

УДК 343.98

ЦИФРОВОЕ АЛИБИ И ЕГО ПРОВЕРКА

И. П. Пономарев

Воронежский государственный университет

Поступила в редакцию 30 сентября 2011 г.

Аннотация: рассматриваются понятие и вопросы проверки «цифрового алиби» – факта непосредственного взаимодействия подозреваемого (обвиняемого) в момент совершения преступления с электронной системой, находящейся в другом месте.

Ключевые слова: цифровое алиби, криминалистическая версия, виртуальный след.

Abstract: the article is devoted to the questions of concept and verification of «digital alibi» – the fact of the direct interaction of the suspect (accused) with an electronic system that is outside the crime scene at the time when the crime was committed.

Key words: digital alibi, forensic version, virtual trace.

При уголовно-процессуальном исследовании преступлений, механизм совершения которых с необходимостью включает в себе какие-либо действия субъекта на месте преступления в момент его совершения (а таковых – большинство), всегда возникает необходимость в выдвижении и проверке криминалистических версий об алиби подозреваемых (обвиняемых). В основе выдвижения таких версий в большинстве случаев лежит информация, полученная в ходе допроса указанных лиц, которые, как убедительно показывает практика уголовного судопроизводства последних лет, в обоснование заявляемого алиби все чаще ссылаются на то, что в момент совершения преступления они осуществляли взаимодействие с какими-либо электронными системами (работали с персональным компьютером, пользовались мобильным телефоном, попадали в поле зрения систем видеонаблюдения, авторизовались в системах контроля доступа в помещение и т.д.), находящимися в другом месте.

За рубежом такие объяснения получили, на наш взгляд, вполне удачное название «цифровое алиби» (digital alibi), ибо основным источником формирования доказательств, их подтверждающих либо опровергающих, выступает информация, записанная в цифровой форме на материальных носителях¹.

Таким образом, под термином «цифровое алиби» следует понимать факт непосредственного взаимодействия подозреваемого (обвиняемого) в момент совершения преступления с электронной системой, находящейся в другом месте.

¹ См.: Иванов Н. А. Применение специальных познаний при проверке «цифрового алиби». URL: <http://www.infolaw.ru/lib/2006-4-digital-alibi-expertise>

© Пономарев И. П., 2011

Серьезные исследования, выполненные В. И. Шикановым, Н. В. Кручининой, А. Т. Тимербаяевым и рядом других авторов, посвященные теоретическим проблемам алиби и их прикладному значению в уголовном судопроизводстве, методикам проверки, а также вопросам разоблачения ложного алиби, проводились до появления в следственной и судебной практике ситуаций, связанных с заявлением цифрового алиби. 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, поэтому нуждается в самостоятельном рассмотрении.

Во-первых, доказательственная информация, подтверждающая либо опровергающая «цифровое алиби», недоступна непосредственному восприятию. Для ее извлечения необходимо использование программно-технических средств.

Во-вторых, такая доказательственная информация является крайне неустойчивой, так как может быть легко уничтожена (например, неправильными действиями следователя).

В наибольшей степени специфика проверки цифрового алиби, на наш взгляд, проявляется в процессе выдвижения и проверки соответствующих криминалистических версий. Для того чтобы выдвинуть версию, следователь, как известно, должен располагать необходимой информацией, но информацией, недостаточной для однозначного по ней вывода. К такой информации относятся непосредственно сообщенные подозреваемым (обвиняемым) либо полученные из других источников сведения о наличии у лица цифрового алиби на момент совершения преступления.

Именно в результате накопления и логического осмысления данной информации может быть сформулирована версия о цифровом алиби в любом из возможных ее вариантов:

- 1) подозреваемый (обвиняемый) имеет цифровое алиби;
- 2) подозреваемый (обвиняемый) цифрового алиби не имеет;
- 3) цифровое алиби подозреваемого (обвиняемого) сфальсифицировано.

Принимая во внимание, что криминалистическая версия – лишь мысленный образ того или иного события, практической проверке поддаются только следствия из нее, которые обуславливают соответствующие направления поиска. Поэтому особое внимание, с нашей точки зрения, необходимо уделить формированию системы следствий, указывающих на наличие либо отсутствие цифрового алиби подозреваемого (обвиняемого) в расследуемом криминальном событии.

Как верно пишет О. Я. Баев, являясь «информационной базой выдвижения соответствующей криминалистической версии, предположительно объясняющей одну из возможных причин возникновения следствия, действия причины неизбежно должны нести на себе отпечатки (следы) причины. Это положение – перенос структуры от причины к следствию,

² См.: Кручинина Н. В., Шиканов В. И. Тактическая операция «Проверка алиби»: методические указания. Иркутск, 1989.

т.е. отображение первой во второй является, как известно, фундаментальной чертой динамики процесса причинения и лежит в основе свойства отражения»³. Из этого положения следует, что причина ведет к своему исчерпывающему отражению в следствиях своего действия – взаимодействие лица с электронной системой влечет появление соответствующих следов.

Пользуясь системой, разработанной криминалистикой для классификации следов преступления, которая, по нашему мнению, универсальна и применима для любого процесса действительности, среди указанных следов взаимодействия с электронной системой вполне обоснованно можно выделить:

- материальные следы – на периферийном оборудовании, клавишах, других материальных объектах, участвующих в процессе работы (например, листах бумаги при распечатке текстов на принтере), остаются отпечатки пальцев, потожировые следы, следы табака и т.д.;

- идеальные следы – процесс взаимодействия с электронной системой отражается в сознании, памяти подозреваемого (обвиняемого).

Особенность установления алиби состоит в том, что выясняют, где находилось то или иное лицо в уголовно-релевантное время⁴. Это означает, что исследуемые при этом следы, в первую очередь, необходимо оценивать с учетом времени их возникновения и существования.

Материальные следы, возникшие в результате взаимодействия человека с электронной системой, зачастую довольно трудно привязать к определенному времени. Задача представляется вовсе не разрешимой, если с данной системой лицо контактирует постоянно. Примером этого могут послужить материальные следы, возникающие в процессе работы с компьютером – явно неоднократным и повторяющимся в течение довольно длительного времени. Некоторые авторы отмечают, что среди таких следов можно интуитивно выделить лишь «свежие» и «старые» по имеющимся в них изменениям⁵.

Идеальные следы в данном аспекте более содержательны, поскольку отображение течения времени в сознании человека происходит гораздо глубже и полнее, чем в материальных объектах. Р.С. Белкин, в частности, отмечает, что по сравнению с материальными, идеальные следы содержат информацию о таких сторонах объекта, которые не отображаются в материальных следах. Они могут применяться для установления как причинно-следственных связей, так и пространственных и временных связей и отношений. Однако их точность является относительной, поскольку она зависит от протекания психических процессов восприятия,

³ Баев О. Я. Тактика уголовного преследования и профессиональной защиты от него. Следственная тактика : науч.-практ. пособие. М., 2003. С. 54.

⁴ См.: Аббасова И. С. [и др.]. Вопросы теории и практики проверки алиби (по материалам, опубликованным в зарубежной печати) : лекция. Иркутск, 1982. С. 14.

⁵ См.: Мешков В. М. Основы криминалистической теории о временных связях. Изд. 2-е, доп. и перераб. Калининград, 1999. С. 110.

запоминания и воспроизведения такой информации. В первую очередь, речь идет о непреднамеренных или умышленных ее искажениях.

Ряд проведенных исследований⁶ показывает, что существует еще один вид следов, занимающих промежуточное положение между следами материальными и идеальными, – *следы виртуальные*.

В. А. Мещеряков, первым обративший внимание на ряд специфических свойств таких следов, определил их «как любое изменение состояния автоматизированной информационной системы (образованного ею «кибернетического пространства»), связанное с событием преступления и зафиксированное в виде компьютерной информации (т.е. информации в виде, пригодном для машинной обработки) на материальном носителе, в том числе на электромагнитном поле»⁷.

Виртуальные следы, возникающие в ходе взаимодействия с электронной системой, имеют наибольшее значение при проверке версий о цифровом алиби подозреваемого (обвиняемого), поскольку они, в силу своей природы, имеют жесткую привязку ко времени их возникновения.

Доказательственное значение временных отметок возникающих виртуальных следов работы обусловлено наличием в электронных системах так называемых компьютерных часов, ход которых отсчитывается встроенным тактовым генератором и временной организацией процессов обработки и хранения данных.

Рассмотрим процесс выдвижения и проверки криминалистических версий о цифровом алиби на примере ситуации, когда лицо заявляет, что в момент совершения преступления оно осуществляло работу с персональным компьютером, находящимся в другом месте.

Так, время включения и отключения компьютера, подключения к компьютерной сети и внешнему оборудованию, время запуска и остановки системных служб, время установки программного обеспечения и других событий фиксируется в системном «журнале событий».

Помимо системного «журнала событий» большинство прикладных программ (текстовых редакторов, интернет-браузеров, систем обмена мгновенными сообщениями) имеют встроенные функции сохранения истории своей работы. Многие компьютерные программы «ведут» также собственные так называемые файлы протокола.

440 Файл протокола или «лог» (англ. log) – файл с записями о событиях в хронологическом порядке. Данные файлы генерируются автоматически и содержат различную информацию (сервисные сообщения, коды ошибок и т.д.) о сеансах работы программы, их создавшей.

Кроме того, при работе лица с персональным компьютером происходит изменение файлов и их временных меток (времени создания, модификации, последнего доступа). При этом необходимо учитывать, что компью-

⁶ См.: Мещеряков В. А. Преступления в сфере компьютерной информации : правовой и криминалистический анализ. М., 2001 ; Краснова Л. Б. Компьютерные объекты в уголовном процессе и криминалистике. Воронеж, 2005. 152 с.

⁷ Мещеряков В. А. Преступления в сфере компьютерной информации : основы теории и практики расследования. М., 2002. С. 104.

терная информация является легко модифицируемой. Отсюда возникает не менее важная задача установления, не были ли виртуальные следы работы подозреваемого (обвиняемого) с компьютером во время совершения преступления сфальсифицированы в целях создания себе алиби.

Фальсификация виртуальных следов работы возможна путем перевода компьютерных часов, добавлением ложной информации в файлы «журнала событий» и файлы протокола, использованием макросов, а также иными способами.

Макрос (от англ. macros) – программный объект, при обработке «развертывающийся» в последовательность действий или команд. Во многих «офисных» продуктах, в текстовых и графических редакторах при обработке макроса автоматически выполняется заданная для каждого макроса последовательность действий – нажатия на клавиши, выбор пунктов меню и т.д. Указанные программы также предоставляют интерфейс для записи новых и редактирования существующих макросов⁸.

Заметим, что возможность установления фальсификации обоснована положением о том, что, уничтожая, добавляя или модифицируя виртуальные следы работы с компьютером, пользователь порождает другие следы – соответственно следы уничтожения, добавления или модификации информации. Это объясняется тем, что практически никто не обладает в полном объеме сведениями об изменении временных характеристик всех файлов и информации в них.

Таким образом, с методологических позиций и для целей формирования системы следствий, влияющих на процесс выдвижения версии относительно цифрового алиби, необходимо учитывать, что:

1) алиби представляет собой логическую систему, состоящую из трех элементов: время совершения преступления, место его совершения и место фактического нахождения заявителя алиби в момент совершения преступления⁹;

2) основным источником формирования доказательств, подтверждающих либо опровергающих цифровое алиби, выступает информация, находящаяся в цифровой форме на машинных носителях;

3) данная информация благодаря своей природе легко может быть создана, изменена (модифицирована) и уничтожена, в том числе и в целях ее фальсификации для последующего обеспечения доказательств ложного алиби.

Согласно рассмотренным выше положениям, в самом общем виде можно выделить все необходимые следствия, вытекающие из версий о цифровом алиби лица, осуществлявшего работу с персональным компьютером:

1. Следов работы с компьютером в момент времени, зафиксированный как время преступления, нет.

⁸ Компьютерра ONLINE : программы для записи макросов. URL: <http://www.computerra.ru/softerra/raznosoft/34556/>

⁹ Шиканов В. И. Проверка алиби в процессе расследования уголовных дел об убийстве : учеб. пособие. Иркутск, 1978.

2. Имеются следы работы лица на стационарном (не портативном) компьютере, находящемся в месте, отличном от места преступления, в момент времени, зафиксированный как время совершения преступления.

3. Имеются следы работы лица на портативном компьютере (ноутбук, нетбук), место нахождения которого на время совершения преступления не установлено.

4. Признаков фальсификации (модификации, искусственного создания) следов работы с компьютером в указанное время нет.

Заметим, что установить место нахождения портативного компьютера в интересующий момент времени возможно лишь при наличии следов его подключения в этот момент времени к сети Интернет либо к периферийному непортативному оборудованию, место нахождения которого установлено.

Очевидно, что для опровержения цифрового алиби подозреваемого (обвиняемого) достаточно хотя бы одного из следующих следствий:

- следов работы с компьютером в момент времени, зафиксированный как время преступления, нет;
- имеются признаки фальсификации (модификации, искусственного создания) следов работы с компьютером в момент времени, зафиксированный как время преступления.

Кроме того, могут быть рассмотрены и возможные следствия, вытекающие из такой версии о цифровом алиби. Например, при наличии подключения компьютера подозреваемого (обвиняемого) к компьютерной сети Интернет можно выделить такие следствия:

- у поставщика услуг Интернет (интернет-провайдера) имеются данные о сеансе работы с компьютером подозреваемого (обвиняемого);
- кто-то мог связываться с подозреваемым (обвиняемым) посредством интернет-коммуникаций (системы мгновенных сообщений, электронная почта, видеоконференции, интернет-телефония и т.д.).

Сформулированная система необходимых и возможных следствий из версий о цифровом алиби предопределяет планирование их проверки. Практическая проверка должна привести либо к подтверждению версии о цифровом алиби, либо к ее опровержению.

Известно, что проверка заявленного алиби требует исчерпывающего установления его истинности или ложности. Если имеются какие-то сомнения в отношении истинности или ложности заявленного алиби, то проверять необходимо до полного устранения этих сомнений¹⁰. Таким образом, если достоверного (положительного или отрицательного) знания по версии не получено, то ее проверка продолжается.

Полученное положительное достоверное знание о цифровом алиби подозреваемого (обвиняемого) завершает версиюную деятельность по данному обстоятельству. В данном случае полностью исключается возможность совершения конкретным лицом расследуемого преступления.

¹⁰ *Тимербаев А. Т.* Актуальные вопросы проверки алиби на предварительном следствии // Криминалистические проблемы пространственно-временных факторов в расследовании преступлений. Иркутск, 1983. С. 82.

Здесь, безусловно, происходит изменение направления расследования преступления, так как необходимо установить человека, действительно учинившего это криминальное деяние.

Отрицательный достоверный ответ означает окончание проверки версии, но обуславливает необходимость нового витка версионной деятельности: снова осмысливание информации, но информации, зачастую вновь полученной или модифицированной в результате проверки неподтвердившейся версии¹¹. Например, при проверке следствий, вытекающих из версии о цифровом алиби, может быть установлено, что лицо, кроме совершения преступления, по поводу которого заявило алиби, совершило и другое преступление.

Как известно, проверка следствий, вытекающих из версии, осуществляется средствами, либо прямо предусмотренными, либо не противоречащими действующему уголовно-процессуальному законодательству. Применительно к задаче проверки версии о цифровом алиби следовательно может потребоваться весь комплекс возможностей и, прежде всего, все многообразие следственных действий, предусмотренных законом.

В качестве первоочередных, как правило, при этом выполняются действия, направленные на обнаружение и фиксацию быстроизменяющихся следов, а также доказательств, которые могут быть утрачены или умышленно видоизменены. Именно это обуславливает первоочередную необходимость осмотра компьютерных средств и содержащейся в них или на отдельных носителях информации, а также иных объектов (например, периферийного оборудования).

Следователи, обладающие углубленными (специальными) познаниями в той или иной области компьютерных технологий, представляют большую редкость, поэтому привлечение специалиста к участию в следственных действиях, проводимых при проверке следствий, вытекающих из версии о цифровом алиби, крайне необходимо, «поскольку даже малейшие неквалифицированные действия с компьютерной системой зачастую заканчиваются безвозвратной утратой ценной розыскной и доказательственной информации»¹². Именно благодаря специалисту, обладающему специальными познаниями в области компьютерных технологий, возможно решение намеченных задач в ходе следственного действия.

Привлечение специалиста для участия в осмотре требуется в тех случаях, когда изучение самого объекта, изменений в нем, а также обнаружение и фиксация следов и других вещественных доказательств требуют применения либо знаний, умений, которыми следователь не обладает, либо технических средств, в пользовании которыми следователь не имеет должных навыков¹³.

¹¹ См.: Баев О. Я. Основы криминалистики : курс лекций. 3-е изд., перераб. и доп. М., 2009. С. 115.

¹² Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М., 2001.

¹³ См.: Баев О. Я. Тактика уголовного преследования и профессиональной защиты от него. Следственная тактика : науч.-практ. пособие.

Следует отметить, что необходимые следствия, вытекающие из версии о цифровом алиби подозреваемого (обвиняемого), не всегда возможно проверить в ходе следственного осмотра. В таком случае возникает необходимость в изъятии объектов осмотра и последующем назначении компьютерно-технической и иных экспертиз.

Как известно, алиби имеет важное уголовно-правовое, уголовно-процессуальное и криминалистическое значение.

Уголовно-правовое значение алиби в том, что оно влияет на правильное решение вопроса о виновности. Подтвердившееся алиби свидетельствует о невиновности лица, а опровергнутое – о возможной причастности лица к преступлению. Кроме того, заявление и отстаивание ложного алиби учитываются при индивидуализации наказания.

Значение заявленного алиби с точки зрения уголовного процесса заключается в том, что оно служит средством защиты. Подозреваемые, обвиняемые на предварительном следствии защищаются от подозрения или обвинения в совершенном преступлении различными способами, в том числе и путем заявления алиби. Ни в коем случае нельзя игнорировать и оставлять без проверки или формально проверять сообщения об алиби, потому что такое отношение будет грубым ущемлением процессуальных прав подозреваемого или обвиняемого¹⁴.

Криминалистическое значение алиби, как и отмечалось выше, выражается в появлении с момента его заявления подозреваемым (обвиняемым) новых следственных версий, что приводит к возникновению перед следователем новых задач и влияет на планирование расследования.

Более того, такие версии могут быть сформулированы и в отношении иных уголовно-релевантных лиц: потерпевших, свидетелей, которые, как показывает практика, зачастую пытаются «отмежеваться» от причастности к событию преступления и тем самым избежать возможного участия в производстве процессуальных действий, либо, наоборот, дают ложные показания о своем нахождении на месте криминального события. Именно этим и обусловлена необходимость разработки вопросов выдвижения и проверки весьма специфичных версий о цифровом алиби в целях оптимизации следственного поиска при наличии минимальной информации.

¹⁴ См.: Тимербаев А. Т. Актуальные вопросы проверки алиби на предварительном следствии. С. 82.