МВД России
Санкт-Петербургский университет
Ленинградский областной филиал

Э.В. Лантух

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Учебно-методическое пособие

Ленинградская область
2023

План-график 2023, поз. 133

УДК 347.948.2
ББК 67.52
Л 22

Лантух Э.В.

Л 22 Использование специальных знаний при расследовании преступлений в сфере информационных технологий: учебно-методическое пособие: Изд-во ЛОФ СПб ун-та МВД России, 2023. – 64 с.

ISBN: 978-5-91837-707-9
EDN: LYRUCQ

В учебно-методическом пособии предполагается рассмотрение вопросов, связанных с использованием специальных при расследовании преступлений в сфере информационных технологий, а также деятельность следственных и экспертно-криминалистических подразделений, осуществляющих их применение.

УДК 347.948.2
ББК 67.52
Л 22

Рецензенты:

А.Ш. Габдрахманов, начальник кафедры криминалистики Казанского юридического института МВД России, кандидат юридических наук, доцент
Е.Н Федорова, начальник 4-ого отдела ГСУ ГУ МВД России по Санкт-Петербургу и Ленинградской области

ISBN: 978-5-91837-707-9

Оглавление

ВВЕДЕНИЕ

Современное общество уже сложно представить без информационно-телекоммуникационных технологий, которые представляют собой совокупность методов, производственных процессов, программно-технических и лингвистических средств, интегрируемых с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах ее пользователей[1].

Масштаб проникновения в процессы жизнедеятельности указанного понятия является впечатляющим, и, в первую очередь, это связано с его транснациональным характером.

Одновременно с формированием общественных отношений, возникающих в сфере информационно-телекоммуникационных технологий, развитие получили и преступления, совершаемые с использованием данных технологий, способы совершения которых имеют тенденцию к своему совершенствованию и видоизменению.

Задействованы в таких схемах глобальные сервисы информационного развития. Возможность конспирации и обезличивания абонентов, подмены номеров телефонов, а также совершения преступлений дистанционно, осуществления действий связанных с сокрытием следов его совершения, очень сильно привлекло внимание правонарушителей и предоставила преступной среде огромные масштабы своего развития.

Согласно официальной статистике главного информационно-аналитического центра МВД России (ГИАЦ) о состоянии преступности в России, в январе – декабре 2021 года зарегистрировано 517,7 тыс. преступлений, совершенных с использованием информационно – телекоммуникационных технологий или в сфере компьютерной информации,

[1]Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. — М.: Институт развития информационного общества, 2009. — С. 61.

что на 1,4% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 25,0% в январе – декабре 2020 года до 25,8%[2].

Учитывая тенденцию к увеличению преступных посягательств, указанные преступления привлекают к себе внимание общественности и нуждаются в выработке алгоритмов, способных оказывать им достойное противодействие.

Для достижения поставленной цели, в настоящей работе усилия направлены на решение следующих задач:

1) раскрыть понятие и способы совершения преступлений с использованием информационно-коммуникационных технологий;

2) проанализировать проблемные вопросы, возникающие в ходе расследования преступлений, совершенных с использованием информационно-коммуникационных технологий;

3) сформировать алгоритмы расследования преступлений, совершенных с использованием информационно-коммуникационных технологий, на примере проведения основных следственных действий.

[2] Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2021 года // МВД России [Электронный ресурс] // URL: https://мвд.рф/reports/item/28021552/ (дата обращения: 05.01.2022).

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Информационно-телекоммуникационные технологии – это совокупность методов и средств передачи различной информации, материальную основу которых составляют наземные, сотовые, волоконно-оптические линии связи, а также спутники, представляющие из себя самостоятельные, но дополняющие друг друга информационно-телекоммуникационные системы.

Информационно-телекоммуникационные системы используются в различных отраслях хозяйства и сферах социальной деятельности для обмена информацией, включая телефонную сеть общего пользования, специальную и правительственную связь, электронную почту, телетекст, телефакс, доступ к удаленным базам данных, интеграцию национальной сети связи с мировой, а также телекоммуникационное обеспечение задач мониторинга экологической и дорожно-транспортной обстановки. Особенно важное значение информационная инфраструктура имеет для управления экономикой в связи с необходимостью оперативного реагирования на изменения ситуации в производственной и финансовой областях.

Преступления в сфере информационно-телекоммуникационных технологий — это предусмотренные уголовным законом общественно опасные деяния, причиняющие вред и (или) создающие опасность причинения вреда безопасности производства, хранения, использования либо распространения информации или информационных ресурсов. В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере информационно-телекоммуникационных технологий понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Любой обыватель в современном мире без труда самостоятельно отнесет к рассматриваемой категории преступлений такие преступления, как преступления, направленные на неправомерный доступ к компьютерной информации – взлом и (или) неправомерное получение паролей, личных конфиденциальных данных; распространение вредоносных компьютерных программ, направленных на уничтожение, блокирование, копирование, модификацию компьютерной информации, нейтрализацию средств защиты указанной информации;[3] хищение и подмена банковских реквизитов, включая сведений банковских карт, счетов; распространение противоправной информации – клевета, материалы возбуждающие межнациональную и межрелигиозную вражду и прочее через сеть «Интернет», а также вредоносное вмешательство через компьютерные сети в работу различных систем.

При этом в подавляющем большинстве, преступления, совершаемые в рассматриваемой сфере, несут корыстный характер и направлены на преступное получение выгоды.

Ответственность за совершение рассматриваемых преступлений предусмотрена особенной частью Уголовного законодательства Российской Федерации. При этом законодательно – главой 28 Уголовного кодекса Российской Федерации (далее – УК РФ) закреплены преступления в сфере компьютерной информации к которым относится:

– неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

– создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и распространение порнографии (ст. 274 УК РФ).

[3] Левин, Л. М. Киберпреступность как новое направление психологических исследований / Л. М. Левин // IV Международный пенитенциарный форум "Преступление, наказание, исправление" : Сборник тезисов выступлений и докладов участников, к 140-летию уголовно-исполнительной системы России и 85-летию Академии ФСИН России, в 10 т., Рязань, 20–22 ноября 2019 года. – Рязань: Академия ФСИН России, 2019. – С. 364.

Общественная опасность отнесенных в отдельную группу преступлений предусмотренных главой 28 УК РФ выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьёзное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные как с материальный ущербом, так и с физическим вредом людям.

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ), а также создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) совершаются только путём действий, в то время как нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) – путём как действий, так и бездействием.

При этом в современных реалиях жизни повсеместный характер носят хищения, связанные с различными способами обмана граждан. Указанные преступления законодательно закреплены главой 21 УК РФ и относятся к преступлениям против собственности.

В отличии от 28 главы УК РФ, преступления закрепленные в 21 главе УК РФ являются наиболее распространёнными и занимают до 87 % от всех преступлений, совершенных в сфере информационно-телекоммуникационных технологий.

Так преступники, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронными платежами денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации (к примеру, в связи с необходимостью освобождения от уголовной ответственности). Нередко злоумышленники сами представляются сотрудниками органа правопорядка[4], сотрудниками банковских кредитных

[4] Какие опасности подстригают доверчивых граждан в интернете // city-n. [Электронный ресурс] // URL:

учреждений и под предлогом защиты денежных средств, размещённых на банковских счетах, вынуждают доверчивых граждан предоставить доступ к указанным счетам с последующим совершением хищения.

Хищение денежных средств также возможно путем неправомерного списания их с банковских счетов граждан при банальной ситуации – когда в руки преступников попадают мобильные телефоны потерпевших, с установленными на них сервисами банков и кредитных учреждений (например, «Сбербанк онлайн»). Аналогичная ситуация и с банковскими картами, когда злоумышленники, заполучив банковскую карту или ее идентификационные данные совершают хищение бесконтактным способом – путем онлайн покупок, покупок посредствам терминалов оплаты, а при наличии пароля доступа – PIN-кода – деньги снимаются в банкоматах.

Велика доля хищений дистанционного характера посредством размещения на открытых интернет ресурсах сети «Интернет» заведомо ложных («фейковых») объявлений о предоставлении услуг и продаже товаров за денежное вознаграждение, которое в дальнейшем перечисляется на банковские счета злоумышленников.

Различные интернет ресурсы в том числе под видом ресурсов государственных учреждений, банковских организаций используются как платформы распространения вредоносных компьютерных программ. Переход пользователя по ссылке как правило приводит к инсталлированию вредоносной программы на устройство пользователя после чего злоумышленник получает удаленный доступ с возможностью управления мобильным устройством в том числе путем осуществления перечисления денежных средств посредствам абонентских номеров, установленных сервисов банков и кредитных учреждений. Указанная техника остается эффективной, поскольку многие пользователи, не раздумывая кликают по любым вложениям или ссылкам. Особенно это актуально в связи с глобальной цифровизацией общества, которая затрагивает и социально уязвимые слои населения – пожилых людей,

---

https://www.city-n.ru/view/449610.html (дата обращения: 09.01.2022).

испытывающих сложности при освоении современной техники, а также страдающих излишней доверчивостью.

В целях пресечения указанных видов преступлений, которые в общем объеме преступлений носят подавляющее большинство, наиболее эффективным методом является повсеместная пропаганда об их видах, способах обмана, используемых злоумышленниками.

Практика показывает, что наиболее популярным способом хищения денежных средств граждан, с использованием информационно – телекоммуникационных технологий, на сегодняшний день, является неправомерный доступ к их расчетным банковским счетам.

Основным объектом преступления данного вида выступают общественные отношения, связанные с отношениями собственности, независимо от ее формы. Особенностью компьютерной информации считается ее относительная простота и быстрота в пересылке, то есть за доли секунд компьютерная информация может достичь своего адресата, находящегося на другом конце света. В примечании 1 к ст. 272 УК РФ указывается, что под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. У информации нет собственника, но имеется обладатель, поэтому информация, имея стоимость, не является имуществом, понимаемым как совокупность вещей[5].

В соответствии с диспозицией ч. 1 ст. 272 УК РФ, данное преступление представляет хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

---

[5] Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. No 2. - С. 74.

Не смотря на указанное, стоит акцентировать внимание на то, что данный вид хищения является мошенничеством, который вне зависимости от разновидности (ст. 159 – 159.6 УК РФ) включает в себя два разных способа совершения, а именно:

1) Обман, который определяется как ложное утверждение о том, что не соответствует действительности.

2) Злоупотребление доверием, при котором виновный использует определенные отношения, основанные на доверии сторон для получения от потерпевшего денег или иного имущества под условием выполнения заведомо не выполнимых или впоследствии не выполненных обязательств.

Злоупотребление доверием взаимосвязано с обманом, так как злоумышленник использует особые доверительные отношения, установившиеся между ним и собственником или иным законным владельцем, чтобы обман был более убедительным, либо прибегает к обману, чтобы заручиться доверием потерпевшего.

При совершении преступления, предусмотренного ст. 159.6 УК РФ злоумышленник, используя один (или несколько) способов, указанных в диспозиции рассматриваемой статьи, фактически выдает себя за собственника денежных средств, находящихся на счету потерпевшего, и без его ведома, а также согласия, обращает данные средства в свою пользу. Следует отметить, что при совершении данного мошенничества непосредственного контакта потерпевшего с обвиняемым не происходит.

Удаление компьютерной информации по аналогии с уничтожением компьютерной информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Следует отметить, что удаление и уничтожение (ст. 274 УК РФ) это понятия, наполненные разным содержанием. Удаление по смыслу ст. 159.6 УК РФ это, прежде всего один из способов совершения преступления, из реализации которого образуются негативные для информации последствия. При этом удаленная информация может быть восстановлена по инициативе ее

законного владельца (потерпевшего) или злоумышленника. Уничтожение информации, по смыслу ст. 274 УК РФ – это последствия, которые явились результатом совершения данного преступления. Кроме того, уничтожение – это процесс необратимый. Восстановление информации в этом случае невозможно. В случае применения определённой компьютерной программы к конкретной электронной информации происходит ее блокирование, в результате чего, становится невозможным осуществлять какие-либо действия в течение определенного времени или постоянно, то есть происходит ограничение или закрытие доступа к выполнению законным пользователем всевозможных операций. Но такое блокирование не является способом или причиной дальнейшего уничтожения информации.

Модификация компьютерной информации – это внесение изменений в компьютерную информацию (или ее параметры)[6]. Под иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей можно понимать другие различные способы воздействия на компьютерную информацию, с помощью которых совершаются хищения денежных средств.

Например, копирование информации на другой носитель, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме – от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации[7].

В теории уголовного права выделяют и другие способы (приемы) мошенничества в сфере компьютерной информации: незаконное завладение регистрационными данными учетных записей; использование платежных сервисов Интернет-ресурсов; взлом электронных кошельков; организация

---

[6] Белоус В.Г., Грацкая Н.С. Проблема классификации хищений с использованием компьютерных технологий /В.Г. Беловус, Н.С. Грацкая // Актуальные вопросы образования и науки. 2016. No 1-2 (53-54). - С. 50.

[7] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» // Гарант [Электронный ресурс] // URL: https://base.garant.ru/70642118/ (дата обращения: 09.01.2022).

благотворительных акций через Интернет, где на банковский счет предлагается перечислять денежные средства,[8] внесение грубой подделки банкноты в банкомат. Хищение может совершаться со счетов граждан, привязанных и непривязанных к банковским картам. Очень часто с целью хищения денежных средств со счетов клиентов банков преступники создают и распространяют вредоносные программы. Таким образом, виновные лица могут получить информацию о ключах доступа к банковским системам управления счетами клиентов, а также возможность дистанционного управления ими.

Легальное определение электронных средств платежа содержится в п. 19 ст. 3 Федерального закона от 27 июня 2011 г. N 161-ФЗ «О национальной платёжной системе», согласно которому это средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения 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.

Результатом внесения законодательных изменений стали проблемы, с которыми столкнулись правоохранительные органы при отграничении различных составов преступлений связанных с хищением чужого имущества совершенных тем или иным способом, при котором использовались современные технологии, а именно деяния, предусмотренные п. "г" ч. 3 ст. 158 УК РФ, ст. 159 УК РФ, ст. 159.3 УК РФ, ст. 159.6 УК РФ.

Выбор преступником способа хищения денежных средств с банковских счетов граждан, зависит от профессиональных навыков преступников, наличия

[8] Коломинов В.В. О способе совершения мошенничества в сфере компьютерной информации / В.В. Коломинов // Человек: преступление и наказание. - 2015. - № 3. - С. 146.

специальных средств для совершения преступления, что в дальнейшем определяет уровень общественной опасности[9].

Для того чтобы понимать природу рассматриваемых преступлений, необходимо изучить личности лиц в них вовлечённых – личность преступника – злоумышленника и потерпевшего – жертвы.

Как показала практика для совершения преступлений в сфере информационно-телекоммуникационных технологий преступник должен обладать высоким уровнем образования в указанной сфере, обусловлено это тем, что современная компьютерная техника обладает высокой степенью сложности, а также средствами защиты. При этом в данном контексте не всегда выступает наличие у лица «диплома» об окончании учебных заведений. Наиболее важным для преступника является практический опыт, который может быть получен и в ходе самостоятельного изучения информационно-телекоммуникационных технологий.

Так лица, создающие вредоносные программы, скорее всего являются специалистами в области программирования, системного администрирования, автоматизированных систем, которые используются в деятельности определенных отраслей, в частности, банковской.

Исходя из сложившейся следственной практики, на основе анализа изученных уголовных дел можно сделать вывод, что указанные виды преступлений, как правило, совершаются группой лиц, так как из-за сложности механизма их совершения и мероприятий связанных с конспирацией преступных деяний, совершать их в одиночку достаточно сложно. Данные преступные группы создаются заблаговременно до совершения преступления, в нее входят только проверенные временем лица. Часто объединяются для совершения указанных преступлений знакомые, не имеющие отрицательных характеристик в кругу своего общения (то есть никогда не предававшие, всегда выполняющие просьбы, умеющие молчать и хранить тайны и т.д.). В группе

существует четкая специализация участников: в зависимости от распределения преступных ролей каждым выполняются строго свои обязанности. Они объединены между собой единой целью, с четкой системой конспирации и защиты от разоблачения правоохранительными органами. Каждому участнику определена обязанность со строгим подчинением руководителю, при этом особенностью таких преступных групп является то, что их члены, выполняя конкретные функции, могут быть незнакомы друг с другом, или знакомы только с кем-то из других участников.

Механизм совершения хищений определяется распределением ролей участников в преступной группе, которых можно разделить на виды:

- Организатор.
- Лица, занимающиеся распространением вредоносных программ.
- Лица, занимающиеся выводом денег с взломанных счетов, так называемые «заливщики».
- Участники «дроп-проекта», предназначенного для обналичивания похищенных денежных средств. Это «псевдокомпания», которая может заниматься чем угодно: продажами, перевозками и т.д. В его состав входят руководитель дроп-проекта, «дроповоды», «дропы».
- При возникновении необходимости создания вредоносной программы в состав преступной группы также может входить их разработчик или разработчики.

В отличии от преступника личность потерпевшего не носит какие-либо определенные черты, так как потерпевшим может выступать как физическое, так и юридическое лицо, в том числе государственные органы и государство в целом.

Потерпевшими от указанных преступлений как правило выступают лица, имеющие денежные средства на счетах в банках, иных организациях, также держателями различных видов пластиковых карт, осуществляющие пользование электронными платежными системами.

В зависимости от вида совершенного преступления и используемых средств злоумышленником потерпевшим могут выступать как лица, вовлеченные в процесс интеграции компьютерной информации, так и лица, не участвующие в данном процессе – прежде всего это пожилые лица.

При этом дать точные возрастные и иные характеристики как преступника, так и потерпевшего не представляется возможным в связи с глобальным процессом информатизации общества.

Преступления рассматриваемой категории происходят в специфической среде — виртуальном кибернетическом пространстве, где в одном преступлении одновременно могут быть задействованы множество территориально удаленных друг от друга компьютеров. Каждое из мест нахождения электронного устройства имеет свою обстановку. Для характеристики времени совершения преступления используется астрономическое время, то есть определенная временная точка и продолжительность осуществления способа посягательства от его начала до окончания в виде наступления общественно опасных последствий[10].

Судебно-следственная практика показала, что в большинстве случаев преступники самостоятельно создают условия совершения преступления. Так, могут создаваться компьютерные вирусы и специальные программы взлома, направленные на снижение уровня защиты. Обстановка является динамичной категорией.

Местом совершения преступления и подготовки к его совершению могут являться места временного нахождения преступника, для этого они как правила арендуют съемные помещения, где пребывают недолгое время. Через недолгие промежуток времени, преступники место своего пребывания меняют, чтобы их не могли установить. Для совершения хищений, используются различные технические средства, такие как ноутбуки, планшеты, компьютеры, имеющие возможность выхода в сеть «Интернет». Чаще всего это не

[10] Соколов, А. С. Особенности расследования преступлений в сфере компьютерной информации / А. С. Соколов, А. А. Погосян // Аллея науки. – 2018. – Т. 2. – № 7(23). – С. 334.

стационарные компьютеры, а удобные в переносе, портативные средства, которые можно будет быстро собрать и вынести из помещения, в случае предположения о том, что они были зафиксированы правоохранительными органами. Кроме того, для осуществления незаконного внедрения в банковское программное обеспечение приобретают вирусные программы, для хищения денежных средств граждан через банкоматы приобретаются скимминговое оборудование.

Наиболее сложным в расследовании способом совершения указанных преступлений является хищение[11] денежных средств в системе дистанционного банковского обслуживания, установленной на компьютерном устройстве потерпевшего. В настоящее время очень развита такая система дистанционного банковского обслуживания[12] как «Мобильный банк» (например, «Сбербанк-Онлайн», «ВТБ-онлайн», «Home Credit bank» и др.), которые позволяют гражданам управлять своими денежными средствами в любом месте не посещая отделение банка. С помощью мобильных приложений, установленных на смартфоны, либо на компьютеры можно осуществлять платежи за коммунальные услуги, отправлять переводы физическим лицам, производить платежи по кредитам, оплачивать налоги, штрафы, открывать счета или вклады и многое другое. Практически большая часть населения Российской Федерации пользуется данными приложениями, которые созданы для удобства граждан, но и преступники используют созданные условия в своих корыстных целях. Они осуществляют рассылку на электронную почту граждан или смс-сообщения на номера мобильных телефонов, подключенных к мобильному банку с предложениями якобы от банка, например, предоставление кредита на выгодных условиях, или сообщением о подозрительных операциях по счету и в сообщении указывают ссылку, по которой необходимо перейти в личный кабинет для проверки или подтверждения указанной информации. В случае

[11] Брызгалов, Г. Е. Механизм преступления при хищении денежных средств, совершаемом с использованием вредоносных компьютерных программ / Г. Е. Брызгалов // Алтайский юридический вестник. – 2018. – № 3(23). – С. 103.

[12] Скогорева, Т. Ф. Процессуальные и организационно-тактические особенности расследования преступлений, связанных с хищением денежных средств, совершаемых с использованием компьютерных технологий / Т. Ф. Скогорева, Э. Ж. Чхвимиани // Современная научная мысль. – 2018. – № 3. – С. 197.

перехода по ссылке и введения пароля от личного кабинета, злоумышленники получают доступ к мобильному банку пользователя и осуществляют списание всех имеющихся на счету денежных средств.

Последующие этапы механизма совершения хищений – вывод денежных средств со счетов потерпевших и их последующее обналичивание, рассмотрены при описании функций участников преступной группы.

Время совершения хищения напрямую зависит от момента поступления денежных средств на счет потерпевшего. Обладая доступом к сведениям о состоянии счета, преступники дожидаются данного момента, после чего осуществляют вывод денег. В ряде случаев, если это крупная сумма, операции по выводу денежных средств преступники стараются проводить под конец рабочего дня банка, лишая возможности потерпевшего и банк оперативно заблокировать транзакцию.

Рассылку смс-сообщений с просьбой̆ о возврате денег или помощи якобы родственнику отправляют как правило рано утром или ночью, так как в это время человек обычно спит и не может в полной мере осознавать реальность происходящих событий, обдумать действия или сообразить позвонить своему знакомому или проверить баланс.

Как и любые преступления, рассматриваемая категория наделена специфичными «следами», присущими характеру и способу его совершения. Так следы преступления могут содержаться на компьютерах, ноутбуках, планшетах, смартфонах потерпевшего и могут быть представлены в виде вредоносных компьютерных программ, информации об отправке и получении SMS-сообщений и USSD-команд с технического устройства.

Подключение устройства преступника к информационно-телекоммуникационной сети «Интернет», образует следы об IP-адресе устройства, которые остаются на серверах, посредством которых осуществлялось подключение и работа. Сведения о банковских транзакциях фиксируются на банковском процессинговом сервере, в связи с чем, в случае совершения преступления следователь может получить всю необходимую

информацию в банке о счетах потерпевшего и дальнейшему движению денежных средств.

Основная часть доказательств в рассматриваемой категории преступлений содержится в компьютерной технике, носителях электронной информации (жесткие магнитные диски, компакт-диски, флеш-карты), а также документах, выполненных в бумажном виде. Поэтому при расследовании уголовных дел по настоящим преступлениям в первую очередь надо обращать внимание на указанные предметы, на них могут быть обнаружены следы преступной деятельности, указывающие на хищение денежных средств в сфере компьютерной информации.

Такие технические устройства как ноутбук, смартфон, планшетный компьютер содержат на себе массу доказательств, свидетельствующих о том, что именно злоумышленник пользовался устройством. При этом это не только следы в виде какой-либо специфической индивидуальной цифровой информации (дата рождения, фотографии, электронные подписи и т.п.), но и естественные следы такие как следы пальцев рук, микрочастицы, следы биологического происхождения и т.д.

При этом изученная литература показала, что к единому мнению относительно указанной категории исследователи не пришли до сих пор, поэтому в литературе можно встретить понятия «бинарные следы», «виртуальные следы». Так Вехов В.Б. предлагает понятие «электронно-цифровой след», под которым понимает любую криминалистически значимую компьютерную информацию, то есть сведения, находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе либо передающиеся по каналам связи посредством электромагнитных сигналов.

ГЛАВА 2. ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ХИЩЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

При совершении хищения денежных средств или иного имущества потерпевших, совершенных с использованием информационно-коммуникационных технологий, заявители могут обратиться в территориальные органы МВД России по телефону или лично в письменной форме, а также посредством «Интернет», путем направления электронного письма. При этом в большинстве случаев, потерпевшие не сразу обращаются с заявлением в органы внутренних дел о пропаже денежных средств с их счетов, так как пытаются самостоятельно выяснить, куда они делись, либо, осознавая, что сами по своей доверчивости перевели денежные средства преступникам, стесняются об этом сообщить, либо ждут какое-то время, надеясь, что им предоставят ту услугу или товар, за который они перевели денежные средства. Таким образом потерпевшие, сами того не осознавая, дают преступникам больше времени, для сокрытия следов своих преступлений.

После обращения потерпевшего с заявлением о произошедшем в отношении него неправомерном деянии, связанным с хищением принадлежащих ему денежных средств с банковского счета, орган дознания, следователь, в соответствии с нормами Уголовно-процессуального законодательства обязаны провести первоначальную проверку по установлении обстоятельств преступления.

Комплекс первоначальных мероприятий направленных на установление обстоятельств преступления, порядок их проведения, определяются исходя из конкретного преступления. Указанные мероприятия осуществляются исходя из объема и достоверности криминалистически значимой информации полученной на первоначальном этапе – сообщения о преступлении.

Для принятия процессуального решения о возбуждении уголовного дела по факту хищения, совершенного с использованием компьютерной информации, необходимо наличие достаточных оснований о признаках преступления и наличие материалов, содержащих информацию о хищении. Как

правило, поводами для возбуждения уголовного дела являются заявления и сообщения потерпевших, поданные в компетентный правоохранительный орган в любой форме; обнаруженные органами дознания или следователем признаки преступлений в результате расследования других преступлений, рассмотрения иных сообщений; достоверные сведения, полученных из средств массовой информации, а также сети «Интернет».

Так для принятия следователем законного и обоснованного решения по заявлению по факту хищения денежных средств с банковского счета, необходимо установление следующей информации:

- денежные средства списаны со счета потерпевшего неустановленным лицом, за услугу которая ему (потерпевшему) не оказывалась;
- денежные средства списаны со счета потерпевшего без его ведома;
- денежные средства перечислены самим потерпевшим за товар, который ему так и не был предоставлен;
- денежные средства переведены со счета потерпевшего на другой счет, без его согласия.

Перед возбуждением уголовного дела, орган дознания, следователь, проводит предварительную проверку по поступившему заявлению, по результатам которой принимает решение в соответствии с уголовно-процессуальным законодательством Российской Федерации (УПК РФ).

При наличии основании и достаточных данных для возбуждения уголовного дела, на основании собранных первоначальных материалов уполномоченное должностное лицо выносит постановление о возбуждении уголовного дела и определяет перечень оперативных мероприятий и следственных действий, направленных на раскрытие и расследование преступления.

Успешное расследование указанных преступлений, совершенных с использованием информационно-коммуникационных технологий зависит от оперативных действий следователя и сотрудника уголовного розыска (оперативного сотрудника) непосредственно после получения такой

информации, а также четко совместного организованного взаимодействия подразделений правоохранительных органов, при участии специалистов в области компьютерных технологий сторонних организаций (операторов сотовых сетей, провайдеров, служб безопасностей банков и т.п.).

В рамках полноты проведения доследственной проверки, и с целью соблюдения сроков, предусмотренных УПК РФ, обеспечения качества собранного материала должностным лицом формируется план (указания) в который включаются следующие мероприятия:

1) получение письменного объяснения от заявителя, в котором указываются обстоятельства совершения хищения денежных средств, то есть каким образом были списаны денежные средства, за какие услуги, на какие реквизиты, когда произошло событие с точным указанием даты и времени списания. Также выясняется, сообщал ли потерпевший кому-либо идентификационные реквизиты от своей банковской карты и CVC-код на ее обороте, кода из смс сообщения полученных от банка на номер его мобильного телефона.

К заявлению (объяснению) о совершении преступления необходимо истребовать от потерпевшего приобщения выписки из банка о движении денежных средств по счету за интересуемый период, так как в случае ее не предоставления, орган дознания или следователь может получить ее только через судебное решение и (или) запрос соответственно, а указанные промедления дадут возможность злоумышленнику скрыть или уничтожить следы преступления и его установление будет уже труднее.

2) провести осмотр места происшествия, изъятие интересующих предметов и документов. Согласно ст. 176 УПК РФ осмотр места происшествия возможно проводить как до возбуждения уголовного дела, так и в процессе расследования уголовного дела. В рамках осмотра места происшествия возможно изъятие мобильных телефонов (смартфонов), компьютер, планшетов, ноутбуков заявителя для проведения экспертизы, детального осмотра и приобщения к материалам уголовного дела в качестве вещественного

доказательства. Так документально необходимо оформить факт поступления и отправки сообщений разрешительного и уведомительного характера; зафиксировать наличие или отсутствие вредоносных программ;

3) осуществить опрос лиц, которые по предположению потерпевшего могут быть причастны к происшедшему, либо обладают значимой информацией по данному факту;

4) произвести выемку у потерпевшего сведений о соединениях по абонентскому номеру (если им осуществлялось общение с преступником с помощью мобильного телефона). Указанные сведения желательно, чтобы потерпевший предоставлял самостоятельно, так как его получение сотрудниками правоохранительных органов возможно только по судебному решению;

5) подготовить и направить запросы операторам связи на получение информации о принадлежности абонентских номеров, используемых злоумышленником; провайдерам на установление IP-адреса технического устройства с использованием которого осуществлялся выход злоумышленником в сеть «Интернет» (к примеру, если общение происходило в социальных сетях или на каких-либо интернет сайтах); отдельные поручения для производства оперативных мероприятий направленных на установление злоумышленника.

Перечень первоначальных мероприятий не является окончательным и может быть изменен или дополнен в зависимости от сложившейся ситуации и наличия информации о преступлении.

По результатам доследственной проверки материалов сотрудник органа предварительного расследования должен получить четкое и полное представление о характере деятельности и структуре объекта, где было совершено хищение денежных средств с использованием компьютерных технологий, о технических характеристиках используемой компьютерной техники и программного обеспечения.

Качественное проведение доследственной проверки по заявлению, сообщению и иной информации о хищении денежных средств или иного имущества гражданина с его банковского счета, совершенного с использованием информационно-коммуникационных технологий, а также собранная в полном объеме необходимая информация, позволяют следователю принять законное, обоснованное решение о возбуждении уголовного дела и применить правильную квалификацию деяниям злоумышленника.

Успешное расследование указанных преступлений, совершенных с использованием информационно-коммуникационных технологий зависит от оперативных действий следователя и сотрудника уголовного розыска непосредственно после получения такой информации, а также от четко организованного взаимодействия между службами и подразделениями правоохранительных органов, в том числе и со специалистами в области компьютерных технологий.

Для хищений, совершаемых с использованием информационно-коммуникационных технологий, на первоначальном этапе расследования, характерны следующие следственные ситуации:

1. Событие преступления известно, необходимо установить лицо его совершившее, и обстоятельства совершения преступления.

2. Событие преступления и лицо, его совершившее известно, необходимо установить все обстоятельства по расследуемому делу[13].

Именно от следственной ситуации зависит ход планирования расследования уголовного дела, которое состоит из нескольких этапов:

1) анализ полученной информации с выдвижением версий и установлением задач расследования;

[13] Решняк, О. А. Организация расследования мошенничеств, совершенных с использованием сети "Интернет", на первоначальном и последующем этапах / О. А. Решняк, С. А. Ковалев // Вестник Волгоградской академии МВД России. – 2020. – № 2(53). – С. 108.

2) составление письменного плана расследования уголовного дела, куда включены оперативно-следственные мероприятия и перечень необходимых следственных действий, направленных на отработку версий.

Согласно указанных этапов планирования расследования преступления, связанного с хищением, совершенным с использованием информационно-коммуникационных технологий уполномоченное должностное лицо правоохранительного органа изучает имеющуюся исходную информацию, анализирует ее, изучает данные о предмете преступления, способе хищения, личности потерпевшего, месте и времени совершения преступления.

При производстве расследования, подлежат доказыванию следующие обстоятельства:

1. Событие преступления (время, место, способ совершения преступления);
2. Виновность лица в совершении преступления, форма его вины и мотивы;
3. Обстоятельства, характеризующие личность обвиняемого;
4. Характер и размер вреда, причиненного потерпевшему;
5. Обстоятельства, исключающие преступность и наказуемость деяния;
6. Обстоятельства, смягчающие и отягчающие наказание;
7. Обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания;
8. Обстоятельства, подтверждающие, что имущество, подлежащее конфискации в соответствии со статьёй 104.1 Уголовного кодекса Российской Федерации, получено в результате совершения преступления или является доходами от этого имущества либо использовалось или предназначалось для использования в качестве орудия, оборудования или иного средства совершения преступления либо для финансирования терроризма, экстремистской деятельности (экстремизма), организованной

группы, незаконного вооруженного формирования, преступного сообщества (преступной организации).

9. Обстоятельства, способствовавшие совершению преступления[14].

Следующий этап планирования заключается в определении способов проверки выдвинутых следственных версий.

На данном этапе уполномоченное должностное лицо планирует мероприятия и алгоритм проведения необходимых следственных и процессуальных действий оперативно-розыскных мероприятий по уголовному делу для решения поставленных задач.

Перечень следственных, процессуальных, оперативно-розыскных мероприятий, не имеет определенной структуры и состава и может меняться в зависимости от обстоятельств и сложившихся следственных ситуаций.

На основе изученной следственной практики, по рассматриваемой тематике, можно привести примерный перечень оперативно-розыскных мероприятий и следственных действий, проводимых на первоначальном этапе расследования:

1. допрос потерпевшего или его представителя, допрос свидетелей;

2. производство выемки, осмотр и приобщение в качестве доказательств документов, содержащих охраняемую законом тайну, в том числе документов, отражающих принадлежность платёжной карты конкретному лицу, выписки по счетам физических и юридических лиц, которые фигурируют в уголовном деле;

3. изъятие у потерпевшего и осмотр технического устройства, с которого им осуществлялась переписка с злоумышленником, а также перевод денежных средств, если на данном устройстве установлены приложения дистанционного банковского обслуживания;

[14] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 No 174- ФЗ (ред. от 17.04.2017) (с изм. и доп., вступ. в силу с 01.06.2017). (Дата обращения 05.06.2022).

4. подготовка и направление запросов в банки для установления принадлежности счетов на, которые были осуществлены переводы денежных средств со счета потерпевшего;

5. выемка в банке выписки по счетам лиц, на которые были осуществлены переводы денежных средств, фигурирующие в рамках уголовного дела;

6. осмотр полученных выписок банка по счетам лиц фигурирующих в рамках уголовного дела;

7. выемка видеозаписей с видеокамер банкомата, в котором были обналичены похищенные денежные средства и осмотр указанных видеозаписей;

8. подготовка и направление запросов в доменную компанию на установление IP-адреса технического устройства, с которого осуществлялся выход в сеть «Интернет» во время общения с потерпевшим;

9. подготовка и направление запроса провайдеру, которому принадлежит установленные IP-адреса, с целью получения данных пользователя;

10. проведение обыска, с участием соответствующих специалистов, по месту регистрации либо фактического проживания лиц, причастных к хищению;

11. допрос подозреваемого, обвиняемого.

При этом с целью визуализации необходимых следственных действий и оперативно-розыскных мероприятий, по уголовным делам указанной категории необходимы разработка и составление схемы движения безналичных денежных средств.

В плане проверки выдвинутых версий для каждого запланированного мероприятия следователем должен быть определен срок его исполнения. Это необходимо делать для того, чтобы было легче отследить ход расследования уголовного дела, и проконтролировать исполнение плана.

При расследовании уголовных дел, связанных с хищением, совершенным с использованием информационно-коммуникационных технологий, не следует пренебрегать помощью иных служб и подразделений, а также пользоваться помощью иных организаций. Так основная информация, на первоначальном этапе расследования может быть получена от банков и иных кредитных и провайдерских организаций, платежных систем. Такая информация может дать направление раскрытию и расследования преступления.

С целью обеспечения полного и качественного расследования руководителю правоохранительного органа следует проводить служебные совещания совместно со следственными подразделениями и оперативными подразделениями, в ходе которых, обсуждать наиболее важные и проблемные вопросы, с целью их решения.

ГЛАВА 3. ТАКТИКА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

Основополагающим элементом сбора доказательственной базы по уголовным делам, а также материалам доследственной проверки рассматриваемой категории преступлений является своевременное, полное и объективное получение «следов» преступления на непосредственных носителях информации, которыми могут выступать как стационарные электронно-вычислительные машины, включающие – персональные компьютеры, ноутбуки, блоки серверов и иное сетевое оборудование; носимые «гаджеты», такие как смартфоны, «умные часы», электронные планшеты, а также источники информации на бумажных носителях содержащие сведения печатного и рукописного характера.

Указанные средства и оборудование в современном мире позволяют получать доступ к информационно-телекоммуникационной сети «Интернет», сетям операторов стационарных и подвижных систем связи (сотовой, спутниковой). Однако не смотря на весь прогресс в информационном пространстве, значительную долю информации до настоящего момента в себе могут содержать бумажные носители.

Основополагающими и дополняющими друг друга в комплексе сбора доказательств по рассматриваемой категории преступлений являются такие следственные действия как обыск, выемка, осмотр.

При этом стоит особо подчеркнуть, что по преступлениям, совершаемым в сфере информационно-телекоммуникационных технологиях, основная часть доказательств содержится на электронных носителях. В настоящее время уголовно-процессуальным законодательством Российской Федерации (статьи 144, 176 УПК РФ), закреплено право уполномоченных должностных лиц на частичное производство одного из указанных следственных действий – осмотра в части проведения осмотра места происшествия, документов, предметов, при проведении первоначальной проверки по сообщениям о преступлении.

Согласно статье 176 УПК РФ осмотр места происшествия, предметов и документов производится в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела.

Исходя из указанной нормы права, тактика проведения указанного следственного действия, прежде всего направлена на сбор, фиксацию первоначальных сведений и следов преступления, которые фиксируются уполномоченными должностными лицами в первую очередь при поступлении и регистрации сведений о совершенном преступлении и как правило при участии лица в отношении которого совершено преступление.

При этом осмотр документов, предметов в большей степени является продолжением таких следственных действий как выемка, обыск, осмотр места происшествия, при проведении которых зачастую в силу продолжительности и значительного объема изъятого имущества и документов, не в полной мере возможно получить всю хранимую информацию.

По рассматриваемым преступлениям, в зависимости от характера совершенного преступления следует выделить два основных места «происшествия», которыми являются:

- местонахождение стационарных точек связи, в том числе домашних телефонов, персональных компьютеров, планшетов, смартфонов, ноутбуков, используемых заявителем (потерпевшим). При этом таким местом как правило будет выступать жилье заявителя, его рабочее место, либо территориальное расположение на момент осуществления контакта заявителя с злоумышленником;
- место осуществления заявителем (потерпевшим) безналичных денежных переводов, которым чаще всего выступают банкоматы, платежные терминалы, офисы банковских и кредитных учреждений, почтовые отделения.

При осуществлении осмотра мест происшествия в первом случае следственная практика показала, что по рассматриваемой категории преступлений значительный объем информации, которая в последующем

может быть использована в качестве доказательств содержится в зависимости от способа преступления в «носители» информации используемом заявителем которым может выступать как электронное устройство, так и бумажные носители. При проведении осмотра места происшествия необходимо не только зафиксировать средства связи, ЭВМ, которые выступили средством коммуникации между потерпевшим и злоумышленником, но и произвести изъятие данного средства связи – смартфона, компьютера, планшета, ноутбука и т.п. используемого заявителем для последующего проведения осмотра предмета с участием специалиста, назначения и проведения экспертизы, с целью обнаружения информации способствовавшей совершению преступления (сведения о интернет ресурсах, дате времени получения сообщений, звонков, истории интернет мессенджеров, наличие вредоносных программ и т.п.). При этом в ходе осмотра в протоколе следственного действия следует в обязательном порядке отразить индивидуальные признаки изымаемых предметов такие как: IMEI-номер устройства, сведения о количестве и идентификационных номерах сим-карт, сведения о абонентских номерах, данные о поступивших и исходящих звонках, сообщениях (дате, содержании, номере абонентского устройства, с которого поступило каждое сообщение), данные о входящих (исходящих) телефонных звонках (дате, времени, продолжительности соединений) иные идентификационные данные и обозначения.

Конституционным Судом Российской Федерации в определении от 25 января 2018 г. № 189-0 «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации» указано, что проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения.

Полученную в ходе осмотра абонентского или иного устройства информацию можно изначально скопировать (с целью приобщения к материалам уголовного дела) путём снятия скриншота, составления фототаблицы.

До настоящего момента в значительных случаях при контакте со злоумышленником потерпевшие продолжают использовать бумажные носители в качестве средства фиксации и как следует хранения информации предоставляемой злоумышленником (к примеру информации, о абонентских номерах, банковских счетах, адресах, данных о личности и т.п.). В связи с чем при проведении осмотра уполномоченное должностное лицо фиксирует текст, содержащийся на бумажные носители в протоколе и изымает указанный бумажный носитель, используемый фактически как вещественное доказательство и подтверждающий показания потерпевшей стороны.

Так примером проведения осмотра места происшествия с участием заявителя «К» по уголовному делу № 1210187*****0486 (по факту совершения мошенничества, под предлогом продажи автомобиля через сайт «Авито»), следует отметить, что следователем на момент проведения проверки по заявлению «К» в квартире по месту жительства заявителя был обнаружен и осмотрен ноутбук «Acer» s/n **********, в котором была осмотрена история интернет браузера «Yandex», в ходе которого была восстановлена переписка на интернет ресурсе «www.Avito.ru. В указанной переписке злоумышленник при продаже товара – автомобиля марки «Лексус 570» стоимостью 850 000 рублей среди 5 банковских карт, используемых для перевода заявителем с целью покупки машины денежных средств, указал номер банковской карты, оформленной на мать, с которой он проживал в момент совершения преступления. Зафиксированная в должном порядке информация с указанием дословного содержания в протоколе обнаруженной переписки позволила в кратчайшие сроки установить владельцев банковских карт, на которые был осуществлен денежный перевод, получить оперативным сотрудникам видеозаписи с камер 3-х банкоматов, используемых злоумышленником при

снятии денежных средств, идентифицировать личность злоумышленника и адрес его местонахождения.

Точная и полная фиксация в протоколе вышеуказанной информации необходимо прежде всего в связи с тем, что заявитель не всегда может в точности и в полном объеме отразить детали совершенного в отношении него преступления, в том числе указать точные даты, время, а также сведения и информацию которые позволят установить злоумышленника такие как сведения о абонентских номерах, банковских реквизитах и т.п.

Вторым обозначенным местом происшествия по рассматриваемой категории преступлений является место осуществления заявителем (потерпевшим) безналичных денежных переводов.

Проведения осмотров банкоматов, терминалов оплаты, офисов банков и кредитных организаций, почтовых отделений является немаловажным источником получения доказательств по уголовному делу. Так должностному лицу следует зафиксировать полные идентификационные данные устройства обслуживания, его точное местонахождение, обратить внимание на наличие средств аудио и видео фиксации. Указанная информация в последующем может способствовать восстановлению «картины» совершенного преступления в том числе установлению сведений способствующих идентификации злоумышленников.

Следственная практика показала, что после установления идентификационного номера устройства самообслуживания (банкомата, терминала оплаты и т.п.), возможного периода проведения операций потерпевшим, номера банковской карты, используемой в качестве электронного средства платежа, в порядке, предусмотренном ч. 4 ст. 21 УПК РФ и ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности», с согласия руководителя следственного органа возможно направить запрос в банк (кредитную организацию) на предоставление копии электронного журнала указанного устройства, что позволит точно установить, какие именно манипуляции (банковские операции)

совершил потерпевший с использованием указанного устройства самообслуживания, точное время проведения и вид операции.

В значительном количестве случаев злоумышленник путём обмана потерпевшего побуждает последнего совершить такие манипуляции с использованием платёжной карты и устройства самообслуживания:

- подключить абонентский номер телефона злоумышленника (в качестве дополнительного номера) к приложению «Мобильный банк», тем самым преступник получает возможность осуществлять операции по переводу денежных средств со счёта (банковской карты) потерпевшего путём отправления текстовых СМС- сообщений;
- перерегистрировать «личный кабинет» в системе по дистанционному банковскому обслуживанию;
- осуществить перевод денежных средств со счёта (банковской карты) потерпевшего на счёт либо электронное средство платежа преступника.

Так примером проведения осмотра места происшествия с участием заявителя «Ж» по уголовному делу № 1200187*****1313 (по факту мошенничества – под предлогом звонка от сотрудника банка с целью защиты денежных средств на банковских счетах), следует отметить, что следователем в рамках возбуждённого уголовного дела совместно с потерпевшим «Ж» был осуществлён выезд по месту нахождения платёжного терминала № ***** ПАО «Сбербанк России» по адресу Республика Коми, г. Сыктывкар, ул. Карла Маркса д. 114. В ходе проводимого осмотра терминала, указанного потерпевшим, был установлен его идентификационный номер, в мусорном ведре обнаружены распечатки (чеки) работы терминала о смене абонентского номера подключенной услуги мобильный банк, на которых был указан новый номер, используемый при работе с «Мобильным банком». Указанная информация позволила в кратчайшие сроки в порядке ст. 186.1 УПК РФ получить сведения о соединениях по абонентским устройствам, базовых станциях и принадлежности абонентского номера и как следствие лица совершившего преступление. Кроме того, благодаря полученному

электронному журналу работы устройства по запросу правоохранительных органов, были установлены точные суммы похищенных денежных средств, сведения о счетах, используемых при хищении.

Таким образом уже на первоначальной стадии проведения проверки в порядке ст. 144 УПК РФ, сотрудники правоохранительных органов при должном своевременном и качественном проведении осмотра места происшествия могут получить значительный объем информации и доказательств, необходимых для установления обстоятельств совершенного преступления (даты, времени, способа), подтверждения показаний заявителя (потерпевшего), установления круга лиц причастного к совершению преступления, размеров причиненного ущерба.

В соответствии со статьей 177 УПК РФ осмотр следов преступления и иных обнаруженных предметов производится на месте производства следственного действия, за исключением случаев, когда для производства такого осмотра требуется продолжительное время или осмотр на месте затруднен, то предметы должны быть изъяты, упакованы, опечатаны, заверены подписью следователя на месте осмотра.

Зачастую, как было указано, не в полном объеме возможно при проведении осмотра места происшествия и тем более обыска, выемки получить всю значимую информацию с изъятых носителей информации – предметов и документов. Указанное обстоятельство обусловлено и тем фактом что в ходе расследования уголовного дела по исследуемому направлению значительную часть занимает анализ полученной информации от компетентных органов – банков, кредитных учреждений, операторов сотовой связи, интернет провайдеров и иных организаций. Анализ полученных от указанных органов сведений сопоставление их с показаниями лиц, полученных в ходе расследования уголовного дела, а также с изъятыми предметами и документами является следующей ступенью получения и закрепления доказательств по уголовному делу.

В качестве доказательств электронные и бумажные носители информации используются при расследовании значительного количества преступлений. Получение и использование информации, содержащейся на электронных и бумажных носителях, по уголовным делам является одной из основных и трудно решаемых на практике задач, требующей как правило наличия специальных познаний в области компьютерной техники и программного обеспечения.

Значительный объем материалов уголовного дела по рассматриваемой тематике, занимают осмотры предметов и документов, изъятых при проведении иных следственных действий и полученных на основании запросов.

В настоящее время процесс проведения и протоколирования осмотра предметов и документов уголовно-процессуальным законодательством облегчен путем возможности применения фото-видео фиксации, без участия посторонних лиц – понятых, согласно ст. 170 УПК РФ. Стоит отметить что зачастую участие незаинтересованных лиц – понятых могло привести как к затягиванию самого осмотра, так и к «утечки» значимой информации, а также методов и способов ее получения, сведений о используемом правоохранительными органами оборудовании.

Изучение материалов уголовных дел показало, что значительный объем доказательств содержится в изъятых у злоумышленников предметах и документах.

Так примером проведения осмотров предметов по уголовному делу № 1200187*****1313 (по факту мошенничества – под предлогом звонка сотрудника банка с целью защиты денежных средств на банковских счетах), следует отметить, что следователем в рамках возбуждённого уголовного дела после проведенных обысков осмотрен мобильный телефон, изъятый по месту жительства подозреваемого «У» с сим-картой, находящиеся в пользовании подозреваемого, личные рукописные записи, содержащиеся в блокноте, распечатки банков с номерами банковских карт, оформленных на сторонних лиц. Указанные предметы и документы проанализированы и осмотрены,

содержимое внутренней памяти телефона специалистом – экспертом отдела ЭКЦ участвующим в осмотре выгружено и сохранено на отдельный оптический диск, с указанием на значимую информацию – смс-сообщения, контакты, личные фотографии подозреваемого, мест его пребывания в различных населенных пунктах Кировской области в которых осуществлялось последующее обналичивание похищенных денежных средств, что полностью совпадало при сопоставлении с ответами банков полученных по уголовному делу. Восстановлены переписки в интернет мессенджерах подозреваемого с иными лицами причастными к совершению преступления. В блокноте при осмотре были обнаружены рукописные сведения о иных потерпевших с указанием города и данных о имени отчестве, примерный сценарий телефонного разговора, сведения о часовых поясах в городах потерпевших.

Указанный пример осмотра также показал, что если при осмотре бумажных носителей трудностей фиксации и сопоставления информации не возникает, то при осмотре мобильного устройства существует ряд специфических действий, которые необходимо выполнить для извлечения данных из таких электронных носителей информации, а именно осмотр начинают с определения состояния мобильного устройства, а именно заряда аккумулятора, наличия кодов доступа, интерфейсов внешнего подключения к специальному оборудованию используемому экспертами ЭКЦ.

При наличии благоприятных составляющих – отсутствие кода доступа, заряд аккумулятора, исправность устройства осмотр начинается с перевода устройства в «режим полета», при котором отключаются функции, способные принимать или передавать сигнал: сотовая связь, Bluetooth, WI-FI, GPS. Устройство продолжает функционировать как стандартное компьютерное оборудование без передачи или приема данных с внешних устройств. После определения состояния мобильного устройства фиксируются с занесением в протокол основные признаки мобильного устройства такие как идентификационный номер устройства – IMEI, операционная система, версия прошивки, телефонный номер сим-карты, IP-адреса, MAC-адреса устройства.

Далее идет протоколирование и фиксация электронных данных мобильного устройства:

- «Контакты», в котором содержатся внесенные пользователем телефонные номера, фотографии и краткие сведения об их владельцах. Осмотр данной информации позволяет установить круг общения пользователя мобильного телефона, его интересы, место работы;
- «Журнал вызовов» мобильного устройства отображаются принятые, непринятые, исходящие телефонные вызовы в виде номеров. Изучение данного раздела дает общее представление о количестве, повторяемости последних местных или междугородних звонков. При описании в протоколе осмотра исходящих и входящих телефонных номеров следует обращать внимание на дату, время начала и продолжительность соединения пользователя мобильного телефона с номером конкретного абонента.
- «Сообщения» содержит сведения о входящих, исходящих SMS, MMS, EMS, голосовых сообщениях и отчет о доставке таких сообщений. Принятые и отправленные сообщения могут содержать текст, иллюстрации, фотографии, звукозаписи. В протоколе следственного действия отображаются сведения о SMS-, EMS-, MMS-сообщениях и их дословное содержание (для текстов). Сведения о SMS-, EMS-, MMS-сообщения включают номер, на который они отправлены и с которого они получены, дата и время отправления и получения сообщения.
- «Приложения» содержит сведения о установленных на устройстве программах в том числе банковских продуктов. В протоколе следственного действия отображаются сведения о всех значимых программах в частности о программах мобильного управления банковскими счетами – «Сбербанк онлайн» и иных подобных.
- «Галерея» содержит сведения о фотоизображениях, полученных на устройство не только посредством камеры, но и со сторонних приложений – интернет мессенджеров.

Для быстрого создания копии памяти устройства, участвующий в осмотре специалист, может подключить телефон к стационарному компьютеру и при необходимости инсталлировать предлагаемую телефоном программу синхронизации, после чего сохранить на компьютере сведения памяти телефона, записать их на оптический диск или распечатать на бумажный носитель, с обязательным отражением данной операции в протоколе.[15]

Как следует из представленного анализа запись памяти устройства на оптический диск и приложение его отдельно к протоколу осмотра предметов выступает обеспечительной мерой сохранения запротоколированных данных в случае выхода из строя первоисточника информации.

Таким образом следует сделать вывод что осмотр предметов, документов является неотъемлемой частью в процессе сбора доказательств, сопоставления данных с полученными сведениями. Проведенный должным образом осмотр предметов и документов сопоставляет ранее полученные доказательства на первоначальном этапе, служит основой для выявления дополнительных сведений в рамках уголовного дела, способствующих установлению обстоятельств совершенного преступления, а также подтверждающей причастность лиц к совершению преступлений.

Неотъемлемой частью процесса сбора доказательств по уголовному делу является получение показаний участников уголовного дела путем проведения и протоколирования допросов лиц.

Процессуальные положения, являющиеся обязательной и составной частью проведения допроса указаны в главе 26 УПК РФ.

При этом с учетом разности сторон – участников уголовного судопроизводства, а также необходимостью получения от каждого из участников конкретизированных сведений тактика допроса лиц является индивидуальной.

---

[15] Участие специалиста при осмотре сотового телефона по преступлениям, связанным с незаконным оборотом синтетических психоактивных веществ, совершаемым с использованием интернет-магазинов. [Электронный ресурс] // URL: https://u.sovpravo.press/Beh (дата обращения: 02.04.2022).

В процессуальном плане закреплены следующие статусы лиц – участников уголовного судопроизводства на тактике проведения допросов которых следует остановится: потерпевший, подозреваемый (обвиняемый).

В соответствии со статьей 42 УПК РФ потерпевшим является физическое лицо, которому преступлением причинен физический, имущественный, моральный вред, а также юридическое лицо в случае причинения преступлением вреда его имуществу и деловой репутации.

Тактика допроса потерпевшего зависит от обстоятельств совершенного в отношении него преступления, при этом наиболее значимой следует считать тактику проведение допроса указанного лица при совершении в отношении него, так называемого дистанционного преступления, при котором потерпевший и злоумышленник не осуществляют личный контакт.

Важность правильного и полного сбора информации при проведении допроса потерпевшего является неотъемлемой частью при получении первоначальных сведений, которые в последующем закладываются при процессе сбора и оценки доказательств по уголовному делу, являясь отправной точкой для хода расследования и выстраивания линии обвинения.

Изучение уголовных дел рассматриваемой категории показало, что указанного рода преступления с учетом сформированной тактики и методики допросов потерпевших можно условно разделить на две категории, к первой стоит отнести преступления, в ходе которых инициатором контакта выступает злоумышленник (это преступления, отнесенные к категории телефонных разговоров, при которых злоумышленник лично инициирует общение с потерпевшим под различными предлогами). Ко второй категории стоит отнести преступления, в которых заявитель (потерпевший) сам инициативно находит контакт с злоумышленником (это преступления, отнесенные прежде всего к категории интернет продаж, извлечения прибыли, получения доходов, участия потерпевших в различных акциях и т.п.).

С учетом указанного в данном случае стоит разграничить несколько моделей проведения допроса потерпевшего, а также лица выступающего в роли

заявителя, которыми нередко в уголовном деле на первоначальной стадии выступают лица в статусе свидетеля, в связи с чем далее по тексту потерпевший и заявитель будут отнесены к единой категории.

Допрос потерпевшего (заявителя) при факте дистанционного мошенничества, совершенного посредством телефонного звонка.

Данный факт дистанционного мошенничества является наиболее распространенным и заключается в общении между потерпевшим и злоумышленником посредством телефонных переговоров. Злоумышленник в данном случае выступает инициатором контакта с заявителем (потерпевшим), осуществляет активное вовлечение потерпевшего в переговоры. При этом общении злоумышленник в зависимости от способа совершения преступления будет представляться потерпевшему от лица родственника, знакомого, сотрудника правоохранительных органов, банковского или кредитного учреждения, сотрудником различных организаций. При этом нередки случаи представления злоумышленника несколькими лицами одновременно путем изменения манеры разговора, голоса, либо участия нескольких лиц.

При указанном сценарии преступления в ходе допроса потерпевшего в обязательном порядке необходимо выяснить следующие обстоятельства:

– дата, время поступления звонка (звонков), подробное описание содержания разговора, с указанием сведений о том: кем представился звонивший, о чем говорил, что предлагал сделать, каким образом заявитель должен был исполнить требования. При этом отдельно необходимо дать описание голоса, звонившего (наличие дефектов речи – хрипота, картавость, шепелявость, заикание), интонация голоса, разговаривал ли он шепотом или обычным тембром, какие особенности в интонации в произношении звуков, слов, использование в разговоре специальных терминов, специфических речевых оборотов; выяснить по каким приметам заявитель сможет опознать голос звонившего. Точно описать данные которыми представился злоумышленник, называл ли должность, ФИО, свое местонахождение, принадлежность к службе, организации;

– какие сведения заявитель сообщил злоумышленнику при поступлении от последнего вопросов. В обязательном порядке необходимо выяснить имеются ли у заявителя сведения об абонентском номере злоумышленника, сведения об абонентском номере самого заявителя (потерпевшего), на который поступил звонок, с обязательным отражением принадлежности к стационарной или мобильной связи, каково было качество связи между заявителем (потерпевшим) и злоумышленником, имелись ли какие-либо помехи, посторонние звуки, шум или голоса, какова была слышимость разговора, и прерывалась ли связь в ходе разговора.

– выяснить длительность телефонного разговора с злоумышленником, количество состоявшихся разговоров (указанные сведения необходимо сверить в последующем с данными детализации телефонных переговоров);

– в случае если при звонке злоумышленник представился родственником, знакомым, необходимо выяснить у заявителя, как часто его посещает указанное лицо, от имени которого шел телефонный разговор, как заявитель характеризует данное лицо, в каких взаимоотношениях находится с указанным лицом, указать на род деятельности, источники доходов, известный круг круга общения лица от имени которого шел разговор, выяснить сведения о привлечении к уголовной ответственности, отбытии наказания, в частности, в местах лишения свободы, указанного в разговоре лица;

– установить кто из посторонних лиц посещает или посещал в последнее время заявителя, в т.ч. социальный работник, медицинский работник, представители государственных организаций, правоохранительных органов и т.п., полные анкетные данные указанного лица с отражением контактных номеров телефонов; как заявитель может охарактеризовать данное лицо, когда последний раз тот посещал заявителя, знакомо ли лицо с родственниками заявителя;

– выяснить источник материальных ценностей (денежных средств) заявителя – личные накопления, заемные денежные средства, вклады и т.п. В случае если передача денежных средств осуществляется путем банковских и

иных переводов установить сведения о счетах и банковских картах заявителя, участвующих в операциях по переводу.

Далее в зависимости от способа передачи материальных ценностей (денежных средств), у заявителя (потерпевшего) следует подробно выяснить:

В случае контактной передачи материальных ценностей (денежных средств, ценностей, переданных «курьеру»):

– как злоумышленник и в последующем «курьер» узнал точный адрес места жительства заявителя: последний сам назвал его, либо неизвестный, уже знал его место жительства;

– в какой период времени общения с злоумышленником (в период общения или после состоявшегося общения) к месту жительства (месту нахождения) заявителя подъехало неизвестное лицо – выполняющее роль «курьера»;

– описание действий неизвестного лица (курьера, таксиста), с указанием и описанием особенностей поведения, голоса, интонации, произношении звуков, в обращении к заявителю он заметил; по каким приметам заявитель сможет опознать указанное лицо, а именно подробное описание черт лица, рук, особенностей телосложения, походки, поведения для составления детального композиционного портрета личности, полное описание одежды;

– если передача денег осуществлялась в жилище заявителя, установить: когда неизвестный «курьер» зашел в квартиру (помещение), до каких предметов интерьера, иных предметов дотрагивался, как себя вел, что сообщил, говорил, задавал ли какие-либо вопросы, задавал ли заявитель ему какие-либо вопросы, какие получил ответы. Осуществлял ли неизвестный – «курьер» какие-либо звонки, если, да то описание данного разговора;

– сообщал ли заявитель неизвестному – «курьеру» точную сумму денег, которую передал ему, сведения о материальных ценностях и для каких целей он передает ему указанные ценности. Отразить наличие или отсутствие упаковки при передаче материальных ценностей (денег) ее описание, точные сведения и количество передаваемых ценностей (денежных средств);

– выяснить у заявителя личную оценку действиям «курьера» по поведению неизвестного, а именно было ли очевидно, что последний осведомлен о содержимом переданном ему, о причинах (целях) передачи ему материальных ценностей;

– установить провожал ли заявитель неизвестного – «курьера», наблюдал ли за направлением его движения (точное описание маршрута), передвигался ли неизвестный на автомобиле (с указанием цвета, модели регистрационных данных, наличие особенностей в окраске кузова и т.п.);

В случае бесконтактной передачи материальных ценностей (банковского или иного перевода денежных средств, ценностей):

– необходимо выяснить, какие сведения для осуществления бесконтактной передачи материальных ценностей сообщил заявителю злоумышленник, а именно данные о номере банковской карты (счета), сведения о номере абонентского номера, данных на чье имя осуществляется перевод (установочные данные получателя). При этом необходимо у заявителя истребовать квитанцию о переводе, чек (при их наличии).

– выяснить обстоятельства осуществления бесконтактной передачи материальных ценностей, в случае осуществления перевода через банкоматы, терминалы и т.п. выяснить их точное местонахождение; в случае осуществления перевода денежных средств с использованием мобильных устройств установить с помощью какого устройства и программного обеспечения осуществлялся перевод, истребовать сведения с устройства путем его осмотра;

– установить количество осуществлённых операция по переводу, размер и суммы переводов денежных средств, наличие изъятых комиссий;

– выяснить, какие меры предприняты заявителем после обнаружения факта мошеннических действий, какие лица были осведомлены о совершенном преступлении, явились его очевидцами, данные указанных лиц;

– в обязательном порядке установить является ли ущерб для заявителя

значительным, если да, то обязательно отразить обстоятельства, подтверждающие это, каков состав семьи, близких родственников, лиц, находящихся на иждивении, размер доходов и расходов заявителя по состоянию на момент совершения в отношении него преступления.

Так примером полноты допроса потерпевшего по уголовному делу № 1180187*****0015 (по факту мошенничества под видом телефонного звонка от родственника), следует отметить, что следователем в рамках возбуждённого уголовного дела при допросе потерпевшего «К» согласно представленного алгоритма были выяснены обстоятельства телефонного разговора с неизвестным лицом, представившимся родным братом потерпевшего, попавшим в ДТП со смертельным исходом. Потерпевший не только подробно смог описать обстоятельства разговора, посторонние шумы, присутствующие при разговоре, характерные для колонии поселения в виде лая собак, но и дал описание лица согласно которого был составлен субъективный портрет лица выступившего в роли «курьера» для передачи денежных средств. На основании фоторобота был установлен сотрудник службы такси – подозреваемый «Т», который по просьбе своего знакомого, отбывающего наказание в колонии поселения – подозреваемого «О», получал денежные средства от потерпевших после чего осуществлял их зачисление на банковские счета и абонентские номера подозреваемого «О». При этом своевременно составленный фоторобот и выявленное лицо позволили изъять сотрудникам правоохранительных органов похищенные у потерпевшего «К» денежные средства в сумме 120 000 рублей и золотую цепочку.

Далее стоит рассмотреть особенности тактики построения допроса по условной второй категории преступлений, когда инициатором выступает потерпевший (заявитель): при факте дистанционного мошенничества, совершенного с использованием информационно-телекоммуникационной сети «Интернет» при осуществлении покупок/продаж.

В ходе допроса заявителя (потерпевшего) необходимо установить:

– дату, время обнаружения объявления, ссылку на соответствующий Интернет-ресурс, зафиксировать его URL-адрес, при наличии возможности сделать снимок экрана, который приобщить к материалам проводимой проверки (уголовного дела);

– установить с использованием какого технического устройства заявитель (потерпевший) выходил на интернет сайт с размещенным объявлением (переходил по интернет-ссылке) – стационарный компьютер, мобильное устройство;

– содержание объявления с указанием характеристик продаваемого товара, цены, местонахождения, наличия фотографических изображений;

– условия купли-продажи, указанные в объявлении (условия о предоплате, оплате товара, сроках и видах поставки, ответственности сторон);

– какие контактные данные продавца содержались в объявлении, имелись ли отзывы, комментарии к объявлению, какие данные о профиле продавца были указаны (дата и время создание профиля);

– каким образом, когда (дата, время) заявитель связался с продавцом, каким способом происходила «связь» покупатель-продавец – путем переписки, телефонных звонков; как продавец представился, какие сведения сообщил о своем местонахождении и местонахождении товара (отразить подробное содержание разговора (переписки) с продавцом. В случае «живого» общения путем телефонных переговоров, видео-звонков выяснить описание голоса продавца (внешности), сможет ли заявитель его опознать (по каким приметам). В случае общения путем переписки – истребовать переписку;

– указать что продавец сообщил о продаваемом товаре, условиях оплаты, сроках и способах доставки покупателю товара, какие документы имеются на товар подтверждающие принадлежность продавцу;

– выяснить, когда (дата, период времени), каким образом (через банкомат, посредством услуги «Сбербанк Онлайн», «Мобильный банк»), в каком размере заявитель перечислил на какой счет (№ счета, либо банковской карты, открытые

на чье имя) денежные средства в счет оплаты приобретаемого товара; Если заявитель осуществил перевод денежных средств со своей банковской карты на банковскую карту неизвестного посредством услуги «Сбербанк Онлайн», через «Личный кабинет», установить место входа потерпевшего в сеть «Интернет» (с какого компьютера, ноутбука, планшета, с использованием какого модема, WI-FI-роутера, их MAC-адреса, логины и пароли, какая компания-провайдер предоставляла в этот день заявителю услуги доступа в «Интернет»). Установить дату и место открытия счета (банковской карты), с которой заявитель перечислил денежные средства;

– установить каким образом заявитель (потерпевший) известил «продавца товара» о перечислении денежных средств на указанную им банковскую карту (электронный кошелек, абонентский номер) и что ему сообщил после подтверждения оплаты «продавец»;

– когда заявитель (потерпевший) осознал, что в отношении него совершено мошенничество, предпринятые заявителем действия после обнаружения факта мошеннических действий;

– в обязательном порядке установить является ли ущерб для заявителя значительным, если да, то обязательно отразить обстоятельства, подтверждающие это, каков состав семьи, близких родственников, лиц, находящихся на иждивении, размер доходов и расходов заявителя по состоянию на момент совершения в отношении него преступления.

Так примером полноты допроса потерпевшего по уголовному делу № 1200187*****0123 (по факту мошенничества под предлогом продажи «снегохода» через интернет сайт «Авито»), следует отметить что следователем в рамках возбуждённого уголовного дела при допросе потерпевшего «А» согласно представленного алгоритма были выяснены обстоятельства переписки, состоявшейся между «продавцом-покупателем». Потерпевший пояснил что во время диалога «продавец» отправил видео сообщение посредствам мессенджера «Вайбер» в котором показывал гараж, в котором стоял внешне

схожий со снегоходом предмет, накрытый брезентом, при этом как указал потерпевший на представленном видео, на общем плане гаражного массива имелась табличка «ГК Калинка-1 г. Сызрань». На основании полученных от потерпевшего данных сведений банковского учреждения, согласно которых обналичивание денежных средств по счету, на который осуществлено зачисление потерпевшим, происходило на территории Самарской области, было установлено место проведения сьемки и в последующем лицо совершившее преступление.

При этом ко второй категории рассматриваемой в представленной работе, также следует отнести преступления при факте дистанционного мошенничества, совершенного с использованием вредоносного программного обеспечения. Несмотря на тот факт, что в данном случае значительную роль играет процесс выявления и осмотра носителей вредоносных программных продуктов, проведение соответствующих экспертиз, при этом первоначально имеет немаловажное значение выяснение отдельных вопросов у потерпевшего (заявителя), так в ходе допроса необходимо в обязательном порядке установить сведения о посещении каких-либо сайтов за последний период времени, инсталляции каких-либо сторонних приложений, сведения о характере, распространении и уничтожении вредоносным программным обеспечением каких-либо имеющихся сведений на носители электронной информации, выяснение сведений о наличии сбоев в работе оборудования (перезагрузки, «подвисание» программ или блокировка в период работы и прочее).

Зачастую работа вредоносного программного обеспечения отражается на работе устройства.

Так примером полноты допроса потерпевшего по уголовному делу № 1190187*****2419 (по факту мошенничества в сфере компьютерной информации), следует отметить, что следователем в рамках возбуждённого уголовного дела при допросе потерпевшего «З» подробно был выяснен вопрос работы смартфона «Самсунг» находящегося в пользовании указанного лица. Потерпевший «З» сообщил что после посещения интернет ресурса

содержащего сведения о проведении лотерей, на смартфон последнего было инсталлировано программное обеспечение, которое не отображалось на «рабочем столе» устройства, при этом в ходе использования смартфона и посещения интернет ресурсов банка «Сбербанк», смартфон постоянно зависал на вводе данных в личный кабинет пользователя. В дальнейшем потерпевший при получении выписки по банковскому счету обнаружил 15 операций по списанию денежных средств в счет оплаты «Google - сервисов», которые последний не производил. Изъятый и осмотренный следователем смартфон, был направлен на проведение компьютерной экспертизы, по результатам которой экспертом было детектировано наличие вредоносного программного обеспечения.

Используемое ранее по тексту работы слово «злоумышленник», подразумевает в себе лицо совершившее преступление рассматриваемой категории, которому уголовно-процессуальным законодательством присвоены статусы – подозреваемого, обвиняемого. При этом в ходе предварительного следствия указанными статусами на временном промежутке расследования конкретного уголовного дела обладает фактически одно и тоже лицо.

Статья 46 УПК РФ, дает юридическое, процессуальное определение подозреваемого лица.

Статья 47 УПК РФ, дает юридическое, процессуальное определение обвиняемого лица.

При этом не смотря на разные процессуальные статусы подозреваемого и обвиняемого и как следствие объем процессуальных полномочий, тактика проведения допроса указанных лиц является единой.

Изученная следственная практика по уголовным дела указанной категории показала, что на момент установления лица, относящегося к категории подозреваемого (обвиняемого) сотрудники правоохранительных органов обладают значительным объемом полученных доказательств, изобличающих виновное лицо. При расследования уголовных дел рассматриваемой категории следователь (дознаватель) часто сталкиваются с тем

что что подозреваемые (обвиняемые) в значительном количестве случаев обладают высокими познаниями в информационных технологиях, позволяющих конспирировать свою преступную деятельность, часто используют специфическую терминологию в том числе жаргонного характера. Указанная терминология не всегда понятна обывателю, следователю.

Планируя проведение допроса подозреваемого (обвиняемого), с целью получения информации по уголовным делам, в частности о лицах, способствовавших совершению преступления, участвовавших в совершении групповых преступлений следует тщательно подготовиться к проведению допроса и протоколированию показаний.

Прежде всего сотрудник правоохранительных органов перед проведением допроса изучает личность лица, его сферу работы, уровень образования, владения ЭВМ, а том числе навыки программирования, круг общения, в том числе изучается личность на наличие компрометирующей информации, в частности, наличие судимостей за аналогичные преступления. Так при наличии у подозреваемого (обвиняемого) судимостей следователь, дознаватель может изначально определить указанные выше сведения, а также характер показаний и степень взаимодействия лица с правоохранительными органами.

Изучение сферы деятельности подозреваемого (обвиняемого) на первоначальном этапе позволяет определить прежде всего необходимость привлечения к допросу специалистов узкой направленности, в том числе для получения развернутых определений специальных терминов, установления возможности и алгоритма работы оборудования, используемого злоумышленником и т.п.

При этом при работе с указанным участником уголовного процесса возможно два сценария проведения допроса, которые в большей степени зависят только от степени участия подозреваемого (обвиняемого) в самом допросе.

Материалами изученных уголовных дел установлено что в случае отказа подозреваемого (обвиняемого) идти на сотрудничество с правоохранительными

органами, следователь (дознаватель) в режиме «вопрос – ответ» выясняет обстоятельства совершенного преступления, в том числе выясняет принадлежность изъятого у лица имущества, выясняет возможные версии, которые подозреваемый (обвиняемый) выдвигает на поставленные вопросы, при этом во время проведения допроса уделяется значительное внимание на обстоятельства и события указанные подозреваемым по выдвинутой версии для последующего сравнения с полученными в рамках уголовного дела доказательствами. Во время проведения допроса по указанному сценарию подозреваемому (обвиняемому), также могут быть частично представлены для обозрения полученные доказательства, в частности видеозаписи с камер наружного наблюдения, выписки банковских и кредитных учреждений, иные материалы. По представленным для обозрения материалам подозреваемому (обвиняемому) задаются конкретизированные вопросы с целью выяснения позиции лица. Дальнейшее проведение допросов и иных следственных действий зависит от собранных в рамках уголовного дела доказательств, полученной информации и последующей позиции подозреваемого (обвиняемого).

Так примером допроса подозреваемого по уголовному делу № 1200187*****0123 (по факту мошенничества под предлогом продажи «снегохода» через интернет сайт «Авито»), следует отметить что следователем в рамках возбужденного уголовного дела при допросе подозреваемого «Б», который отрицал свою причастность к совершению данного преступления были продемонстрированы протокол допроса потерпевшего, с приложенными фотоизображениями гаража, арендованного подозреваемым «Б» на территории г. Сызрань в период совершения преступления, видеозаписи с камеры банкомата в котором осуществлялось обналичивание похищенных денежных средств, на которых был зафиксирован подозреваемый «Б». После предъявления указанных материалов подозреваемый «Б», при предъявлении постановления о привлечении в качестве обвиняемого, в ходе допроса в качестве обвиняемого, изложил подробные признательные показания по

совершенному преступлению.

При осуществлении допроса подозреваемого (обвиняемого) по второму условному сценарию, указанное лицо оказывает взаимодействие правоохранительным органам. В данном случае должностному лицу фактически необходимо зафиксировать событие совершенного преступления «зеркально» от тех вопросов, которые предполагаются для выяснения у потерпевшего, при этом обязательному выяснению подлежит уточнение обстоятельств, способствовавших совершению преступлению, этап подготовки к его совершению в т.ч. путем приискания средств и оборудования, а также последующие действия лица после совершенного преступления включая способ распоряжения похищенным имуществом, сведения о соучастниках, используемом оборудовании, как для совершения преступлений (сотовые телефоны, ЭВМ, ноутбуки и т.п.), так и для получения похищенного имущества (банковские счета, карты, банкоматы, электронные кошельки и т.п.).

При выяснении обстоятельств преступления следователь самостоятельно определяет перечень вопросов, исходя из полученной информации и имеющихся доказательств.

Стоит отметить, что при активном участии подозреваемого (обвиняемого) в раскрытии преступления сотрудниками правоохранительных органов проводится целый ряд дополнительных следственных действий, направленных в т.ч. на установление новых способов совершения рассматриваемых преступлений, средств, предметов и оборудования способствующих их совершению – проверка показаний, следственный эксперимент, очные ставки, осмотры и иные.

Так примером допроса обвиняемого по уголовному делу № 1200187*****0123 (по факту мошенничества под предлогом продажи «снегохода» через интернет сайт «Авито»), следует отметить что следователем в рамках возбужденного уголовного дела при допросе обитаемого «Б», пожелавшего сотрудничать с органами предварительного следствия, при выяснении обстоятельств совершенного преступления, установлено что

обвиняемым расследуемое преступление совершено с использованием ноутбука «HP» при проживании в дачном доме знакомого (указанное обстоятельство в ходе следствия установлено не было). В ходе проведения проверки показаний обвиняемого «Б» и последующей выемки обнаружен и изъят ноутбук, содержащий информацию о совершенных преступлениях, зафиксировано место совершения обвиняемым преступления, осуществлена фиксация показаний обвиняемого на месте с проверкой возможности совершения преступления с указанного дачного дома посредствам сети «Интернет».

Таким образом допрос - это неотъемлемая часть процесса сбора доказательств по уголовному делу, получение первоначальных сведений, которые в последующем закладываются при процессе сбора и оценки доказательств по уголовному делу, является отправной точкой для хода расследования и выстраивания линии обвинения. Тактика допроса зависит от обстоятельств совершенного преступления, наиболее значимой следует считать тактику проведение допроса при совершении дистанционного преступления, при котором потерпевший и злоумышленник не осуществляют личный контакт.

При расследовании преступлений рассматриваемой категории как уже было указано ранее, следователь (дознаватель) сталкиваются с значительным объемом изымаемой информации. Специфика настоящих преступлений заключается в том, что преимущественно информация несущая доказательственное значение для уголовного дела содержится на носителях информации в электронно-вычислительных машинах, включающих – персональные компьютеры, ноутбуки, блоки серверов и иное сетевое и периферийное оборудование; носимых «гаджетах» - смартфоны, «умные часы», электронные планшеты, а также иных устройствах, позволяющих осуществлять доступ к средствам электронной телекоммуникации.

Практика показала, что расследованием и раскрытием уголовных дел рассматриваемой категории занимаются должностные лица – сотрудники органов предварительного следствия и оперативных подразделений,

обладающих достаточными знаниями и умениями использования оборудования и средств электронной телекоммуникации, что позволяет осуществлять первоначальные следственные действия (осмотры предметов) без привлечения специалистов и экспертов с целью получения информации являющейся фундаментом для дальнейшего расследования уголовного дела. Между тем расследование уголовных дел по преступлениям указанной категории не обходится без привлечения экспертных подразделений для проведения экспертиз.

Глава 27 УПК РФ определяет процессуальный порядок производство судебных экспертиз.

С учетом наличия специфики в совершении любых преступлений, тактика назначения и проведения экспертиз различна и основывается на выработанных методиках. Как правило по указанной категории преступлений назначается компьютерная экспертиза. Объектом указанной экспертизы выступает хранящаяся в устройстве информация, содержащая сведения о: действиях пользователя, связанных с процессом обработки файлов, ведения баз данных, передачи данных и т.п.; отдельные технические средства и устройства компьютера; системы обработки информации в целом. Основанием для назначения экспертизы является необходимость исследования: информации, записанной в устройстве; данных о действиях пользователя и возможности совершения определенных действий с помощью устройства; свойств программ и программных продуктов; фактических обстоятельств совершения преступления с использованием устройства.

При этом практика показала, что устройство, направляемое на экспертизу может принадлежать как потерпевшей стороне, так и злоумышленнику – подозреваемому (обвиняемому).

На подготовительном этапе, назначения судебной экспертизы уполномоченное должностное лицо проводит консультацию с экспертами, проводящими исследования компьютерной информации и их носителей. Именно на указанном этапе определяется объем предоставляемого в

распоряжение эксперта материалов, а также перечень вопросов, которые эксперт сможет выяснить при исследовании исходя из представленных объектов.

При этом стоит отметить что предоставление полученных в ходе доследственной проверки, либо в ходе расследования уголовного дела изъятых (полученных) носителей информации (смартфонов, ноутбуков, планшетных компьютеров) для проведения экспертизы необходимо осуществить в кратчайшие сроки. Указанное обстоятельство вызвано прежде всего тем фактом, что в большинстве случаев изымаемые телекоммуникационные средства связи, являющиеся носителем информации, защищены от свободного доступа паролем, при этом если в ходе оперативно-розыскных или следственных мероприятий такой пароль выяснить удалось, то осмотр устройства следователь может провести без особых проблем. Если же владелец отказывается сообщить пароль и каким-либо другим путем установить его не представляется возможным, то следует помнить, что в экспертных учреждениях существуют специальные устройства, которые позволяют войти в операционную систему такого устройства, минуя пароль, либо «взломав» его[16].

Согласно сложившейся практике расследования уголовных дел выработан примерный перечень вопросов для проведения экспертиз:[17]

– имеются ли на изъятых ЭВМ, представленных на исследование, интересующие следствие сведения (типы файлов, ключевые слова, определенное программное обеспечение и пр.). Если да, то какие именно и где они располагаются;

---

[16] Скобелин С.Ю. Юридическая основа и процессуальное оформление извлечения и анализа данных из мобильных устройств / С.Ю. Скобелин // Расследование преступлений: проблемы и пути их решения: Сборник научно-практических трудов. - 2013. - № 1. - С. 183.

[17] Расследование преступлений, совершенных с использованием информационно-коммуникационных технологий / А.Ю. Ушаков, А.М. Столповский, А.Г. Саакян. – Н. Новгород, 2017. – С. 63.

– возможно ли осуществление доступа к сети «Интернет» с использованием представленных на исследование объектов? Если да, то, каким образом осуществлялся доступ;

– имеются ли следы доступа к Интернет-ресурсу (указывается интересующий интернет-сайт, форум, блог и т. д.), какие именно, можно ли получить доступ к переписке? Если да, то приобщить переписку с указанием «ник-неймов» - имен пользователей участников общения;

– имеются ли на изъятой электронно-вычислительной технике, представленной на исследование, информация об осуществлении сеансов доступа к сети «Интернет» за интересующий следствие период, в том числе файлы-cookie? Если да, то, какие учетные данные использовались для выхода в сеть «Интернет»? В каких файлах содержатся сведения об использовавшихся учетных записях и паролях;

– какие MAC-адреса имеет сетевое оборудование представленных на экспертизу объектов;

– использовалось ли представленное на экспертизу сетевое оборудование для выхода в сеть «Интернет» в интересующий следствие период;

– имеется ли в представленном на экспертизу мобильном телефоне на установленных в нем сим-карте и карте памяти информация о номерах телефонов, SMS-сообщениях, исходящих и входящих звонках, аудио-, видео- и графические файлы, если да, то какая именно;

– имеются ли в компьютерной системе признаки (указывается интересуемый перечень конкретных признаков) неправомерного доступа к данным;

– имеется ли на жестком магнитном диске системного блока персонального компьютера программное обеспечение для ...;

– имеется ли на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, программное

обеспечение, позволяющее сканировать ip-адреса компьютеров пользователей сети Интернет, имеющих открытые для удаленного доступа из сети Интернет ресурсы? Если да, то такое программное обеспечение (название, версии, место расположения на носителе)? Имеются ли данные, свидетельствующие об использовании этого программного обеспечения? Если да, то какие именно;

– имеется ли на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, программное обеспечение, позволяющее подобрать пароль для подключения к жесткому диску удаленного компьютера? Если да, то какое программное обеспечение (название, версии, место расположения на носителе);

– имеются ли на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, вредоносные программы, заведомо приводящие к модификации, блокированию, копированию или уничтожению компьютерной информации, нарушению работы ЭВМ, системы ЭВМ или их сети? Если да, то каково их назначение, предназначение, расположение? Имеются ли данные, свидетельствующие об их создании на исследуемом машинном носителе и распространении (в том числе по сети Интернет)? Если да, то какие именно;

– имеется ли на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, программное обеспечение, позволяющее пользоваться услугами электронной почты? Если да, то, какое программное обеспечение (название, версии)? Имеются ли на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, информация о файлах, содержащих почтовые сообщения? Каков адрес электронного почтового ящика, на который получены входящие сообщения;

Экспертизы по уголовным делам о преступлениях рассматриваемого вида рекомендуется назначать в государственных экспертных учреждениях системы

МВД России и Минюста России, сотрудники которых имеют допуски на проведение соответствующих экспертиз[18].

Так примером компьютерной судебной экспертизы по уголовному делу № 1200187*****0123 (по факту мошенничества под предлогом продажи «снегохода» через интернет сайт «Авито»), следует отметить что следователем в рамках возбужденного уголовного дела по изъятому ноутбуку принадлежащему обитаемому «Б», в ЭКЦ МВД по Республике Коми назначена компьютерная экспертиза, включавшая в себя вопросы, указанные по тексту представленной работы. Экспертом проведено исследование НЖМД ноутбука, восстановлена информация о работе браузеров в сети «Интернет» на сайте «Авито.ру», выявлены фотографии по создаваемым «фейковым» объявлениям по продаже мототехники. По результатам экспертизы выявлено 5 ранее не заявленных фактов хищения денежных средств граждан путем мошенничества, по которым приняты решения о возбуждении уголовных дел.

[18] Методические рекомендации «Особенности квалификации и расследования преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ» ФГКУ «ВНИИ МВД России» // коллектив авторов Улейчик В.В., Мусеибов А.Г., Лебедева А.А., Куприянов Е.И., Гусев Д.В.

ЗАКЛЮЧЕНИЕ

Широкое распространение преступлений, совершаемых с использованием информационно-коммуникационных технологий, предопределило подготовку данной работы, в которой рассмотрены основные направления работы правоохранительных органов на стадии досудебного производства по уголовным делам о преступлениях, совершаемых с использованием информационно-коммуникационных технологий.

Проанализировав материалы следственной практики, положения действующего законодательства, разработанные алгоритмы и методики расследования позволили определиться с понятиями и способами совершения преступлений с использованием информационно-коммуникационных технологий, определить проблемы, возникающие как на стадии доследственной проверки, так и в ходе расследовании подавляющего числа преступлений указанной направленности.

Так рассмотрев преступления, совершаемые с использованием информационно-коммуникационных технологий следует сделать вывод что наибольший удельный вес из общего числа регистрируемых преступлений, имеют преступления, представленные в 21 «Преступления против собственности» и 28 «Преступления в сфере компьютерной информации» главах УК РФ соответственно.

На примере указанных категорий преступлений, ставших предметом исследования, изучены алгоритмы и методические материалы, оказывающие практическую и теоретическую помощь должностным лицам:

1) по расследованию преступлений, совершаемых против собственности с использованием информационно-коммуникационных технологий (ст. 158, 159, 159.3, 159.6 УК РФ);

2) по расследованию преступлений, совершаемых в сфере компьютерной информации (ст. 272, 273 УК РФ).

Представленной работой выявлена основанная проблематика, выраженная в постоянном совершенствовании способов совершения преступлений, применяемых средств и способов со стороны злоумышленников. Только анализ и изучение указанной проблематики способствует совершенствованию методов борьбы с преступлениями указанной категории.

Алгоритмы и методики, разработанные для выявления и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий, не являются исчерпывающими и требуют постоянного совершенствования.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

Нормативные-правовые акты

1. Федеральный закон от 27.06.2011г. № 161-ФЗ «О национальной платежной системе» (ред. от 02 июля 2021г.) // Собрание законодательства РФ. - 2011г. - № 27. - ст. 3872.

2. Федеральный закон от 02.12.1990г. № 395-1-ФЗ «О банках и банковской деятельности» (ред. от 01 апреля 2022г.) // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. - 1990 г. - № 27. - ст. 357.

3. Уголовный кодекс Российской Федерации : федер. закон от 13 июня 1996г № 63-ФЗ : [ред. от 25.03.2022] // Собрание законодательства РФ. - 1996г. - №25. - ст. 2954.

4. Уголовно-процессуальный кодекс Российской Федерации : федер. закон от 18 декабря 2001г № 174-ФЗ : [ред. от 25.03.2022, с изм. От 19.05.2022] // Собрание законодательства РФ. - 2001г. - №52. - ст. 4921.

Научная и учебная литература

5. Белоус, В.Г., Грацкая Н.С. Проблема классификации хищений с использованием компьютерных технологий /В.Г. Беловус, Н.С. Грацкая // Актуальные вопросы образования и науки. 2016. No 1-2 (53-54). - С. 49-54.

6. Брызгалов, Г. Е. Механизм преступления при хищении денежных средств, совершаемом с использованием вредоносных компьютерных программ / Г. Е. Брызгалов // Алтайский юридический вестник. – 2018. – № 3(23). – С. 99-04.

7. Елин, В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. - 2013. - № 2. - С. 70-76.

8. Коломинов, В.В. О способе совершения мошенничества в сфере компьютерной информации / В.В. Коломинов // Человек: преступление и наказание. - 2015. - № 3. - С. 145- 149.

9. Левин, Л. М. Киберпреступность как новое направление психологических исследований / Л. М. Левин // IV Международный пенитенциарный форум "Преступление, наказание, исправление" : Сборник тезисов выступлений и докладов участников, к 140-летию уголовно-исполнительной системы России и 85-летию Академии ФСИН России, в 10 т., Рязань, 20–22 ноября 2019 года. – Рязань: Академия ФСИН России, 2019. – С. 364-366.

10. Решняк, О. А. Организация расследования мошенничеств, совершенных с использованием сети "Интернет", на первоначальном и последующем этапах / О. А. Решняк, С. А. Ковалев // Вестник Волгоградской академии МВД России. – 2020. – № 2(53). – С. 106-111

11. Скобелин С.Ю. Юридическая основа и процессуальное оформление извлечения и анализа данных из мобильных устройств / С.Ю. Скобелин //

Расследование преступлений: проблемы и пути их решения: Сборник научно-практических трудов. - 2013. - № 1. - С. 183.

12. Скогорева, Т. Ф. Процессуальные и организационно-тактические особенности расследования преступлений, связанных с хищением денежных средств, совершаемых с использованием компьютерных технологий / Т. Ф. Скогорева, Э. Ж. Чхвимиани // Современная научная мысль. – 2018. – № 3. – С. 194-200.

13. Соколов, А. С. Особенности расследования преступлений в сфере компьютерной информации / А. С. Соколов, А. А. Погосян // Аллея науки. – 2018. – Т. 2. – № 7(23). – С. 331-336.

14. Улейник В.В. Особенности квалификации и расследования преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ : методические рекомендации / В.В. Улейник [и др.]; ФГКУ «ВНИИ МВД Росии». - Москва : Юрайт, 2015. - С.53.

15. Ушаков А.Ю. Расследование преступлений, совершенных с использованием информационно-коммуникационных технологий / А.Ю. Ушаков, А.М. Столповский, А.Г. Саакян. – Н. Новгород, 2017. – С. 241.

16. Хохлов, Ю.Е. Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. — М.: Институт развития информационного общества, 2009. — С. 166.

Электронные ресурсы

17. Криминалистические версии и планирование расследования // Краснодарский университет МВД России [Электронный ресурс] // URL: https://ставф.крду.мвд.рф/upload/site122/document_file/13._Versii_i_planirovanie_Inter._Rezyumir.pdf (дата обращения: 25.02.2022).

18. Наметкин Д.В. , Маринин С.А. Правовые основы производства судебных экспертиз, выявления и доказывания преступлений, совершаемых в сфере игорного бизнеса с использованием компьютерной техники и Интернета // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2013. №21. [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/pravovye-osnovy-proizvodstva-sudebnyh-ekspertiz-vyyavleniyai-dokazyvaniya-prestupleniy-sovershaemyh-v-sfere-igornogo-biznesas (дата обращения: 08.04.2022).

19. Бондарева Г.В. Электронные доказательства в раскрытии и расследовании преступлений // ЮП. 2020. №3 (94). [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/elektronnye-dokazatelstva-v-raskrytii-i-rassledovanii-prestupleniy (дата обращения: 08.05.2022).

20. Определение Конституционного Суда РФ от 25.01.2018 №185-0 // Уголовный Кодекс РФ [Электронный ресурс] // URL:

https://ukrfkod.ru/pract/opredelenie-konstitutsionnogo-suda-rf-ot-25012018-n-185-o/? (дата обращения: 15.01.2022).

21. Старостенко Н.И. Типичные следственные ситуации первоначального этапа расследования мошенничеств, совершенных с использованием методов социальной инженерии в сфере информационно-телекоммуникационных технологий // Вестник Удмуртского университета. Серия «Экономика и право». 2021. №4. [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/tipichnye-sledstvennye-situatsii-pervonachalnogo-etapa-rassledovaniya-moshennichestv-sovershyonnyh-s-ispolzovaniem-metodov (дата обращения: 08.03.2022).

22. Информационно-телекоммуникационные технологии и электроника // ЮЗГУ [Электронный ресурс] //URL: https://swsu.ru/nauka/kt1.php (дата обращения: 15.01.2022).

23. Преступления в сфере компьютерной информации // Уголовное право. Особенная часть [Электронный ресурс] // URL: https://be5.biz/pravo/u032/14.html? (дата обращения: 23.01.2022).

24. Мошенничество путем обмана или злоупотребления доверием // advokat-bukov.ru [Электронный ресурс] // URL: https://www.advokat-bukov.ru/administrative-law/fraud-through-deception-or-abuse-of-trust-the-right-to-property-in-the-concept-of-fraud-and-extortion/ (дата обращения: 14.02.2022).

25. Зеленкина О.Ю. Особенности расследования преступлений в сфере компьютерной информации // Сибирские уголовно-процессуальные и криминалистические чтения. 2019. №2 (24). [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/osobennosti-rassledovaniya-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения: 08.03.2022).

26. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2021 года // МВД России [Электронный ресурс] // URL: https://мвд.рф/reports/item/28021552/ (дата обращения: 05.01.2022).

27. Участие специалиста при осмотре сотового телефона по преступлениям, связанным с незаконным оборотом синтетических психоактивных веществ, совершаемым с использованием интернет-магазинов. [Электронный ресурс] // URL: https://u.sovpravo.press/Beh (дата обращения: 02.04.2022).

28. Какие опасности подстригают доверчивых граждан в интернете // city-n. [Электронный ресурс] // URL: https://www.city-n.ru/view/449610.html (дата обращения: 09.01.2022).

29. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» // Гарант [Электронный ресурс] // URL: https://base.garant.ru/70642118/ (дата обращения: 09.01.2022).

30. Алиев А.Т. Проактивные системы защиты от вредоносного программного обеспечения // Известия ЮФУ. Технические науки. 2014. №2 (151). [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/proaktivnye-sistemy-zaschity-ot-vredonosnogo-programmnogo-obespecheniya (дата обращения: 08.05.2022).

Учебное издание

Лантух Эдуард Владимирович,
кандидат юридических наук

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Учебно-методическое пособие

Компьютерная верстка *Антипов В.А., Джалаева И. Х.*
Дизайн обложки *Антипов В.А.*, *Шеряй А.Н.*

EDN: LYRUCQ

Подписано в печать 20.05.2023 Формат 60×84 $^{1}/_{16}$
Печать цифровая. Объем 4 п. л. Заказ № 3/23 Тираж 100 экз.

Отпечатано в Ленинградском областном филиале Санкт-Петербургского университета МВД России 188662, Ленинградская область, Всеволожский муниципальный район, Муринское городское поселение, производственная зона «Мурино», ул. Лесная д. 18А