемки подробно описывают каждый предмет, где его нашли и как он выглядит. К нему прилагают таблицы хеш-сумм, акты упаковки и опечатывания.

Эксперт в заключении должен чётко ответить на вопросы следствия: история видоизменения файлов, удалялась ли информация, что находится в зашифрованных контейнерах и как всё это между собой связано.

Если работу с материальными объектами и цифровыми носителями провести правильно, то можно уверенно переходить от простого сбора информа-

ции к формированию настоящих доказательств. Эти материалы потом становятся основой для корреляции цифровых идентификаторов - этапа, на котором все разрозненные следы собирают воедино и доказывают, что они принадлежат одному человеку

Список литературы:

[1] Тисен О.Н. Механизм совершения преступлений с использованием криптовалют: по результатам анализа следственной и судебной практики// Российский следователь. 2024, №5. С. 7-11.

[2] Тисен О.Н. Субъекты досудебного соглашения о сотрудничестве// Судебная власть и уголовный процесс. 2013, №2, С. 91-95.

References:

[1] Tisen O.N. Mechanism of committing crimes involving cryptocurrencies: based on an analysis of investigative and judicial practice // Russian Investigator. 2024, No. 5. Pp. 7-11.

[2] Tisen O.N. Parties to a pre-trial cooperation agreement // Judicial Power and Criminal Process. 2013, No. 2, Pp. 91-95.