СПОСОБЫ СОКРЫТИЯ СЛЕДОВ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Ширяев А.В.
Алтайский государственный университет, г. Барнаул
email: anton.vyacheslavovich@inbox.ru

Аннотация. В статье рассматриваются способы сокрытия следов преступления в зависимости от видовой принадлежности преступного деяния, многообразия следов конкретного преступления, как например, кибермошенничества, где присутствуют идеальные, виртуальные и материальные следы.

Ключевые слова: способы сокрытия, кибермошенничество, следы преступления, компьютерная информация.

Лицо, совершившее преступление, стремится максимально возможно скрыть его следы в целях избежания ответственности за содеянное. Р.С. Белкин сокрытие следов преступлений рассматривает как преступную деятельность, направленную на воспрепятствование расследованию преступлений. Она может осуществляться «путем утаивания, уничтожения, маскировки или фальсификации следов преступления либо их носителей». Сокрытие может осуществляться как в активной, так и пассивной форме. В первом случае – это активное уничтожение следов, данных, в том числе информации, ее носителей. Во втором случае – это, чаще всего умолчание об известных обстоятельствах. Кроме того, для сокрытия может применяться маскировка, например, программно-аппаратный сбой, противоправные действия иных лиц и многое другое, при этом для сокрытия электронно-цифровых следов может применяться не только вредоносное, но и законное программное обеспечение, например, позволяющее безвозвратно удалять информацию с носителя путем многократной ее перезаписи [1, с. 165].

Под инсценировкой преступлений Р.С. Белкин понимает «создание обстановки, не соответствующей происшедшему на этом месте событию». При этом Р.С. Белкин предлагает классифицировать способы инсценировки, выделяя по целям – направленные на сокрытие преступления либо деяния, не имеющего криминальный характер, аналогичным образом осуществляется разделение по объекту. Кроме того, по объекту ученый выделяет деление на случаи, когда инсценировка затрагивает отдельные эпизоды, части события, либо все событие в целом. Наиболее интересной является выделенная Р.С. Белкиным классификация по способу легализации – это рассчитанная на то, что событие не будет обнаружено вообще и рассчитанная на обнаружение события [2, с. 29].

Все описанные способы сокрытия следов преступления, в том числе инсценировка, применимы по отношению к кибермошенничеству. Информация как таковая, используется в данном случае для совершения преступления. Преступник может преследовать цели добыть данную информацию, чтобы использовать ее для совершения хищения. Может видоизменить, сформировать ложную информацию, тем самым облегчая себе совершение преступления. В частности, благодаря программному обеспечению непосредственно на оборудовании банка создать платежный документ либо реестр платежей[1]. В этом случае источник формирования информации – непосредственно законный владелец. Следы постороннего вмешательства либо не отслеживаются, либо уничтожаются вредоносным вирусным

[1] Определение Второго кассационного суда общей юрисдикции от 23.07.2020 по делу № 88-15382/2020 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/search/?q=Определение+Второго+кассационного+суда+общей+юрисдикции+от+23.07.2020+по+делу+№+88-15382%2F202-(25.11.2020).

программным обеспечением. Можно использовать доступ к чужому оборудованию, используя программное обеспечение, которое не позволяет отследить источник вмешательства, как, например, это было выявлено по одному из дел в судебной правоприменительной практике, когда преступник использовал чужое оборудование для совершения за счет его собственника звонков в разные страны, вследствие чего образовалась крупная задолженность [1].

Сходным по способу совершения способ сокрытия следов за счет инсценировки совершения действий самим потерпевшим является и «фарминг». При данном способе используется возможность переадресации с официальных сайтов организации на их мошеннические копии, где преступники и получают необходимые им данные [3, с. 34]. Внешне это выглядит как действия совершенные потерпевшим, порой совершенные неудачно, например, при попытке заказать товар. Нередко подобные способы используются при создании копий сайтов для заказа билетов, предполагающих введение персональных данных пассажира. Взаимодействие с мошенническим сайтом, который может существовать в сети непродолжительное время либо просто больше не использоваться преступниками, не позволяет достоверно установить, кто именно получил запрошенную информацию, а затем воспользовался ею для своих преступных целей.

Как отмечает в своем исследовании П.В. Малышкин, специфика преступлений в сфере компьютерной информации заключается в том, что способ и механизм совершения прорабатываются и реализуются таким образом, чтобы уже на стадии совершения преступления совершить действия, направленные на его сокрытие. Чаще всего для данных целей, по утверждению П.В. Малышкина, используется новейшее программное обеспечение, а также способы инсценировки, когда выявленные следы преступления указывают на иное лицо, что обеспечивает анонимность и снижает риск выявления преступника. В числе известных в настоящее время программ П.В. Малышкин выделяет программы, использующие принцип «луковичной маршрутизации», обеспечивающих анонимность при посещении сайтов в сети интернет и используемые порой вполне легально, в том числе для защиты собственной персональной информации от посягательств третьих лиц [4, с. 43].

В аналитическом обзоре о новых способам совершения преступлений указано, что с целью сокрытия следов преступлений в последние годы все чаще используются такие анонимайзеры как «VPN», «TOR», «Proxy». Использование данных программ предполагает не только шифрование передаваемых и получаемых сведений, но и серверов, неподконтрольных российским правоохранительным органам. Кроме того, широкое распространение получили программы-вымогатели malware типа RANSOMWARE, которые можно разделить на два вида: шифровальщики и блокировщики. Применение данных программ позволяет заблокировать или зашифровать информацию, а впоследствии требовать денежные средства за обеспечение доступа к ней.

Следы совершения преступления блокируются за счет невозможности установить источник заражения вирусом, а также за счет возможности анонимного обналичивания денежных средств либо их иного использования, например, для оплаты товаров, заказываемых из-за рубежа, когда идентификация покупателя не осуществляется либо крайне затруднена, потому что покупатель и мошенник – не одно и то же лицо [3, с. 41].

Как способ сокрытия следов совершения преступления при кибермошенничестве можно рассматривать активное вовлечение потерпевшего в его

[1] Постановление Десятого арбитражного апелляционного суда от 17.03.2017 по делу № А41-56987/16 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/search/?q=Постановление+Десятого+арбитражного+апелляционного+суда+от+17.03.2017+по+делу+№+А41-56987%2F16 -(25.11.2020).

совершение. В частности, в аналитическом обзоре о новых способах совершения преступлений в сфере информационных технологий на территории государств – участников СНГ [3, с.25] указано, что довольно широкое распространение получил способ, когда действия, направленные на хищение принадлежащих потерпевшему денежных средств, совершаются самим потерпевшим под руководством преступником. Потерпевшему сообщается о необходимости снятия всех денежных средств и временного зачисления их на так называемые «резервные счета», данные о которых сообщают преступники. В этом случае внешне все выглядит так, как будто потерпевший сам, по собственной воле снял и перечислил третьим лицам деньги. Сами преступники определенное вмешательство в процесс совершения хищения осуществляют дистанционно на стадии телефонных переговоров, пользуясь функцией подмены номера телефона, а также впоследствии, на стадии получения денежных средств, когда используются современные технологии, позволяющие получить деньги, не участвуя в процессе лично. Отчасти, с учетом того, что телефонные переговоры сотовыми операторами записываются и хранятся на протяжении определенного периода времени, подобные следы могут быть выявлены. В том числе путем получения записи разговора, установления номера, с которого был сделан звонок. Однако даже наличие подобных доказательств зачастую не способствует раскрытию преступления, вследствие чего уголовные дела оказываются приостановленными по причине не установления лиц, причастных к совершению преступления.

Если принять во внимание возможность совершения подобных звонков не с территории России, а с территории иного государства, то можно утверждать, что раскрытие преступления будет крайне затруднено. Отношение к допустимости записи телефонных переговоров в отсутствие санкции суда, к их хранению и возможности последующего использования различно в разных странах. Международное же сотрудничество в сфере противодействия кибермошенничеству еще не находится на том уровне, когда получение информации возможно оперативно и в том объеме, который необходим для расследования преступления.

Сокрытие следов преступления существенно облегчается в том случае, когда речь идет о групповом совершении преступления, а в особенности при совершении кибермошенничества в составе организованной группы, когда обеспечивается анонимность руководящих лиц. В результате непосредственные исполнители, которые чаще выявляются правоохранительными органами, ничего не могут сообщить о составе преступной группы, о ее руководстве, масштабах действий и так далее. Причина этого во многом обусловлена спецификой преступлений, а именно, сложностью способов их совершения за счет применения различных приемов сокрытия следов преступлений [5, с. 90-97].

Вовлечение в преступную деятельность сотрудников мобильных операторов, банков, не только позволяет оперативно получить доступ к необходимой информации, но и скрыть следы вмешательства. Например, в ситуации с использованием sim-карт вовлечение в совершение преступления сотрудника мобильного оператора позволяет без участие потерпевшего заблокировать карту, выпустить новую, а затем, с ее использованием получить доступ к «мобильному банку», переведя деньги на любые счета[1]. Иногда данные преступления совершаются сотрудниками компаний – мобильных операторов самостоятельно, что

[1] Приговор Юргинского городского суда Кемеровской области от 09.04.2015 по делу № 1-5/2015 [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/U4T0VseBlSUx/?regular-txt=&regular-case_doc=1-5%2F2015&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=Юргинский+городской+суд+%28Кемеровская+область%29&regular-judge=&_=1607011504561 - (25.11.2020).

еще существенно повышает возможности скрыть следы преступления, изменив информацию о sim-картах и совершенных с их использованием действий [3, с. 28].

Чтобы проиллюстрировать правильность приведенных выше утверждений, необходимо обратиться к анализу судебной правоприменительной практики. По уголовному делу № 1-218/2018, рассмотренному Железногорским городским судом Курской области, преступник, имея правомерный доступ в базам данных сотового оператора в силу того, что являлся его сотрудником, изготавливал поддельные заявления владельцев sim-карт о замене карты[1]. Тем самым он желал создать впечатление, что переводы средств со счетов осуществлялись непосредственно самими правообладателями.

Сходный способ сокрытия следов преступления был применен преступником по делу № 1-345/2019, рассмотренному Кировским районным судом города Ростова-на-Дону[2]. Однако здесь преступник не только создавал видимость обращения обладателей sim-карт с просьбой о их замене, но и постарался уничтожить информацию непосредственно в системе сотового оператора, чтобы невозможно было установить дату внесения изменений в сведения и даты списания средств со счетов клиентов.

По другому делу № 1-277/2018, которое было рассмотрено Балаковским районным судом Саратовской области, преступник использовал не только наличие у него правомерного доступа к базам данных, но и наличие сведений о логинах и паролях иных сотрудников, чтобы войти в систему и изменить данные от их имени, а не от своего. Тем самым обеспечивалось сокрытие факта участия в совершении преступления, а также создавалась видимость правомерности совершенных действий, чтобы в случае обнаружения факта совершения преступления можно было утверждать, что действия инициированы потерпевшими и правомерно совершены работниками компании мобильного оператора[3]. Чужие логин и пароль использовал преступник и по уголовному делу № 1-621/2018, рассмотренному Ленинским районным судом города Новосибирска[4].

Отдельная категория кибермошенничеств – это те, которые совершаются сотрудниками коммерческих организаций, имеющих право доступа к электронной подписи, используемой для взаимоотношений с банковскими организациями. В этом случае лицо старается создать видимость совершения правомерных операций, пользуясь отсутствием реального и досконального контроля за движением средств на счетах организации. Неправомерный доступ к электронной подписи для целей создания второй электронной подписи был использован преступником по делу № 1-202/2017, рассмотренному Куйбышевским районный судом города Санкт-

[1] Приговор Железногорского городского суда Курской области от 15.10.2018. Уголовное дело № 1-218/2018 [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/BTGs3iNkWxUw/?regular-txt=&regular-case_doc=1-218%2F2018&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=Железногорский+городской+суд+%28Курская+область%29&regular-judge=&_=1607011682180 - (25.11.2020).

[2] Приговор Кировского районного суда г. Ростова-на-Дону от 13.09.2019. Уголовное дело № 1-345/2019 [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/LkG0QbZcSoNb/ - (25.11.2020).

[3] Приговор Балаковского районного суда Саратовской области от 21.06.2018. Уголовное дело № 1-277/2018 [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/BMIxiOAh1RUO/ - (25.11.2020).

[4] Приговор Ленинского районного суда г. Новосибирска от 04.10.2018. Уголовное дело № 1-621/2018 [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/Z3bJY9UEbHlv/?regular-txt=&regular-case_doc=1-621%2F2018&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=Ленинский+районный+суд+г.+Новосибирска+%28Новосибирская+область%29&regular-judge=&_=1607011921763 - (25.11.2020).

Петербурга[1]. Наличие доступа к электронной цифровой подписи, при помощи которой осуществлялся документооборот с банковской организацией, позволил сформировать платежное поручение, которое было воспринято банковской системой проверки как допустимое и оформленное надлежащим образом.

Следует также заострить внимание на одном из уголовных дел, приговор по которому был изучен. Приговором Тобольского городского суда Тюменской области от 19 февраля 2018 года по уголовному делу № 1-79/2018 была осуждена сотрудница банка[2]. У нее в силу занимаемой должности был обширный доступ к персональным данным клиентов банка, а также к банковским картам, выпущенным, но не выданным клиентам. Банковские карты до момента их выдачи и активации невозможно использовать. Преступнице это было известно. При этом она имела возможность, обращаясь к базам данных банковской организации, получить сведения о наличии денежных средств на счетах, привязанных к не выданным банковским картам. Обращает на себя внимание то обстоятельство, что, понимая легкость проверки сведений о получении банковских карт клиентами банка, сотрудница не использовала специальных способов сокрытия факта совершения преступления. Она просто активировала в ближайшем банкомате карты, зная пин-код, затем снимала денежные средств. При этом необходимо отметить, что подобные действия преступница совершала на протяжении длительного периода времени систематически. Не было препятствием для совершения преступления и то обстоятельство, что банкоматы, при помощи которых были сняты денежные средства с карт, оборудованы видеокамерами.

Скрыть следы преступления возможно и физически уничтожив носитель информации. Современные технологии позволяют в определенных случаях восстановить утраченную информацию, но только при наличии самого, пусть поврежденного носителя. Если же, например, выкинуть носитель в водоем, оставить его в труднодоступном месте, предварительно повредив, или полностью уничтожить тем или иным способом, то восстановить информацию будет невозможно. Как следствие будет невозможно доказать причастность определенного лица к совершению преступления, а порой и сам факт совершения преступления, вследствие чего раскрываемость кибермошенничеств существенно снижается.

Преступники, совершая высокотехнологичные преступления, обычно имеют хорошие специальные знания и навыки работы с компьютерной техникой, всегда стремятся уничтожить или скрыть любые следы преступления, либо только часть их, которая может их персонифицировать [6, с. 256-259].

Преступники чаще избавляются от носителей, выбрасывая, оставляя в людных местах, где заполучить, например, телефон, может любое лицо, непричастное к совершению преступления. Подобная ситуация используется преступниками для обоснования своей непричастности к совершению преступления.

Стоит отметить, что даже опытные киберпреступники бывают не готовы к современным силам и средствам оперативно-розыскной деятельности, например, прослушиванию их телефонных переговоров по только приобретенным средствам сотовой связи или sim-картам [7, с. 114-126].

В частности, по одному из дел, осужденный, оспаривая постановленный в отношении него обвинительный приговор, указал, что мобильный телефон, с использованием которого были совершены преступления, был найден не у него, то

[1] Приговор Куйбышевского районного суда г. Санкт-Петербурга от 25.05.2017. Уголовное дело № 1-202/2017 [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/z0QzgCqg4Mou/ - (25.11.2020).

[2] Приговор Тобольского городского суда Тюменской области от 19.02.2018. Уголовное дело № 1-79/2018 [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/dhxhC74ATAND/ - (25.11.2020).

есть не лично при нем и не в месте его проживания. Данный довод, по мнению осужденного, должен был подтвердить его непричастность к совершению преступления.

Однако суды всех инстанций, рассматривавшие дело, отвергли данный довод, сославшись на заключение судебной экспертизы, а также на данные о соединениях, которые устанавливались при помощи данного мобильного телефона[1]. Кроме того, по делу было установлено, что преступник, посредством сети «Интернет», используя программу для удаленного администрирования персонального компьютера, путем несанкционированного подбора пароля от администраторской учетной записи осуществил удаленный доступ к банкомату, установленному в торговом центре, и установил на жесткий диск банкомата файлы компьютерных программ, позволяющих управлять оборудованием банкомата, в том числе давать команды на выдачу денежных средств. Через мессенджер преступник сообщил осужденному о запуске компьютерных программ на банкомате и о готовности к хищению денежных средств. Обращает на себя внимание то обстоятельство, что преступник, которому удалось воспользоваться программным обеспечением для доступа к банкомату, так и не был установлен и привлечен к уголовной ответственности. Осуждены были только исполнители. Детально восстановить способ установления неправомерного администрирования банкомата, с использованием которого было совершено хищение, также не удалось, поскольку само по себе программное обеспечение позволяло скрыть данные о его установке, то есть о времени, а также способе – имело ли место дистанционное вмешательство либо непосредственное воздействие на банкомат. С учетом того, что банкомат был установлен в людном месте – торговом центре, можно предположить, что воздействие было дистанционным иначе действия преступника неизбежно бы привлекли внимание, поскольку подобная установка требует определенного времени.

Среди действий преступника по отношению к компьютерной информации в процессе сокрытия преступления, согласно Н. Ахтырской, можно выделить следующие группы: сокрытие путем утаивания информации; сокрытие путем уничтожения информации; сокрытие путем маскировки информации и сокрытие путем фальсификации информации [8].

Факт сокрытия следов преступления, в том числе за счет инсценировки события, может быть установлен за счет выяснения следующих вопросов:

- не проявлял ли кто-либо интереса к компьютерной информации, программному обеспечению, компьютерной технике данного предприятия, организации, учреждения, фирмы или компании;
- не появлялись ли в помещении, где расположена компьютерная техника, посторонние лица, не зафиксированы ли случаи работы сотрудников с информацией, не относящейся к их компетенции:
- не было ли сбоев в работе программ, хищений носителей информации и отдельных компьютерных устройств;
- зафиксированы ли сбои в работе компьютерного оборудования, электронных сетей, средств защиты компьютерной информации;
- как часто проверяются программы на наличие вирусов, каковы результаты последних проверок;
- как часто обновляется программное обеспечение, каким путем, где и кем оно приобретается;

[1] Постановление Президиума Верховного суда Республики Татарстан от 10.07.2019 № 44у-141 [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/search/?q=Постановление+Президиума+Верховного+суда+Республики+Татарстан+от+10.07.2019+№+44у-141.+ - (25.11.2020).

- каким путем, где и кем приобретается компьютерная техника, как осуществляется ее ремонт и модернизация;
- каков на данном объекте порядок работы с информацией, как она поступает, обрабатывается и передается по каналам связи;
- кто еще является абонентом компьютерной сети, к которой подключены компьютеры данного предприятия, организации, учреждения или фирмы, каким образом осуществляется доступ в сеть, кто из пользователей имеет право на работу в сети, каковы их полномочия;
- как осуществляется защита компьютерной информации, применяемые средства и методы защиты и др.
- имели ли место случаи неправомерного доступа к компьютерной информации ранее, если да, то, как часто;
- могли ли возникшие последствия стать результатом неосторожного действия лица или неисправности работы ЭВМ, системы ЭВМ, сбоев программного обеспечения и т.п.;
- каков характер изменений информации;
- кто является собственником (владельцем или законным пользователем) скопированной (уничтоженной, модифицированной, блокированной) информации и др. [9, с. 113].

Проблематичность выявления фактов сокрытия следов преступления обусловлена тем, что даже спустя непродолжительное время все следы, которые не были обнаружены в ходе первоначального осмотра места происшествия, могут быть утрачены. Выступает ли местом происшествия помещение организации или жилище гражданина, после завершения первоначальных следственных действий там возобновляется привычный рабочий или бытовой ритм, в результате чего уничтожаются все следы преступления.

Как правило, преступные деяния в сфере информационных технологий состоят из нескольких составляющих звеньев, каждое из которых территориально удалено от других. Например, преступник, находящийся в Барнауле, посредством сети Интернет может совершить несанкционированное проникновение в серверный центр банковской организации, расположенный в Екатеринбурге, незаконно перевести денежные средства на счета своего сообщника, который обналичит их посредством банкомата, расположенного в Нижнем Новгороде. В некоторых способах совершения преступлений могут быть использованы одновременно тысячи компьютеров, зараженных вредоносным программным обеспечением, а их местоположение может быть на территории разных государств [10, с. 123-127].

На основании проанализированной судебной правоприменительной практики можно утверждать, что в число раскрываемых кибермошенничеств входят те, по которым преступники не использовали специальные способы сокрытия следов преступления. Это наиболее примитивные способы кибермошенничества, не предполагающие наличия у преступника специальных познаний и использования вредоносного программного обеспечения. Никакие способы сокрытия следов чаще всего не используются теми, кто похищает денежные средства, пользуясь доступом к телефону и установленной в нем sim-картой. В отдельных подобных случаях преступники удаляют sms-оповещения о переводе денежных средств, чтобы собственник телефона и владелец счета не заметил факт снятия.

В число достоверно установленных способов сокрытия следов преступления вошли такие, как:

- использование устройств, не идентифицированных в ходе следствия;
- изготовление поддельных заявлений владельцев sim-карт о замене карты с целью придания действиям вида правомерных;

- использование чужого логина и пароля для доступа к базе данных. Использование вымышленные персональных сведений для регистрации sim-карт, на счета которых переводились денежные средства;
- создание иных подложных документов с целью придания операциям вида правомерных;
- использование вредоносного программного обеспечения;
- перечисление денежных средств на счета третьих лиц, непосредственно не вовлекаемых в совершение преступления и не осведомленных о неправомерном способе получения денежных средств;
- удаление сведений о сообщениях, связанных с перечислением средств непосредственно из телефона потерпевшего.

Использование специального оборудования, как показывает анализ судебной правоприменительной практики, наряду с вредоносным программным обеспечением позволяет максимально скрыть данные о личности преступника, о характере доступа к информации, о времени и месте совершения преступления. Подобные дела раскрываются крайне редко и только в ситуации, когда один из непосредственных исполнителей, как правило, вовлеченных в финальную стадию обналичивания денежных средств, дает признательные показания и заключает соглашение о досудебном сотрудничестве. Обвинительный приговор выстраивается исключительно на признательных показаниях и, как правило, ограничивается теми эпизодами, в которые непосредственно было вовлечено привлеченное к уголовной ответственности лицо. Изложенное позволяет сделать определенные выводы.

Сокрытие следов преступлений при совершении кибермошенничества может осуществляться различными способами. Речь может идти и об искажении информации, в том числе об источнике доступа к ней, об источнике формирования информации, о времени ее формирования, и об уничтожении информации либо ее носителя. Сокрытие следов нередко обеспечивается за счет использования программного обеспечения, которое самостоятельно, после совершения несанкционированных и явно противоправных действий в автоматическом режиме удаляет сведения о вмешательстве.

Уничтожение самого носителя информации при отсутствии копий гарантированно позволяет затруднить ход расследования уголовного дела, поскольку причинно-следственные связи между негативными общественно опасными последствиями и деянием преступника установить не удается, вследствие чего производство по уголовному делу приостанавливается на неопределенно длительный срок. Использование преступниками разнообразных и эффективных способов сокрытия следов преступления можно определить как одну из причин низкой раскрываемости кибермошенничеств. В число раскрываемых входят преимущественно те случаи, когда кибермошенничество имеет примитивный характер и преступник не использует специальных способов для сокрытия следов преступления.

Библиографический список

1. Поляков, В.В. Средства совершения компьютерных преступлений // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2014. – № 2 (32). – С. 165.
2. Белкин Р.С. Криминалистическая энциклопедия / Р.С. Белкин. – М.: Мегатрон XXI, 2000. – С. 29.
3. Колчевский И.Б., Журавлев В.М., Кузнецов А.Г. и др. Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ: аналитический обзор // М.: ФГКУ «ВНИИ МВД России», 2018.

4. Малышкин П.В. Способы сокрытия преступлений, совершаемых с применением информационных компьютерных технологий // Вестник Мордовского университета. – 2014. – № 4. – С. 43.
5. Polyakov V. (2019). Criminalistics specifics of methods of committing computer crimes and peculiarities of their prevention. Religacion. Journal of Social Sciences and Humanities. – Vol. 4 (21). – pp. 90-97.
6. Поляков, В.В. Особенности личности компьютерных преступников / В.В. Поляков, Л.А. Попов // Известия Алтайского государственного университета. – 2018. – № 6 (104). – С. 256-259.
7. Поляков, В.В. Основы формирования криминалистической методики расследования высокотехнологичных преступлений // Уголовное судопроизводство: правовое, криминалистическое и оперативно-розыскное обеспечение : монография / под ред. С.И. Давыдова – Барнаул : Изд-во Алт. ун-та, 2019. – С. 114-126.
8. Ахтырская, Н.Н. Формы противодействия расследованию преступлений, совершаемых в сфере компьютерных технологий [Электронный ресурс] // Режим доступа: http://www.skte.narod.ru/lib010.htm - (25.11.2020).
9. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации. – М.: ЮИ МВД РФ, Книжный мир, 2015. – С. 113.
10. Поляков, В.В. Начальные следственные ситуации расследования высокотехнологичных преступлений // Цифровые технологии в юриспруденции: генезис и перспективы: материалы I Международной межвузовской науч.-практ. конф., Красноярск, 28 февраля 2020 г. – Красноярск, 2020. – С. 123-127.

METHODS FOR COVERING TRACES OF FRAUD IN THE SPHERE OF COMPUTER INFORMATION

Shiryaev A.V.
Altai State University, Barnaul
email: anton.vyacheslavovich@inbox.ru

Abstract. The article examines the ways of concealing the traces of a crime depending on the type of criminal act, the variety of traces of a specific crime, such as cyber fraud, where there are ideal, virtual and material traces.

Keywords: methods of concealment, cyber fraud, traces of a crime, computer information.