ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

ТАКТИКА ПОДГОТОВКИ И ПРОВЕДЕНИЯ ОБЫСКА ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Методические рекомендации

Воронеж
2024

ББК 67.52

Рецензенты:
О.К. Исаева, заместитель начальника отдела экспертно-криминалистических учетов ЭКЦ ГУ МВД России по Воронежской области, к.ю.н., подполковник полиции;
Н.Н. Кожанов, начальник ЭКЦ ГУ МВД России по Воронежской области, полковник полиции.

Тактика подготовки и проведения обыска по делам о преступлениях в сфере информационных технологий / Е.А. Пидусов, Е.И. Пырьева, А.В. Головчанский, О.А. Ерошенко, Д.А. Корчик – Воронеж : Воронежский институт МВД России, 2024. – 1 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

В методических рекомендациях рассмотрены научные положения об общественных отношениях, складывающихся в связи с организацией и производством обыска по делам о преступлениях, совершенных с использованием информационных технологий. Рекомендации направлены на повышение эффективности деятельности следователей органов внутренних дел при подготовке и проведении обыска по делам о преступлениях в сфере информационных технологий. Методические рекомендации могут быть использованы в образовательном процессе по учебным дисциплинам «Криминалистика», «Методы и способы получения доказательственной информации с электронных носителей» и «Расследование отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий».

ISBN .

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современное общество немыслимо без широкого использования информационных технологий, которые играют все более важную роль. Эти технологии проникают в различные сферы жизни, привнося изменения в повседневность миллионов людей. В результате создалась глобальная информационная среда, которая охватывает множество аспектов человеческой жизни и деятельности.

В России за январь – август 2023 года сохраняется тенденция к увеличению количества – на 28,7% противоправных деяний в сфере информационно-телекоммуникационных технологий. Их удельный вес в числе всех преступных посягательств возрос до 32,9%, а по тяжким и особо тяжким – до 56,4%. Больше совершено дистанционных мошенничеств и краж. Раскрываемость киберпреступлений составила 29,9%, в том числе совершенных с использованием сети Интернет – 28,8%, расчетных (пластиковых) карт – 35,7%[1].

В современном мире борьба с преступлениями в сфере информационных технологий стала одной из ключевых и сложных задач, успешное решение которой имеет прямое значение для общего успеха в борьбе с преступностью. В ходе расследования преступлений в данной сфере применяются различные следственные действия для сбора доказательств, в том числе в электронном формате. Среди самых распространенных следственных действий, применяемых при расследовании таких преступлений, можно выделить осмотр, обыск и допрос.

Одним из основных источников доказательств в уголовном деле при расследовании данного вида преступлений является обыск. Однако его проведение и подготовка порой осложнены ограниченным временем, противодействием со стороны преступников и присутствующих в помещении, где проводится обыск. Традиционные тактические методы обыска неприменимы в полной мере из-за особенностей электронных следов, которые часто характерны

[1] Состояние преступности в России за январь-август 2023 года [Текст] / ФКУ «Главный информационно- аналитический центр МВД России»; ред. Москва; – 2023 — 64 с.

для преступлений в данной области. Поиск электронных доказательств также затруднен их способностью быть скопированными, измененными, воспроизведенными или полностью уничтоженными. В свете этих факторов существует неотложная потребность в разработке тактических подходов к проведению обыска по делам о преступлениях в сфере информационных технологий, которые учитывали бы особенности данных технологий.

Вышеперечисленные обстоятельства показывают актуальность данного исследования.

Объектом исследования выступают общественные отношения, складывающиеся в связи с организацией и производством обыска по делам о преступлениях, совершенных с использованием информационных технологий.

Целью данного исследования является разработка рекомендаций по подготовке и тактике проведения обыска при расследовании преступлений в сфере информационных технологий.

Для достижения поставленной цели проведен анализ научной литературы, статистических данных и материалов уголовных дел, связанных с производством обыска по делам о преступлениях в сфере информационных технологий; определены объекты, подлежащие поиску и изъятию при производстве обыска по рассматриваемым преступлениям, проанализированы характеристики данных объектов; с учетом ситуационного подхода подготовлены тактические рекомендации по подготовке и производству обыска по рассматриваемой категории уголовных дел.

Практическое значение данного исследования обусловлено, во-первых, необходимостью методического обеспечения учебного процесса образовательных организаций МВД России при преподавании следующих учебных дисциплин: «Криминалистика», «Расследование преступлений против личности и собственности», «Методы и способы получения доказательственной информации с электронных носителей»; во-вторых, необходимостью методического обеспечения деятельности следователей ОВД при расследовании преступлений, совершенных с использованием информационных технологий.

1. Общие положения тактики подготовки и производства обыска

Одним из действенных, эффективных процессуальных средств получения доказательств при расследовании преступлений является обыск. Определяя значимость данного следственного действия, многие авторы подчеркивают его ключевую роль в решении как основных задач расследования, связанных с поиском и фиксацией доказательств, так и смежных, связанных с обеспечением возможности возмещения ущерба, причиненного преступлением. Именно от результата производства данного следственного действия в распоряжении правоохранительных органов появляются ключевые объекты и информация, позволяющие в дальнейшем выстроить обвинительную линию в совершении преступлений, особенно совершаемых с использованием современных электронных технологий. В то же время, специфика обыска проявляется в принудительном характере данного следственного действия, сопряженного с ограничением некоторых конституционных прав граждан (ст. 23, 25, 35 Конституции РФ). Поэтому лицо, производящее обыск должно не только уметь грамотно использовать тактические приемы проведения данного следственного действия, но и иметь четкое понимание процессуального порядка производства данного следственного действия, применения мер, ограничивающих конституционные права граждан.

Обыск – это следственное действие, содержанием которого является принудительное обследование помещений, сооружений, транспортных средств, участков местности либо живых лиц в целях отыскания и изъятия предметов, документов и иных объектов, имеющих значение для дела, а также обнаружения разыскиваемых лиц и трупов.

По смыслу ч. 1 ст. 182 УПК РФ основаниями для производства обыска являются имеющиеся в уголовном деле достаточные данные, дающие основание полагать, что в каком-либо помещении или ином месте или у какого-либо лица находятся искомые предметы, документы и пр. Это означает, что в материалах уголовного дела должны содержаться сведения об

объектах, подлежащих отысканию и изъятию, а также о том, где могут находиться искомые объекты.

Процессуальный порядок производства обыска предполагает необходимость соблюдения следующих обязательных условий:

– обыск может производиться только по возбужденному уголовному делу, на основании постановления следователя или судебного решения, если обыск производится в жилище (ч. 2 и ч. 3 ст. 182 УПК РФ), или в отношении физического лица (личный обыск) (ч. 1 ст. 184 УПК РФ);

– при производстве обыска обязательно участие понятых (ч. 1 ст. 170 УПК РФ), за исключением случаев, предусмотренных ч. 3 ст. 170 УПК РФ;

– обыск проводится в дневное время, кроме случаев, не терпящих отлагательства (ч. 3 ст. 164 УПК РФ);

– при производстве обыска участвует лицо, в помещении которого производится обыск, либо совершеннолетние члены его семьи. Кроме того, при производстве обыска вправе присутствовать защитник, а также адвокат лица, в помещении которого производится обыск (ч. 11 ст. 182 УПК РФ);

– обыск осуществляет лично следователь, в производстве которого находится уголовное дело, либо сотрудники органа дознания по письменному поручению следователя;

– в необходимых случаях следователь для участия в производстве обыска привлекает соответствующего специалиста (ч. 5 ст. 164 и ч. 1 ст. 168 УПК РФ).

Успех и результативность обыска во многом зависит от соблюдения ряда принципов, или в трактовке некоторых авторов – тактических условий: законность; своевременность и внезапность; плановость; объективность, полнота и всесторонность; ситуационность; единое руководство; использование технико-криминалистических средств и помощи специалиста; соблюдение криминалистических правил обращения с объектами.

В зависимости от вида обыскиваемых объектов, характеристики искомых объектов и категории субъектов, в отношении которых осуществляется обыск, существенно отличаются организационно-

тактические, а в некоторых случаях и процессуальные особенности его проведения. В связи с этим, целесообразна дифференциация данного следственного действия.

По объектам, подлежащим обследованию, обыски подразделяются на обыски помещений, местности, автотранспорта и живого лица (личный обыск). На практике могут встречаться случаи комбинированного обыска. В свою очередь, в зависимости от размеров и назначения помещений, выделяют обыски жилища (квартир и индивидуальных жилых домовладений), служебных зданий, офисных помещений, отдельных кабинетов, складских, производственных помещений и т.д.

По количеству обыскиваемых объектов обыски дифференцируют на единичные и групповые. Групповой обыск отличается от комбинированного тем, что осуществляется на нескольких территориально не связанных между собой объектах.

По последовательности выделяют первоначальный и повторный обыск. Последний проводится при получении новых данных, ранее не известных, обуславливающих основание его проведения.

Дополнительно к классической классификации, учитывая особенности правовой регламентации условий и порядка проведения, можно выделить и некоторые специальные виды обыска, отличающиеся задачами и определенными тактико-организационными особенностями. В качестве таковых отдельно следует выделить обыск с целью обнаружения и изъятия электронных носителей информации, обыски проводимые с целью получения документов, содержащих охраняемую законом тайну, а равно обыск в отношении специальных субъектов (адвоката, судьи и т.п.).

В криминалистической литературе традиционно в структуре обыска выделяют три этапа: подготовительный, рабочий (поисковый) и заключительный. Каждый из этих этапов в свою очередь характеризуется, комплексом тактических приемов, рекомендаций, которые в своей совокупности призваны обеспечить успех данного следственного действия.

Учитывая требования своевременности и внезапности, являющиеся неотъемлемым условием для успешного, результативного обыска, его часто относят к неотложным следственным действиям. В то же время, обязательным условием эффективного обыска является его должная подготовка. Учитывая неотложность, такая подготовка должна осуществляться в достаточно сжатые сроки.

Подготовительные действия разделяют на две стадии: до выезда к месту проведения и по прибытии к объекту. Первая стадия включает: оценку следственной ситуации и определения достаточных оснований для проведения обыска, их процессуальное оформление (вынесение постановления, получение судебных решений). На этой же стадии осуществляется планирование обыска, в ходе которого определяется содержание поисковых операций; прогнозируется продолжительность и возможные меры противодействия со стороны обыскиваемого; подбирается время его проведения; состав и необходимое количество его участников, осуществляется выбор и подготовка необходимых технико-криминалистических средств, упаковочных материалов; выбор приемов проведения данного следственного действия. Целесообразно на этой стадии изучение личности обыскиваемого с целью выявления закономерностей, могущих повлиять на выбор места и содержания действий по сокрытию объекта, прогнозирования его проведения в ходе следственного действия. Также изучаются доступные сведения об объекте, подлежащем обследованию. После этого определяется содержание и последовательность мероприятий на месте обыска. Целесообразно выбрать способы прибытия на объект, позволяющие скрыть факт планируемого обыска от обыскиваемых и тем самым обеспечить внезапность его проведения.

Подготовка непосредственно перед обыском включает в себя проникновение на обыскиваемый объект; установление личности находящихся там лиц и обеспечение контроля над ними; предъявление постановления следователя или судебного решения; общий обзор подлежащих обыску объектов;

распределение обязанностей между участниками следственно-оперативной группы (инструктаж).

Рабочий (поисковый) этап начинается с предложения обыскиваемым добровольно выдать искомые объекты. Если перечисленные объекты выданы добровольно и нет оснований опасаться их сокрытия, следователь вправе не производить обыск. При этом добровольная выдача объектов не является основанием для завершения обыска. По решению следователя обыск в таком случае может быть продолжен. Далее, при необходимости, проводится личный обыск находящихся в месте его проведения лиц. После этого осуществляется общий обзор обыскиваемых площадей с одновременным сопоставлением с ранее полученной информацией об объекте, обстановки на нем, структуре и характеристиках отдельных элементов обстановки. В ситуации тождества обстановки с ранее полученной информацией, реализуются ранее запланированные приёмы поиска, при наличии расхождений – целесообразна корректировка плана. С учетом характеристик обыскиваемого объекта, особенностей искомых объектов может осуществляться сплошной или выборочный (частичный) обыск. При выполнении активных поисковых мероприятий могут применяться радиальные (концентрические и эксцентрические), линейно-фронтальные приемы, параллельное или встречное обследование, разбивка обследуемого участка на секторы. При этом могут применяться методы поиска, не вносящие изменений в обстановку, и методы разрушающего воздействия.

В качестве тактических приемов могут использоваться общие поисковые методы: простукивание, прощупывание, прокалывание предметов и деталей обстановки; методы измерений; сравнение однородных предметов (метод обнаружения неоднородностей). Кроме того, достаточно эффективными могут оказаться различные психологические приемы: наблюдение за поведением и реакцией обыскиваемого (нервозность, озабоченность, взволнованность, потливость, покраснения кожных покровов и т.д.); метод реконструкции или моделирования обстановки; убеждение. По договоренности с другими

сотрудниками, участвующими в обыске могут реализовываться иные психологические приёмы, провоцирующие обыскиваемого на проявление каких-либо реакций. При этом наблюдение за реакциями и поведением обыскиваемого должен осуществлять сотрудник, не осуществляющий поисковых действий.

Закономерно, что в ходе обыска в поле зрения лиц, осуществляющих обыск попадает большое количество объектов, относительно которых затруднительно определить их возможную относимость к расследуемому или какому-либо иному преступлению. Поэтому следователь должен обращать внимание на необычное положение предметов, нахождение их в местах, не соответствующих назначению, нетипичное количество определенных предметов, наличие на объектах нетипичных следов частых операций (например, следов частого откручивания шурупов, креплений, царапин от перемещения предметов мебели), соответствие характера предмета и способа его хранения, на поведение обыскиваемого (неоправданное беспокойство и попытки отвлечь внимание следователя от того или иного предмета), неубедительность объяснений обыскиваемого по поводу обнаруженного предмета и другие обстоятельства.

Применение поисковых криминалистических средств в совокупности с умением использовать тактические приёмы значительно увеличивает эффективность, а соответственно и результативность данного следственного действия. Поэтому следователем заблаговременно должен быть осуществлен подбор необходимых технико-криминалистических средств и обеспечено участие соответствующего специалиста. Кроме того, при обыске на территории промышленных предприятий, производственных цехов, тактически верно к обыску привлекать специалистов, ориентирующихся в особенностях организации пространства на данных территориях и могущих пояснить следователю назначение и конструкторские особенности отдельных объектов, оборудования, станков и механизмов и помочь в поиске мест возможного сокрытия искомых объектов.

Заключительная стадия представляет собой комплекс действий, выполняемых с целью изъятия искомых объектов и процессуального оформления

хода и результатов обыска. По результатам проведенного обыска, в соответствии с правилами, предусмотренными ст. 166,167,182 УПК РФ составляется соответствующий протокол, в котором отражаются: ход и результаты следственного действия, вносятся сведения о примененных технических средствах и результатах их использования. Анализ следственной практики показал, что часто лицом, проводившим обыск, в содержательной части протокола отражается только перечень обнаруженных и изымаемых объектов и место их обнаружения, а в некоторых случаях не указывается и место обнаружения. Такой подход является недопустимым. Уголовно-процессуальным законом установлено обязательное отражение в протоколе содержания процессуальных действий в том порядке, в каком они проводились, выявленных при их производстве существенных для расследуемого уголовного дела обстоятельств (ч. 4. ст. 166), а так же информации о месте и обстоятельствах обнаружения предметов, документов или ценностей с указанием их количества, меры, веса, индивидуальных признаков и по возможности стоимости (ч.13 ст.182). Кроме того, в случаях попыток уничтожить или спрятать подлежащие изъятию объекты, запись об этом также подлежит внесению в протокол с указанием принятых мер (ч.14 ст.182). Копия протокола в обязательном порядке вручается лицу, в помещении которого был произведен обыск, либо совершеннолетнему члену его семьи, а в случае обыска в помещениях организации – представителю администрации соответствующей организации.

Очевидно, что тактические и организационные особенности производства обыска значительно отличаются от характера и вида обыскиваемых объектов, категории и характеристик искомых объектов. Отдельного, более детального внимания требует рассмотрение особенностей производства обыска по делам о преступлениях в сфере информационных технологий, существенно отличающегося специфичными объектами поиска, предопределяющими целый ряд процессуальных, тактических требований и рекомендаций по поиску, фиксации и изъятию типичных для таких преступлений искомых объектов и информации на них.

2. Характеристика объектов, подлежащих обнаружению и изъятию при расследовании уголовных дел о преступлениях в сфере информационных технологий

След в преступлениях в сфере информационных технологий представляет собой преобразования объектов материальной и виртуальной природы, обусловленные приложением к этим объектам воли преступника[1].

По данному виду преступлений следовая картина весьма специфична, так как формируется как традиционными (материальными и идеальными) следами, так и электронно-цифровыми.

Идеальными следами могут быть мысленные образы, которые остаются в сознании и памяти преступника, потерпевшего, свидетелей и отображаются в протоколе следственных действий.

Материальными следами являются любые объекты материального мира, взаимодействующие на физическом или химическом уровне (в частности, следы рук, орудия преступления, микрообъекты, запаховые следы, программное обеспечение (ПО), средства компьютерной техники, средства кодирования и уничтожения информации; денежные средства, счета в банках, записные книжки) и воспринимаемые через органы чувств.

Понятие электронно-цифровых (виртуальных) следов появилось в связи с тем, что специфика информационных технологий, применяемых на разных этапах криминальной деятельности, независимо от желания пользователя приводит к возникновению информации, которая может быть использована в целях расследования преступлений[2].

---

[1] Каминский А.М. Криминалистическая категория «след преступления» в анализе правонарушений в сфере компьютерной информации // Цифровой след как объект судебной экспертизы: материалы Международной научно-практической конференции. – М.:
РГ-Пресс, 2020. – С. 89.

[2] Баев О.Я. Основы криминалистики. Курс лекций. – URL:http://www.megaeworld.com/upload/iblock/65d/pdf_bk_902_osnovy_kriminalistiki_kurs_lekciy_oleg_baevbook.a4.pdf (дата обращения: 18.09.2023).

Согласно определению, сформулированному Е.В. Смахтиным, «электронно-цифровым следом» являются любые криминалистически значимые электронно-цифровые данные, содержащиеся на материальном носителе, где они отображены в результате электромагнитных взаимодействий, или передаваемые по каналам связи посредством электромагнитных сигналов[1].

А.Г. Себякин предлагает ввести в оборот термин «следы в компьютерных системах», понимая его, по сути, как электронно-цифровой след. По мнению данного исследователя, «следы в компьютерных системах» возникают в результате взаимодействия пользователя и компьютерных систем. Это электронно-цифровой след в виде компьютерных данных, содержащих информацию о событиях (действиях), отображенных в материальной среде и значимых для данного уголовного дела[2].

Как представляется, следующую группу составляют дефиниции, раскрывающие содержание следов, именуемых виртуальными следами.

Вместе с тем ученые расходятся во мнениях относительно понятия и сущности виртуальных следов. В.А. Мещеряков определяет виртуальные следы как любую модификацию состояния автоматизированной информационной системы, связанную с событием преступления и записанное в виде компьютерной информации на материальном носителе, в том числе в электромагнитном поле.

Е.В. Придиус формулирует определение виртуального следа как любого рода изменений в состоянии автоматизированной информационной системы, появившихся в результате функционирования системы кибернетического пространства, связанных с преступлением и

---

[1] Смахтин Е.В. Цифровые технологии и криминалистика: некоторые проблемные аспекты // Российский юридический журнал. – 2018. – № 4. – С. 79.

[2] Себякин А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: дис. … канд. юрид. наук. − М., 2021. − С. 27, 46.

зафиксированных на том или ином материальном носителе в виде электронно-цифровой информации[1].

Обобщая рассмотренные точки зрения относительно сущности виртуальных следов, а также принимая во внимание правовые и технические аспекты данного вопроса, под виртуальными следами мы понимаем модификацию состояния любой информационной системы в результате совершения преступления с использованием информационно-телекоммуникационных технологий, имеющую значение для раскрытия и расследования преступлений.

Электронно-цифровые следы (см. приложение А) находятся на сервере и в компьютерных системах мошенника и его жертвы.

По нашему глубокому убеждению, при распространении компьютерных вирусных программ на серверах и интернет-сайтах, мобильных и других электронно-цифровых устройствах потерпевшего и преступника остаются электронно-цифровые следы в виде кодов таких программ, а также программных средств управления ими, отчетов и статистики антивирусного программного обеспечения.

В связи с разнообразием электронно-цифровых следов в сфере информационных технологий, нами выделяются следующие группы:

1. Сетевые виртуальные следы (сведения о сеансе связи, IP-адресные журналы регистрации провайдера в интернете, скорость передачи электронного сообщения, абонентские номера телефонов, исходящие сеансы связи, а также типы примененных протоколов и т.д.), относящиеся к пользователю и (или) его деятельности, которая подверглась преобразованию в результате воздействия электронно-цифрового устройства и проявилась в доступном для понимания человеком виде. Криминалистически значимые особенности данных следов состоят в том, что содержащаяся в них информация запрещена к распространению на территории нашей страны,

[1] Прудиус Е.В. Криминалистическая характеристика преступлений в сфере компьютерной информации // Евразийский Союз Ученых (ЕСУ). – 2017. – № 11 (44). – С. 97–98.

относится к событию преступления и касается лица, причастного к преступлению.

2. Локальные виртуальные следы (системные реестры ОС, таблицы размещения файлов FAT, NTFS и других, файлы и каталоги хранения сообщений электронной почты, файлы конфигурации программ удаленного доступа, и другие), алгоритмизированные в виде буквенно-цифрового кода и являющиеся результатом работы программного обеспечения, функционирования электронных устройств и информационных систем, благодаря которым осуществляются прием, доставка, передача, хранение и обработка электронных сообщений.

На наш взгляд, между следами обеих групп существует тесная и неразрывная взаимосвязь, в результате действия которой происходит процесс формирования сложной и целостной информационной системы, в которой наибольшую уязвимость представляет сам пользователь. Для его установления необходимо исходить из анализа пользовательских следов и обязательно учитывать алгоритмизированные следы. Лишь при соблюдении этого правила может быть точно установлен интернет-пользователь.

На этапе подключения к сети Интернет с помощью электронно-цифрового устройства образуются пользовательские следы и этому сетевому подключению присваивается IP‑адрес, который обеспечивает скрытость от пользователя, а также служит для идентификации электронно-цифрового устройства в интернете или локальной сети и имеет способность сохраняться в прежнем состоянии при переходе на другой ресурс, фиксироваться на сервере провайдера, обеспечивающего подключение, и администратора соответствующего интернет-ресурса.

Стоит учитывать, что для выполнения подобных действий кроме IP‑адреса нужны дополнительные идентификаторы, которыми являются логин (никнейм) и доменное имя.

Таким образом, можно заключить, что в сети Интернет пользователь и его компьютерное устройство оставляют следы в виде IP‑адреса, логина, доменного имени.

На машинных носителях компьютерной информации остаются электронно-цифровые следы в виде: изменений файловой структуры, системных областей носителей информации, постоянной энергонезависимой памяти; изменений настроек компьютера и отдельных компьютерных программ; нарушения работы компьютера и установленных на нем программ; воздействия на конфиденциальную компьютерную информацию и систему ее защиты; проявлений действия вредоносных компьютерных программ, в частности, видео- и аудио-эффекты, сообщения, выводимые на печатающее устройство.

В то же время, в качестве типовых объектов, подлежащих поиску и изъятию по рассматриваемым преступлениям, необходимо рассматривать сами электронные носители информации, средства компьютерной техники, телекоммуникации, которые с одной стороны являются носителями электронно-цифровых следов, а с другой – средствами, орудиями совершения преступлений.

Учитывая особенности совершения рассматриваемых преступлений, а также задачи любого расследования, следует отметить, что для установления субъекта такого преступления и доказывания его причастности, недостаточно установить с какого места и при использовании каких технических средств совершалось преступное деяние, но требуется доказать что этими средствами пользовался конкретный субъект, для чего одних только электронно-цифровых следов недостаточно. Поэтому наравне с виртуальными следами, в качестве типичных для таких преступлений необходимо рассматривать и традиционные криминалистические следы, позволяющие установить подобные факты (дактилоскопические, трасологические, биологические и т.п.).

Кроме того, поиску и изъятию в ходе обыска подлежат различные записи субъекта преступной деятельности, содержащие сведения о логинах, паролях, счетах вкладах и различных финансовых операциях (особенно с использованием электронных средств платежа), сведения о возможных соучастниках, потерпевших

или иных элементах планируемых или совершенных преступлений. Должно привлекать внимание и наличие и содержание специализированной технической литературы по направлению реализуемых преступных схем.

Итак, можно сделать следующие выводы:

1. След в преступлениях в сфере информационных технологий представляет собой преобразования объектов материальной и виртуальной природы, обусловленные приложением к этим объектам воли преступника. Следовая картина по данным преступлениям весьма специфична, так как формируется не только традиционными (материальными и идеальными) следами, но и электронно-цифровыми следами.

2. Типичными для исследуемых преступлений являются электронно-цифровые следы, которые образуются в процессе взаимодействия информационных объектов, не имеющих формы, в электронно-цифровой среде. Понятие «электронно-цифровые следы» означает криминалистически значимую компьютерную информацию о событиях (действиях), отображенных посредством электромагнитных взаимодействий в материальной среде в связи с ее возникновением, обработкой, хранением и передачей в телекоммуникационной сети, или передаваемые по каналам связи с помощью электромагнитных сигналов. Данная разновидность следов весьма разнообразна. Это, например, коды вредоносных компьютерных программ, программные средства управления ими, отчеты и статистика антивирусного программного обеспечения, файлы и каталоги хранения сообщений электронной почты, файлы конфигурации программ удаленного доступа.

3. Тактика подготовки и проведения обыска при расследовании уголовных дел о преступлениях в сфере информационных технологий

С позиций криминалистики производство обыска по делам о преступлениях в сфере информационных технологий имеет определенную специфику в части его организации и непосредственной работы с отыскиваемыми и изымаемыми объектами, содержащими электронно-цифровые следы.

Только качественная подготовка и планирование обыска позволит обеспечить сохранность криминалистически значимой информации и следов, а также предотвратить их уничтожение или повреждение.

На этапе подготовки следователь выполняет определенные действия, которые должны иметь оптимальную последовательность:

1. Изучить исходную информацию (материалы уголовного дела), в частности показания свидетеля, протокол осмотра места происшествия, результаты оперативно-розыскной деятельности. Основываясь на результатах изученной информации, следует выяснить, на каких материальных носителях она может быть обнаружена и какие компьютерные устройства, относящиеся к расследуемому преступлению, могут находиться в месте обыска.

2. Определить цели и задачи обыска.

3. Определить время, место и границы производства обысков, а также меры по обеспечению конфиденциальности. В первую очередь, необходимо определить время и место проведения обыска, чтобы обеспечить внезапность для подозреваемых и иных лиц, которые могут оказаться на месте проведения данного следственного действия.

4. Собрать полную информацию о месте проведения обыска (точный адрес; особенности строения; планировка помещений; наличие и характеристики телефонной связи, работающие модемы; наличие в

комплекте к компьютерной технике устройства автономного питания, последствия возможного отключения электроэнергии; локальная (глобальная) сеть; наличие Wi-Fi; место нахождения источников питания; место прокладки телекоммуникационных кабелей; наличие систем защиты компьютерной информации и шифрования, их типы и особенности; возможность установки на компьютере программы экстренного (в том числе, удаленного) уничтожения компьютерной информации).

5. Изучить личность обыскиваемого владельца средства компьютерной техники. Получение данной информации может стать определяющим фактором в том случае, когда лица обыскиваемого объекта являются оператором (сотрудником) учреждения, предоставляющего телекоммуникационные услуги, провайдером интернет-услуг, системным администратором, специалистом по обслуживанию компьютерных сетей. Обладание такой информацией позволит следователю правильно выбрать тактические приемы обыска и позволит предугадать вероятное противодействие обыскиваемого в месте проведения обыска.

6. Подготовить материально-техническое обеспечение. Эта мера должна быть согласована со специалистами, участвующими в обыске. Также очень важной является подготовка техники для считывания и хранения информации, изъятой в ходе обыска. Так, при обыске может оказаться полезным материально-техническое обеспечение (см. приложение В).

7. Обозначить состав участников обыска. По нашему мнению, приглашение специалиста-программиста для производства обыска необходимо в связи с тем, что он сможет профессионально и грамотно извлечь необходимую компьютерную информацию (базы данных), расшифровать файлы, обнаружить и извлечь иные электронно-цифровые следы. Для участия в обыске, исходя из конкретных обстоятельств расследуемого преступления (способа совершения и др.), могут привлекаться следующие специалисты: программисты по операционным системам и

прикладным программам; специалисты по средствам связи и телекоммуникациям; специалисты по сетевым технологиям и другие.

При расследовании преступлений, совершенных с использованием информационных технологий, понятые являются обязательными участниками обыска, поскольку согласно ч. 2 ст 164.1 УПК РФ копирование информации с изымаемых электронных носителей осуществляется только в присутствии понятых, которых следует подбирать с учетом их общих навыков работы с компьютерной техникой и телекоммуникационными сетями. Понятыми, например, в данном случае могут быть выбраны студенты факультетов компьютерной инженерии.

До начала обыска следователь должен инструктировать оперативных сотрудников о недопустимости лиц к различным манипуляциям с компьютером.

Для организации точки подключения компьютеров к широкополосному каналу доступа к интернету сегодня широко используются радиоканалы для создания локальных компьютерных сетей, подключения различных электронно-цифровых устройств, в связи с чем также необходимо выяснить топологии сетей, использующих подключение по радиоканалу, и установить места расположения серверного и коммутационного оборудования.

По завершении подготовки следователь незамедлительно приступает к рабочему этапу производства обыска, в процессе которого может быть получена криминалистически значимая информация, включая компьютерную информацию.

Производство поисковых мероприятий на основном этапе обыска подразделяется на две стадии: начальную (обзорную) и поисковую (детальную).

Предлагаем рассмотреть алгоритм действий следователя на обзорной стадии обыска:

1. Прибыв на место проведения обыска, следователю необходимо собрать всех лиц, находящихся в обыскиваемом помещении в одном месте.

Не допускать лиц, находящихся в обыскиваемом помещении, к носителям компьютерной информации, средствам компьютерной техники, а также телекоммуникационным сетям; запретить включать и выключать энергопитание; пресекать все попытки любых манипуляций с компьютерными устройствами. Случаи несоблюдения данных действий должны расцениваться как попытки уничтожить доказательства и отражаться в протоколе.

2. Осуществить обзорную фото- и видеосъемку помещения, в котором будет производиться обыск, и находящиеся в нем средства компьютерной техники.

3. Произвести предварительный осмотр всего обыскиваемого помещения. В ходе осмотра помещения свои усилия следует направлять на поиск портативных электронных устройств памяти, поскольку искомым объектом выступает компьютерная информация.

4. Необходимо определить, связаны ли компьютеры в локальной сети с другими компьютерами и подключены ли они к другим телекоммуникационным сетям.

При проведении обыска в помещении рекомендуется использовать тактический прием «от центра к периферии», который означает, что следователь будет перемещаться по разворачивающейся спирали. В данном случае «центром» выступает компьютер, который использовался для совершения преступления. В ситуации при обнаружении нескольких компьютерных устройств, объединенных телекоммуникационной сетью различного уровня, при наличии специалиста необходимо определить, является ли один из них управляющим (базовым), то есть сервером, и начать обыск с него.

5. Необходимо проверить со специалистом компьютер на наличие средств защиты информации, вирусных программ, а также программ удаленного доступа. При производстве обыска важно отключить специальные функции, которые могут автоматически уничтожить

информацию. Также следует заблокировать возможность удаленного управления компьютером, поскольку через такой доступ можно совершить различные действия, включая уничтожение информации. Например, используя программу LiteManager Pro можно удаленно управлять питанием компьютера, включая его и выключая, перезагружая или включая «спящий» режим. Кроме прочего, с помощью данной программы злоумышленник также может управлять рабочим столом компьютера, запускать различные программы, блокировать доступ к клавиатуре и управлять файловой системой.

6. При осмотре компьютерного устройства необходимо определить, какая операционная система установлена на нем, какие операции были выполнены и какие программы в данный момент выполняются, начиная с момента включения компьютера (если он был включен).

7. Обратиться к специалисту для оперативного отключения компьютера от сетей с целью предотвращения удаленного уничтожения или изменения компьютерной информации, а также предварительно (при возможности) определить участки компьютерной сети, где может храниться электронные доказательства, и контролировать их до окончания обыска.

На начальной стадии рабочего этапа обыска, с целью обнаружения и изъятия носителей компьютерной информации и содержащихся на них данных, следователю необходимо, по нашему мнению, выполнить следующие тактические рекомендации:

1. Уточнить цели и задачи обыска, чтобы довести их до всех участников поиска следов преступления.

2. Принять решение о том, какие объекты могут быть обследованы самостоятельно, а для каких целесообразно привлечь специалистов.

3. Обнаружить и отключить средства защиты компьютерной информации и компьютерной техники, чтобы предотвратить несанкционированный доступ.

4. Проверить, существует ли связь между системой компьютерной техники и каналами электросвязи.

5. Создать подходящие условия для эффективного поиска носителей компьютерной информации, включая оптимальное освещение и другие необходимые условия.

После этого необходимо приступить к детальной стадии обыска, которая наиболее трудоёмка.

Нами предлагается алгоритм действий следователя при обыске работающего компьютера на детальной стадии при расследовании преступлений в исследуемой сфере:

1. Определить программу уничтожения компьютерной информации, остановить ее и начать обыск именно с этого компьютера.

2. Войти в операционную систему и определить последнюю запущенную программу.

3. Проверить наличие внешних устройств компьютера, подключив накопители информации на жестких дисках и внешние устройства удаленного доступа.

4. Отсоединить компьютер от источника питания.

5. При помощи специалиста осуществить поиск необходимой информации в компьютерном устройстве, которая может находиться на жестком диске и в оперативной памяти.

6. Скопировать программы и файлы на носитель информации и отразить это в протоколе следственного действия.

7. По завершении обыска выключить компьютер, упаковать его и изъять.

Алгоритм действий следователя при обыске неработающего компьютерного оборудования следующий:

1. Зафиксировать местоположение компьютера и его периферийных устройств (если они есть).

2. Отразить характеристики компьютерного устройства, такие как серийный номер, название, наличие и типы сетевых карт, разъемов, дисководов и т. д.

3. Найти и зафиксировать соединения компьютера с телекоммуникационными сетями, периферийным оборудованием и другими устройствами.

4. Провести поиск и зафиксировать следы преступления на компьютере, его устройствах, рабочем месте и других местах, включая служебные помещения и квартиру. Важно отметить, что обнаружение и изъятие традиционных следов (записи кодов и паролей доступа; записные книжки с именами соучастников, номерами телефонов, банковских счетов, ПИН-кодами банковских платежных карт; распечатки с принтера; устройства доступа в компьютерные сети) во время обыска имеет большое значение.

Если компьютером воспользовалось постороннее лицо, следователю следует сконцентрировать усилия на поиске отпечатков пальцев на клавиатуре, мониторе и системном блоке. Если требуется доступ к информационным данным, компьютер необходимо включить и скопировать эти сведения. После этого нужно отключить устройства от компьютера и приготовить их к упаковке и изъятию.

Из-за важности детальной стадии обыска следователю рекомендуется использовать подходящие тактические приемы для обнаружения и изъятия электронных носителей информации.

Так, на детальной стадии обыска следователь руководствуется определенными методами и приемами поиска электронных носителей информации. Эти действия включают последовательный или выборочный поиск в зависимости от объема объектов, которые подлежат обыску. При выборочном поиске осуществляется обследование наиболее вероятных мест, где могут находиться искомые объекты.

На этапе проведения обыска в помещении рекомендуется тактически организовать поиск, исходя из направления движения поисковых групп:

встречное и параллельное. Параллельный поиск может быть проведен одновременно в нескольких кабинетах. Особенно целесообразно проводить параллельный поиск в помещении, где находятся несколько персональных компьютеров и серверный компьютер. В этом случае одна группа проводит обыск отдельно стоящих компьютеров, а другая группа – серверного компьютера.

При проведении обыска существует возможность либо нарушить целостность объекта, либо выполнить обыск без такого нарушения. Если требуется изъятие внутреннего жесткого диска, но системный блок защищен от несанкционированного доступа (например, имеется замок на крышке системного блока), то необходимо предпринять действия для поиска ключа от такого замка. В случае, если ключ не может быть найден, и пользователь (собственник) ПК отказывается открыть замок, для изъятия жесткого диска потребуется нарушить целостность замка.

Для обнаружения и раскрытия объектов, включая те, которые могут быть скрыты, следователю рекомендуется использовать специальные тактические приемы. Эффективными тактическими приемами являются «поиск с использованием специальных устройств», «сравнение аналогичных объектов» и «наблюдение за поведением лица, в помещении которого был проведен обыск». Последний метод позволяет определить направление дальнейших поисковых действий. Например, следователь может приближаться или отдаляться от места, где предположительно находится искомый объект, и при этом скрытно наблюдать за реакцией обыскиваемого лица.

Один из дополнительных способов тактического подхода состоит в предложении обыскиваемому указать, откуда следует начать поиск электронных носителей. В этот момент следователь скрытно наблюдает за обыскиваемым, стараясь заметить его реакцию.

Эти приемы обыска направлены на установление психологического контакта с обыскиваемым. Для этого необходимо поддерживать постоянную

беседу с ним о расположении помещений, наличии информационных технологий и используемых программ. Если помещений много, рекомендуется составить схему, включающую последовательность обследования объектов и информацию о сотрудниках, проводивших обыск. Такая схема позволит оценить эффективность следственных действий, а также спланировать последующие оперативно-розыскные мероприятия.

На завершающей стадии обыска следователю рекомендуется придерживаться следующих тактических рекомендаций для выполнения алгоритма действий:

1. Во взаимодействии со специалистом определить носители компьютерной информации.

2. Подготовить к изъятию системы компьютерной техники, завершив работу компьютерной системы, отключив компьютер от источника питания, выполнив маркировку компьютера, прикрепив липкие листы или ленты с указанием даты и подписями участников обыска, а также осуществив фото- или видеозапись положения кабелей перед их отсоединением. Далее запломбировать корпус компьютера, отсоединив устройства системы компьютерной техники и упаковав их отдельно, указав места их обнаружения на упаковке для съемных машинных носителей.

3. Составить протокол следственного действия, в котором следует внести информацию, полученную в процессе обыска, включая все действия специалиста, которые были выполнены.

К протоколу обыска прилагаются приложения, включающие планы и схемы обыскиваемых помещений, а также средства компьютерной техники, которые находятся в них. В дополнение к этому, к протоколу прикладываются кассеты с видеозаписями следственного действия и фототаблицы.

По завершении обыска все изъятые средства компьютерной техники, содержащие искомую криминалистически значимую информацию, должны быть правильно упакованы и запечатаны.

ЗАКЛЮЧЕНИЕ

В результате проведённого исследования были решены поставленные задачи, по существу представленной работы сформулированы выводы, приведённые ниже:

1. След в преступлениях в сфере информационных технологий представляет собой преобразования объектов материальной и виртуальной природы, обусловленные приложением к этим объектам воли преступника. Следовая картина по данным преступлениям весьма специфична, так как формируется не только традиционными (материальными и идеальными) следами, но и электронно-цифровыми следами.

2. Типичными для исследуемых преступлений являются электронно-цифровые следы, которые образуются в процессе взаимодействия информационных объектов, не имеющих формы, в электронно-цифровой среде. Понятие «электронно-цифровые следы» означает криминалистически значимую компьютерную информацию о событиях (действиях), отображенных посредством электромагнитных взаимодействий в материальной среде в связи с ее возникновением, обработкой, хранением и передачей в телекоммуникационной сети, или передаваемые по каналам связи с помощью электромагнитных сигналов. Данная разновидность следов весьма разнообразна. Это, например, коды вредоносных компьютерных программ, программные средства управления ими, отчеты и статистика антивирусного ПО, файлы и каталоги хранения сообщений электронной почты, файлы конфигурации программ удаленного доступа.

3. Подготовку к обыску по делам о преступлениях в сфере информационных технологий целесообразно проводить с учетом следующих рекомендаций, отражающих специфику данного следственного действия:

− изучить исходную информацию (материалы уголовного дела);

− определить цели и задач обыска;

− определить время, место и границы производства обыска, а также меры по обеспечению конфиденциальности;

− собрать полную информацию о месте проведения обыска;

− изучить личность обыскиваемого владельца средства компьютерной техники.;

− подготовить необходимое материально-техническое обеспечение.

− обозначить состав участников обыска.

4. Рабочий этап обыска подразделяется на начальную (обзорную) стадию и поисковую (детальную) стадию. На обзорной стадии следователю целесообразно, в частности:

– Собрать всех лиц, находящихся в обыскиваемом помещении в одном месте.

– Осуществить обзорную фото- и видеосъемку помещения, в котором будет производиться обыск, и находящиеся в нем средства компьютерной техники.

– Произвести предварительный осмотр всего обыскиваемого помещения.

– Определить, связаны ли компьютеры в локальной сети с другими компьютерами и подключены ли они к другим телекоммуникационным сетям.

– Необходимо проверить со специалистом компьютер на наличие средств защиты информации, вирусных программ, а также программ удаленного доступа.

– При осмотре компьютерного устройства необходимо определить, какая операционная система установлена на нем, какие операции были выполнены и какие программы в данный момент выполняются, начиная с момента включения компьютера (если он был включен).

– Принять меры по обеспечению сохранности компьютерной информации.

5. На поисковой стадии обыска тактика выстраивается в зависимости от состояния компьютера (работающий или неработающий).

В ситуации работающего компьютерного устройства целесообразно: определить вид выполняемой программы, наличие внешних устройств; обесточить компьютер; выполнить с помощью специалиста поиск в компьютерном устройстве искомой информации; скопировать программы и файлы на машинный носитель; выключить устройство, упаковать и изъять.

В ситуации неработающего компьютера: зафиксировать месторасположение компьютера и его периферийных устройств; отразить его характеристики; выявить и зафиксировать соединения системы компьютерных технологий с телекоммуникационными сетями, периферийным оборудованием, другими устройствами; выполнить поиск и фиксацию следов преступления на компьютере и т.д.

6. На заключительном этапе обыска следует: определить носители информации, подлежащие изъятию; подготовить аппаратные средства для их изъятия; изъять эти носители; оформить протокол обыска. В виде приложений к протоколу обыска следует приложить планы и схемы обыскиваемых помещений и расположенных в них систем компьютерных технологий, а также видеозаписи проведения обыска и фототаблицы. Все обнаруженные системы компьютерных технологий, содержащие искомую информацию, до изъятия необходимо правильно упаковать и опечатать.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 25.03.2022) // Собрание законодательства РФ. − 1996. − № 25. − Ст. 2954.

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 25.03.2022, с изм. от 19.04.2022) // Собрание законодательства РФ. – 2001. – № 52. – Ст. 4921.

4. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3448.

Литературные источники

1. Каминский А.М. Криминалистическая категория «след преступления» в анализе правонарушений в сфере компьютерной информации // Цифровой след как объект судебной экспертизы : материалы Международной научно-практической конференции. – Москва : РГ-Пресс, 2020. – С. 89.

2. Баев О.Я. Основы криминалистики. Курс лекций. – URL: http://www.megaeworld.com/upload/iblock/65d/pdf_bk_902_osnovy_kriminalistiki_kurs_lekciy_oleg_baevbook.a4.pdf (дата обращения: 18.09.2023).

3. Смахтин Е.В. Цифровые технологии и криминалистика: некоторые проблемные аспекты // Российский юридический журнал. – 2018. – № 4. – С. 79.

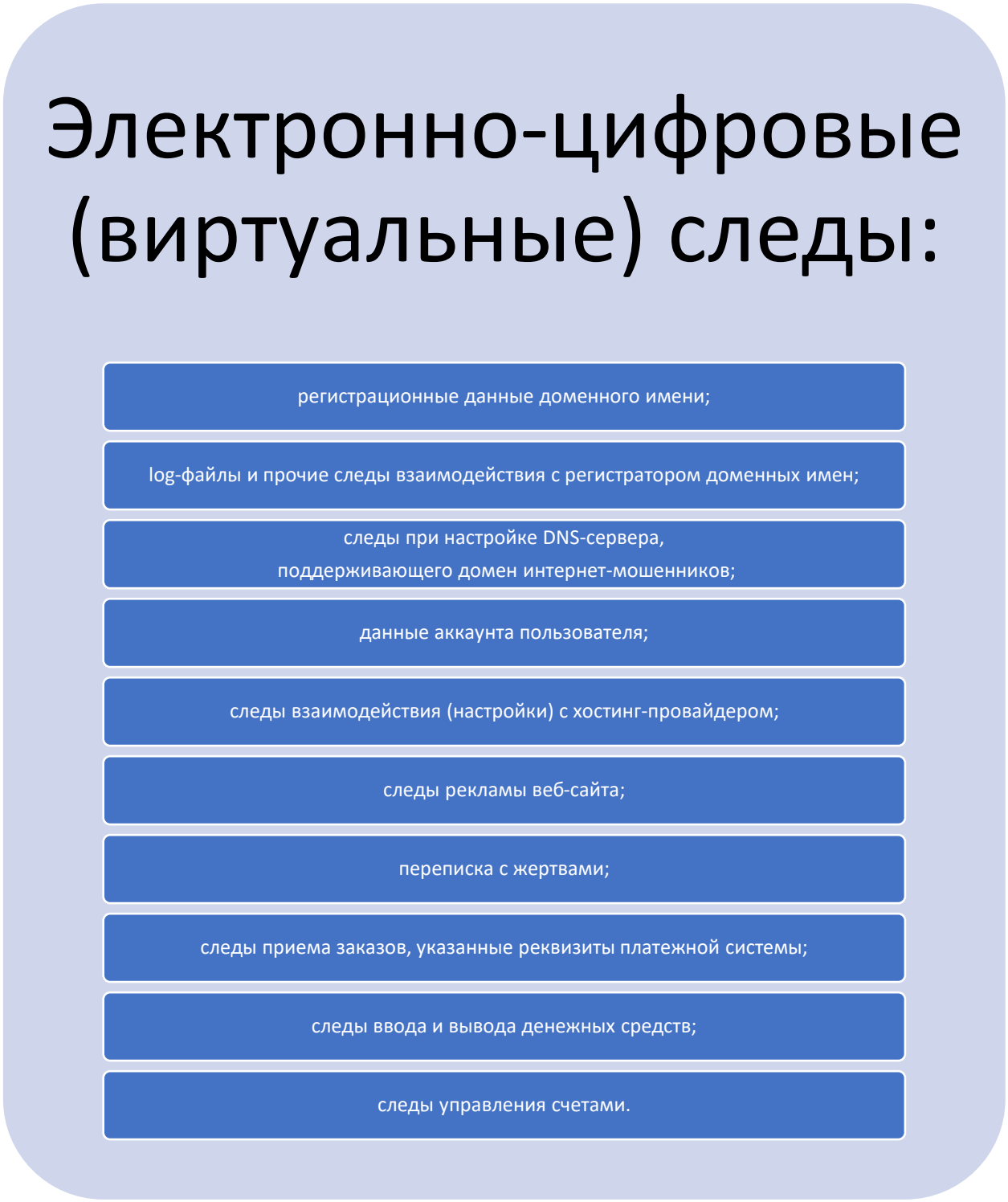
4. Себякин А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации : дис. … канд. юрид. наук. − Москва, 2021. − С. 27, 46.

5. Прудиус Е.В. Криминалистическая характеристика преступлений в сфере компьютерной информации // Евразийский Союз Ученых. − 2017. − № 11 (44). − С. 97−98.

ПРИЛОЖЕНИЕ А

(обязательное)

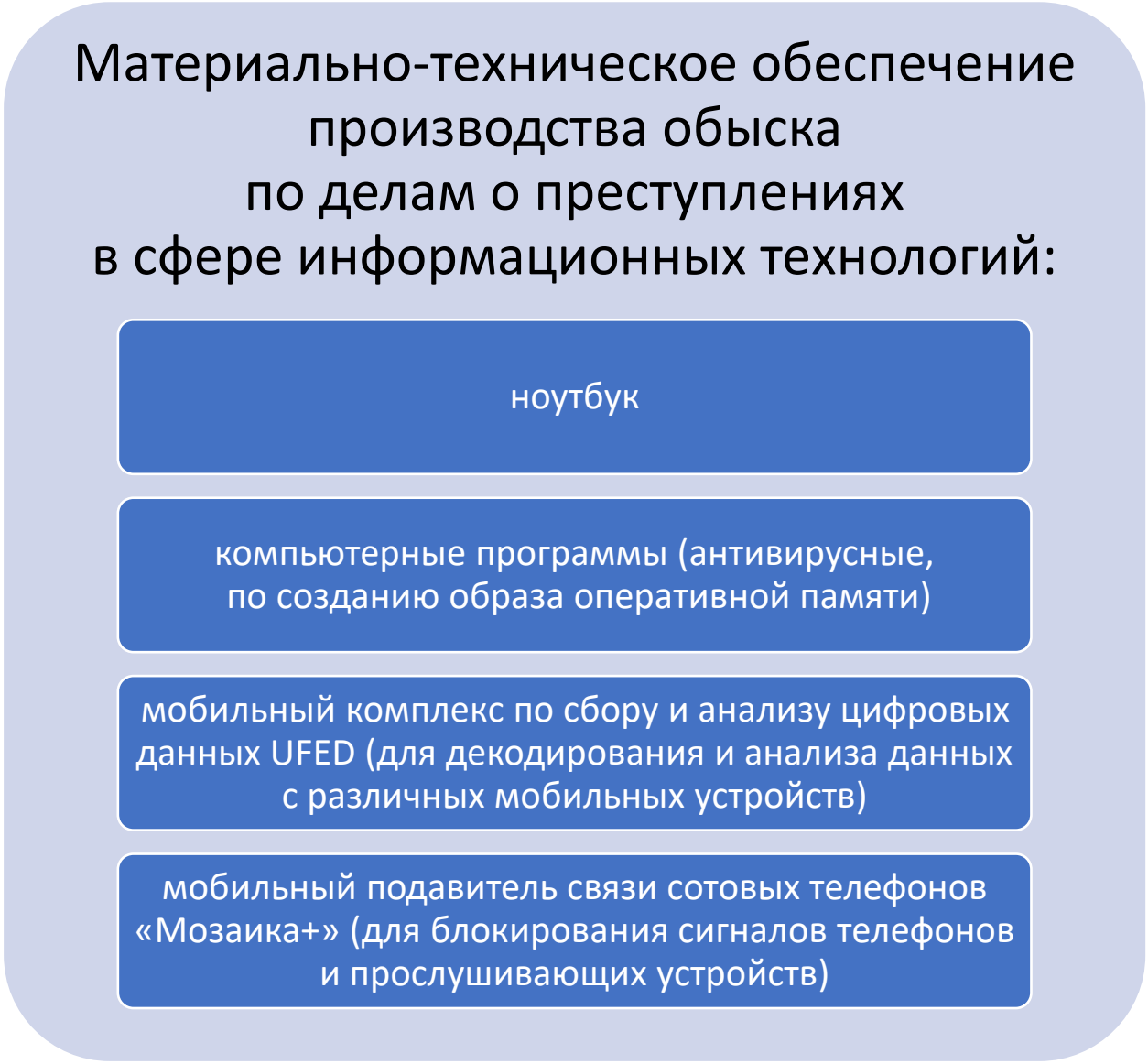
Виды электронно-цифровых (виртуальных) следов



ПРИЛОЖЕНИЕ Б

(справочное)

Материально-техническое обеспечение производства обыска по делам о преступлениях в сфере информационных технологий



ГЛОССАРИЙ

Компьютерная информация – сведения, сообщения или данные, которые представлены в форме электрических сигналов, независимо от способов их хранения, обработки и передачи.

IP-адрес – это идентификатор, с помощью которого может передаваться информация между электронно-цифровыми устройствами в сети.

Домен – это определенная буквенная последовательность, обозначающая имя сайта или используемая в именах электронных почтовых ящиков

Логин – имя (идентификатор) учётной записи (аккаунта) пользователя, которое используется, например, для входа на сайт (форум).

Обыск – следственное действие, направленное на принудительное обследование помещений, сооружений и других объектов или лиц в целях обнаружения и изъятия объектов, могущих иметь значение для уголовного дела.