

електрикою; 7) комп'ютерної техніки – для отримання оперативної інформації з електронних записів, повідомлень, пошти про останні зв'язки загиблої особи, мету спілкування з іншими особами, плани й наміри, встановлення фактів знищення певної інформації та її відновлення.

Попередні висновки, зроблені спеціалістом в процесі огляду місця події, є неостаточними та доказового значення мати не можуть. У той самий час вони відіграють важливу орієнтуючу роль, про що неодноразово наголошували науковці¹. Такі висновки можуть бути покладені в основу побудови версій як обґрунтованих припущень, більшість з яких може бути перевірена (спростована чи відкоректована) у короткий час при триваючому огляді місця події. Версії, висунуті спеціалістом, можуть стосуватися не тільки обставин події злочину (кількості злочинців, характеристики особи-вбивці, часу, місця, способу, механізму, знарядь, мотивів вбивства, способу його приховування), а й характеру зв'язку певних слідів і об'єктів з цією подією та можливостей їх використання у подальшому розслідуванні (у зв'язку з цим спеціаліст визначає, що саме, у якому обсязі та яким чином повинно бути зафіксовано, які питання це надасть можливість вирішити в подальшому).

Викладене дає підстави визначити місце спеціаліста у пізнавальному процесі, який відбувається під час огляду місця події, розглядаючи цю особу як активного суб'єкта, що на підставі своїх спеціальних знань і навичок аналізує обстановку місця події й оцінює наявну інформацію з точки зору її відношення до злочину. Попередні висновки та припущення спеціалістів у процесі огляду місця події є важливим джерелом висунення слідчих версій на початковому етапі розслідування злочинів. Під час організації проведення оглядів місця події при розслідуванні вбивств слідчі мають ураховувати можливості використання типових видів спеціальних знань.

И. П. Пономарев, аспірант кафедри криміналістики юридического факультета Воронежского государственного университета

ТАКТИКА ДОПРОСА ЛИЦА, ССЫЛАЮЩЕГОСЯ НА «ЦИФРОВОЕ АЛИБИ»

Розвиток засобів обчислювальної техніки зумовив появу в практиці кримінального судочинства ситуацій, коли підозрювані (обвинувачувані) в обґрунтування свого алібі посилаються на те, що в момент вчинення злочину вони працю-

¹ Див.: *Быховский И. Е.* Вказ. праця. — С. 30; *Войтович Е. М.* Предварительный анализ и доэкспертные исследования вещественных доказательств / *Е. М. Войтович* // *Держава і право* : зб. наук. пр. : юрид. і політ. науки. — К. : ІДП НАН України, 2001. — Вип. 11. — С. 496–500; *Селиванов Н. А.* Вказ. праця. — С. 125.

вали на персональному комп'ютері, який перебував в іншому місці. Перевірка такого алибі безпосередньо пов'язана із проведенням допиту підозрюваного (обвинувачуваного), оскільки одержані в його ході відомості слугують найважливішим джерелом інформації, необхідної для пошуку інших доказів.

Развитие средств вычислительной техники обусловило появление в практике уголовного судопроизводства ситуаций, когда подозреваемые (обвиняемые) в обоснование своего алиби ссылаются на то, что в момент совершения преступления они работали на персональном компьютере, находившемся в другом месте. Проверка такого алиби непосредственно связана с проведением допроса подозреваемого (обвиняемого), поскольку полученные в его ходе сведения служат важнейшим источником информации, необходимой для поиска других доказательств.

Практика уголовного судопроизводства последних лет убедительно показывает, что все чаще подозреваемые (обвиняемые) в обоснование заявляемого ими алиби ссылаются на то, что в момент совершения преступления они работали на персональном компьютере, находившемся в другом месте. За рубежом такие объяснения получили, на наш взгляд, вполне удачное название – «цифровое алиби» (digital alibi), ибо источником формирования доказательств выступает информация, записанная в цифровой форме на машинных носителях¹. Проверка такого алиби, подчиняясь хорошо известным и достаточно подробно разработанным в криминалистической литературе принципам и приемам проведения этой тактической операции², без сомнений, имеет определенную специфику. Это в первую очередь касается тактики допроса лица, заявившего о наличии у него «цифрового алиби», проблемам которой и посвящена данная публикация.

Особое значение для допроса лица, заявившего «цифровое алиби», имеет его *подготовительный этап*. На нем с учетом того, что большая часть информации, относящейся к предмету предстоящего допроса носит специфический характер, следовательно необходимо уяснить для себя ряд достаточно сложных вопросов, касающихся общих принципов формирования следов работы пользователя с компьютерным объектом. В этих целях наиболее эффективными будут консультации специалиста.

Следователь совместно со специалистом в каждом конкретном случае должен сформулировать вопросы, относительно работы подозреваемого (обвиняемого) на компьютерной технике в момент, зафиксированный как время совершения преступления. В частности, из ответов на них следователь должен получить сведения о следующих обстоятельствах:

¹ См.: Иванов Н. А. Применение специальных познаний при проверке «цифрового алиби» [Электронный ресурс]. — Режим доступа : <http://www.infolaw.ru/lib/2006-4-digital-alibi-expertise>. — 27.02.2009.

² См.: Кручинина Н. В. Тактическая операция «Проверка алиби» : метод. указания / Н. В. Кручинина, В. И. Шиканов. — Иркутск : Изд-во Иркут. гос. ун-та, 1989. — 18 с.

- на каком именно компьютере он работал, его местоположение, конфигурация и технические характеристики;
- вид и последовательность действий, выполнявшихся подозреваемым (обвиняемым) в день расследуемого события на указанном компьютере;
- какое именно программное и аппаратное обеспечение при этом использовалось;
- какие файлы (текстовые документы, электронные таблицы и т. д.) открывались, редактировались, удалялись допрашиваемым в день расследуемого события;
- было ли во время работы подключение к сети (локальной, глобальной);
- пользовалось ли при этом лицо средствами компьютерной коммуникации – электронной почтой, системами обмена мгновенными сообщениями и т. д., с какими лицами через них контактировало;
- не повлияло ли время, прошедшее после расследуемого события, на точность сообщаемой допрашиваемым информации;
- какие лица, кроме подозреваемого (обвиняемого), имеют доступ к указанному компьютеру;
- имеются ли на компьютере какие-либо средства защиты от несанкционированного доступа;
- каковы уровень профессиональных навыков и опыт работы допрашиваемого на компьютерной технике.

Следователь может привлечь специалиста и для непосредственного участия в допросе, в ходе которого он может давать следователю пояснения, помочь выявить обстоятельства, связанные с обнаружением, закреплением и изъятием доказательств, правильно сформулировать вопросы на основании той информации, которая появляется в ходе допроса, а также обратить внимание на те обстоятельства, которые допрашиваемый пытается умышленно или по незнанию исказить¹.

Однако, привлекая специалиста к участию в том или ином следственном действии, следователь должен убедиться в его компетентности. Учитывая многообразие компьютерных систем и программных продуктов, обладание в полной мере знаниями о них тем или иным лицом практически невозможно, поэтому можно говорить лишь о специалисте, компетентном в конкретной области компьютерных технологий. Таким образом, следователь должен определить необходимый профиль знаний специалиста².

Не менее важным для проверки «цифрового алиби» является получение данных о наличии у подозреваемого (обвиняемого) специальных и

¹ См.: *Краснова Л. Б.* Компьютерные объекты в уголовном процессе и криминалистике : учеб. пособ. / Л. Б. Краснова ; науч. ред. В. А. Мещеряков. — Воронеж : Изд-во Воронеж. гос. ун-та, 2006. — С. 114.

² См.: *Кукарникова Т. Э.* Электронный документ в уголовном процессе и криминалистике / Т. Э. Кукарникова. — Воронеж : Изд-во Воронеж. гос. ун-та, 2005. — С. 73–74.

профессиональных навыков владения компьютерной техникой. Представление о квалификации допрашиваемого способствует правильной оценке его показаний и в дальнейшем – решению вопроса о возможности совершения им тех или иных действий с помощью компьютерных объектов, в том числе возможности фальсификации следов работы на компьютере во время совершения преступления. Такую информацию можно получить из бесед с руководством допрашиваемого, его сослуживцами. Также представление о навыках обращения с компьютерной техникой дают факт окончания специального учебного заведения, полученные оценки по предметам, касающимся функционирования и эксплуатации компьютерных объектов, стаж работы по специальности, наличие поощрений и порицаний, оценка коллег по работе относительно опыта и познаний допрашиваемого, наличие хобби в компьютерной сфере и т. д.¹

Заметим, что дополнительные возможности изучения личности человека может предоставить компьютерная сеть Интернет. В настоящее время большой популярностью пользуются так называемые социальные сети – веб-сайты с возможностью указать какую-либо информацию о себе (т. е. зарегистрироваться, указав дату рождения, школу, вуз, любимые занятия и др.). По этой учетной записи («аккаунта» – на «компьютерном жаргоне») его смогут найти иные пользователи² в целях личного общения и создания групп «по интересам». В нашей стране «наибольшим спросом» пользуются сайты «В контакте» (<http://vkontakte.ru>) и «Одноклассники» (<http://odnoklassniki.ru>).

Во время процесса регистрации либо сразу после его окончания пользователю предлагается ввести анкетные данные – имя, фамилию, отчество, псевдоним («ник»), пол, дату рождения, вероисповедание, домашний адрес, телефон, адреса электронной почты, сведения о местах работы и учебы, семье, круге интересов, политических предпочтениях, наиболее часто посещаемых местах (кафе, магазинах) и т. д. Все эти сведения используются при осуществлении поисковых и других функций «социальных сетей». Информация такой «анкеты» сохраняется в базе данных сайта и отображается на персональной странице, зачастую являясь доступной для других пользователей.

Несомненно, эта информация о лице, заявившем «цифровое алиби», может быть использована в криминалистических целях как для составления «личностного портрета», так и для установления иных сведений (адресов электронной почты, номеров телефонов), а так называемый концепт «друзей» и возможность создания сообществ в «социальных сетях» позволяют определить круг знакомств лица, а нередко и характер взаимоотношений. Как уже отмечалось, рассмотренная информация в большинстве случаев находится в свободном доступе, а это означает, что ее использование

¹ См.: Краснова Л. Б. Указ. работа. — С. 113.

² См.: Википедия. Социальная сеть (интернет) [Электронный ресурс]. — Режим доступа : [http://ru.wikipedia.org/wiki/Социальная_сеть_\(Интернет\)](http://ru.wikipedia.org/wiki/Социальная_сеть_(Интернет)). — 27.02.2009.

правоохранительными органами не требует получения на то судебного решения.

Кроме того (что очевидно), на подготовительном этапе допроса составляется план, содержащий, в частности, перечень обстоятельств, на установление которых направлен допрос, последовательность их выяснения, последовательность предъявления доказательств, определяются время и место допроса, подготавливается его обстановка.

Заметим, что многие пользователи компьютеров в своей речи используют весьма специфический сленг, или, как его часто называют, «компьютерный жаргон», а также техническую терминологию. Это вполне очевидно может вызвать некоторые трудности при производстве их допроса. Во-первых, уверенно допрашивать лиц, обладающих теми или иными навыками, можно лишь понимая их слова, выражения, наименования действий и процессов, отчего всецело зависит эффективность рассматриваемого следственного действия. Во-вторых, при составлении протокола необходимо придерживаться принципа информационного единства, сущность которого сводится к требованию использовать в процессуальных документах строго унифицированную и однозначно трактуемую терминологию, понятную всем участникам уголовного судопроизводства. Поэтому, готовясь к допросу, необходимо, насколько это возможно, ознакомиться со специальной литературой, в том числе словарями «компьютерного жаргона»¹. Не лишними в этой связи будут уже упомянутое получение соответствующей консультации у специалиста, а также привлечение его к участию в рассматриваемом следственном действии. Кроме того, уже в ходе допроса весьма важным является выяснение следователем того, что подозреваемый (обвиняемый) подразумевает под тем или иным употребляемым им в показаниях словом, термином, понятием, о чем следует дать соответствующие пояснения в протоколе. Если данные слова без ущерба для точности и однозначности протокола могут быть заменены общеизвестными, то использовать их нецелесообразно.

На *рабочем этапе* в первую очередь выясняется (диагностируется) информационное состояние допрашиваемого, с которым в криминалистической литературе обоснованно связывают тактику допроса. Так, любое лицо, вызванное следователем на допрос, относительно искомой информации может пребывать в одном из следующих состояний:

- 1) допрашиваемый обладает искомой информацией, может и желает объективно и полно передать ее следователю;
- 2) допрашиваемый обладает искомой информацией, желает объективно и полно передать ее следователю, однако мог воспринять ее с неумышленными искажениями или также неумышленно исказить ее, передавая следователю;
- 3) допрашиваемый обладает искомой информацией, но умышленно скрывает или искажает ее;

¹ См., напр.: Мещеряков В. А. Словарь компьютерного жаргона / В. А. Мещеряков. — Воронеж : Изд-во Воронеж. гос. ун-та, 1999. — 120 с.

4) лицо не обладает искомой информацией, но следователь ошибочно полагает, что допрашиваемый умышленно скрывает ее¹. Кроме того, следователь может ошибочно полагать, что допрашиваемый не только скрывает, но и выдает ложную информацию, которая в действительности является объективной.

Первое информационное состояние обуславливает бесконфликтное течение допроса, второе – конфликт «без строгого соперничества», а два последних приводят к строго конфликтной ситуации допроса. Таким образом, допрос в зависимости от ситуации получения искомой информации от допрашиваемого классифицируется на: проводимый в бесконфликтной ситуации; проводимый в слабоконфликтной ситуации («без строгого соперничества»); проводимый в остроконфликтной ситуации («со строгим соперничеством»)².

Заметим, что ситуация конфликтна и тогда, когда лицо, как неумышленно (ситуация «без строгого соперничества»), так и умышленно (ситуация «со строгим соперничеством») скрывает или искажает информацию относительно своего истинного алиби, например, опасаясь неблагоприятного истолкования фактов в невыгодной для него ситуации, а также в том случае, когда у следователя имеются данные об алиби лица, которое признает факт совершения преступного деяния, тем самым оговаривая себя.

Диагностика информационного состояния сводится к установлению контакта с допрашиваемым, определению его отношения к искомой информации, выявлению возможного противодействия установлению истины с его стороны³. Она связана с более узкой проблемой – «диагностикой ложного алиби в ходе допроса», которой посвящены многие публикации зарубежных авторов, русских юристов XIX – начала XX вв. и криминалистов наших дней. В общем виде тактические приемы, позволяющие диагностировать ложное цифровое алиби, сводятся, на наш взгляд, к следующим рекомендациям:

1) предельной детализации показаний, связанных с «цифровым алиби», позволяющей предметно проверить, соответствует ли это алиби действительности;

2) выяснению обстоятельств работы на компьютере, которые имели место несколькими днями ранее расследуемого события, или, наоборот, следовавшие за ним, а в случае неспособности подозреваемого (обвиняемого) припомнить их постановка вопроса, почему запомнились обстоятельства того дня, когда произошло расследуемое событие;

3) проведению ряда повторных допросов по вопросам, вытекающим из результатов проверки «цифрового алиби». Сопоставление показаний с объективными данными, установленными в ходе проверки, позволяет в

¹ См.: Баев О. Я. Тактика уголовного преследования и профессиональной защиты от него. Следственная тактика : науч.-практ. пособ. / О. Я. Баев. — М. : Экзамен, 2003. — С. 182–183.

² См.: Криминалистика : учебник / под ред. Е. П. Ищенко, В. И. Комиссарова. — М. : Юристъ, 2007. — С. 276.

³ См.: Там же. — С. 277.

ряде случаев выявить неточности и противоречия в показаниях, что может быть использовано для изобличения во лжи.

После определения информационного состояния, исходя уже из ситуации допроса, могут применяться такие тактические приемы.

В *слабоконфликтной ситуации*, когда между интересами допрашивающего и допрашиваемого нет принципиальных противоречий, следователю необходимо определить возможные причины искажения, оказать помощь в адекватном воспроизведении подозреваемым (обвиняемым) имеющейся у него информации относительно «цифрового алиби» (например, лицо помнит, что работало на компьютере, но не припоминает отдельных обстоятельств, и т. д.). Тактические приемы этой группы можно охарактеризовать как мобилизующие память допрашиваемого путем использования феномена ассоциативных связей¹. Ассоциативные связи оживляются, как правило, либо путем передачи допрашиваемому вербальной информации, либо созданием условий для повторного воспроизведения допрашиваемым обстановки того или иного события.

В первом случае допрашиваемому, который, например, затрудняется точно указать время начала или окончания работы на компьютере либо иного события, предлагается вспомнить, не связано ли это событие с хорошо известными ему фактами, что позволяет «привязать» показания к соответствующим временным координатам или использовать другие источники доказательственной информации.

Во втором случае оживление ассоциативных процессов в сознании допрашиваемого достигается фактом повторного восприятия им той или иной информации. Немецкий криминалист А. Вайнгарт в своей работе начала XX в. «Уголовная тактика. Руководство к расследованию преступлений» писал: «Могущественным вспомогательным средством для того, чтобы вновь оживить в свидетеле воспоминания, является допрос его на том месте, где он сделал свои наблюдения: многие мелочи, которые он видит, а также разные звуки, доносящиеся до него, воздействуют на него так, что он многое припоминает, о чем бы ему даже и в голову не пришло в присутственном месте»². Иными словами, для мобилизации памяти подозреваемого (обвиняемого) возможно проведение допроса на месте расположения компьютера, на котором, как он утверждает, работал. Однако в этом случае необходимо учитывать вероятность негативного с его стороны воздействия, в том числе умышленного, на соответствующие компьютерные объекты, содержащие криминалистически-значимую информацию относительно заявленного алиби. Поэтому следует исключать возможность непосредственного контакта подозреваемого (обвиняемого) с такими объектами.

¹ См.: Кручинина Н. В. Проверка алиби. Принципы. Методы. Приемы / Н. В. Кручинина. — Иркутск : Изд.-во Иркут. гос. ун-та, 1988. — С. 35.

² Цитр. по: Кручинина Н. В. Проверка алиби. Принципы. Методы. Приемы. — С. 35.

В *остроконфликтной ситуации*, характеризующейся наличием принципиальных противоречий между интересами допрашивающего и допрашиваемого, первичной тактической целью допроса является воздействие на подозреваемого (обвиняемого) для получения в результате этого полных и объективных показаний. Единственным законным способом такого воздействия выступает убеждение, которое, как известно, бывает эмоциональным и логическим. При допросе относительно «цифрового алиби», на наш взгляд, применимы следующие способы убеждения:

1) предъявление доказательств, полученных в результате исследования соответствующих компьютерных объектов: в последовательности «нарастающей силы» до «решающего доказательства» либо комплекса взаимосвязанных доказательств после предварительного выяснения обстоятельств, связанных с ними;

2) демонстрация возможностей следствия путем разъяснения возможности установления истины без показаний допрашиваемого, например, возможностей компьютерно-технической экспертизы или производства следственного осмотра с участием специалиста;

3) маневрирование следователем информацией, когда он пытается создать у субъекта мнение, что тот обладает большей информацией, чем у него есть.

Обратим внимание на то, что следователь достоверно не знает, а лишь предполагает с определенной степенью вероятности, обладает ли подозреваемый (обвиняемый) искомой информацией. Поэтому любой тактический прием, наряду с такими критериями допустимости, как законность и этичность, должен отвечать избирательности воздействия. Иными словами, оказывать желаемое следователем воздействие лишь на лицо, обладающее искомой информацией, и быть нейтральным для всех остальных лиц.

Таким образом, приняв решение о допросе лица, ссылающегося на «цифровое алиби», следователь должен руководствоваться общей методикой проведения допроса, с учетом указанных особенностей.

М. В. Капустіна, асистент кафедри криміналістики Національної юридичної академії України імені Ярослава Мудрого, кандидат юридичних наук

КРИМІНАЛІСТИЧНА КЛАСИФІКАЦІЯ ЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ МЕДИЧНИМИ ПРАЦІВНИКАМИ

Проаналізовано підходи до визначення структури та підстав криміналістичної класифікації злочинів. Розглянуто кримінально-правову класифікацію злочинів, що вчиняються медичними працівниками. Запропоновано