можливості органу дізнання з самого початку розслідування злочину й до закінчення досудового слідства.

9. Нерозголошення учасниками взаємодії даних процесуальної, оперативно-розшукової та іншої діяльності. Вимога нерозголошення даних досудового слідства та оперативних відомостей, будучи однією з умов успішного здійснення пізнавальної діяльності з установлення обставин учиненого злочину, є одним з принципових положень. Таємниця слідства, як обґрунтовано зазначає А. М. Ларін, – це важлива умова виявлення доказів у тому вигляді, у якому вони є, без змінень. Злочинці та пов'язані з ними особи не повинні знати про плани, джерела та межі поінформованості слідчого[1]. Передчасне розголошення може дозволити винним уникнути відповідальності або скомпрометувати добропорядних громадян, якщо стосовно них слідчий одержав недостовірні відомості, що їх ганьблять.

Отже, підбиваючи підсумок викладеному, уважаємо за необхідне відзначити, що в діяльності правоохоронних органів взаємодія між слідчим та іншими учасниками досудового слідства виникає задовго до порушення кримінальної справи, у ході проведення перевірочних і оперативно-розшукових заходів, здійснюється із залученням не тільки правоохоронних органів, а й також спеціалістів, співробітників контролюючих органів, громадськості. Взаємодія суб'єктів повинна відбуватися в умовах взаємної відповідальності усіх учасників за обсяг і якість виконуваних ними дій. Процес взаємодії між учасниками обов'язково має будуватися на перелічених принципах для досягнення спільної мети або вирішення окремих завдань, що виникають на досудовому слідстві.

И. П. Пономарев, аспирант кафедры криминалистики Воронежского государственного университета

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ ПРОВЕРКЕ ВЕРСИИ О ЦИФРОВОМ АЛИБИ

У практиці кримінального судочинства останніх років все частіше трапляються ситуації, коли підозрювані (обвинувачені) в обгрунтуванні свого алібі посилаються на те, що в момент учинення злочину вони працювали на персональному комп'ютері, який знаходився в іншому місці. Перевірка відповідних версій має певну специфіку та потребує використання спеціальних знань у формі судових експертиз.

[1] Див.: *Ларин А. М.* Работа следователя с доказательствами / А. М. Ларин. — М. : Юрид. лит., 1966. — С. 49–50.

В практике уголовного судопроизводства последних лет все чаще встречаются ситуации, когда подозреваемые (обвиняемые) в обосновании своего алиби ссылаются на то, что в момент совершения преступления они работали на персональном компьютере, находящемся в другом месте. Проверка соответствующих версий имеет определенную специфику и требует использования специальных знаний в форме судебных экспертиз.

Как убедительно показывает практика уголовного судопроизводства последних лет, в обоснование заявляемого алиби подозреваемые (обвиняемые) все чаще ссылаются на то, что в момент совершения преступления они работали на персональном компьютере, находящемся в другом месте. За рубежом такие объяснения получили, на наш взгляд, вполне удачное название «цифровое алиби», ибо основным источником формирования доказательств выступает информация, записанная в цифровой форме на материальных носителях.

Проверка версий относительно цифрового алиби, без сомнений, имеет определенную специфику и в первую очередь, предполагает использование специальных знаний, как правило, в форме соответствующих судебных экспертиз, вопросам назначения которых и посвящена данная публикация.

Учитывая, что: 1) алиби представляет собой логическую систему, состоящую из трех элементов: времени совершения преступления, места его совершения и места фактического нахождения заявителя алиби в момент совершения преступления[1]; 2) основным источником формирования доказательств, подтверждающих либо опровергающих цифровое алиби, выступает информация, находящаяся в цифровой форме на материальных носителях; 3) эта информация, благодаря своей природе, легко может быть создана, изменена (модифицирована) и уничтожена, в том числе в целях ее фальсификации для последующего обеспечения доказательств ложного алиби, из версии о цифровом алиби, в самом общем виде, можно выделить следующие необходимые следствия[2]:

— следы работы лица на стационарном (не портативном) компьютере, находящемся в месте, отличном от места преступления,

[1] См.: *Шиканов В. И.* Проверка алиби в процессе расследования уголовных дел об убийстве : учеб. пособ. / В. И. Шиканов. — Иркутск : Изд-во Иркутск. гос. ун-та, 1978. — С. 13.

[2] Исследование любой криминалистической версии в первую очередь предполагает выведение и формулирование вытекающих из нее необходимых и возможных следствий. Именно они (а не сама версия, как идеальная модель) поддаются практической проверке (см. об этом: *Баев О. Я.* Основы криминалистики : курс лекций / О. Я. Баев. — [3-е изд., перераб. и доп.]. — М. : Эксмо, 2009. — С. 110–121; *Пономарев И. П.* Выдвижение и проверка следственных версий о цифровом алиби подозреваемого (обвиняемого) / И. П. Пономарев // Криминалистика **XXI столетия :** матер. междунар. науч.-практ. конф., Харьков, 25–26 нояб. 2010 г. — Х. : Право, 2010. — С. 453–458).

в промежуток времени, зафиксированный как время совершения преступления, действительно имеются, и нет признаков их фальсификации;

— имеются следы работы лица на портативном компьютере (ноутбуке, нетбуке), место нахождения которого на время совершения преступления не установлено.

Кроме того, могут быть сформулированы и возможные следствия. Например, при наличии подключения компьютера подозреваемого (обвиняемого) к сети Интернет они могут быть такими:

— у поставщика услуг Интернет (интернет-провайдера) имеются данные о сеансе работы на компьютере подозреваемого (обвиняемого);

— некие лица могли связываться с подозреваемым (обвиняемым) посредством Интернет-коммуникаций (системы мгновенных сообщений, электронной почты, видеоконференции, Интернет-телефонии и т. д.);

— подозреваемый (обвиняемый) мог создавать или редактировать какую-либо информацию в сети Интернет (записи блогов, статус-сообщения, веб-страницы).

Согласно приведенной системе необходимых и возможных следствий в ходе проверки версии о цифровом алиби закономерно возникают следующие задачи, которые без привлечения для этого специальных познаний разрешены быть не могут:

— установление факта работы на указанном персональном компьютере в заданный интервал времени;

— определение перечня работ и действий, осуществлявшихся на персональном компьютере в указанный временной интервал;

— установление того, не были ли данные о работе, производившейся заявителем алиби на компьютере во время совершения преступления, сфальсифицированы;

— определение места нахождения компьютера в момент совершения преступления (в случае если компьютер портативный);

— идентификация лица (пользователя), работавшего на указанном персональном компьютере в интересующий интервал времени.

С этой целью на разрешение экспертизы с учетом объяснений подозреваемого (обвиняемого) по обстоятельствам заявленного им цифрового алиби могут быть поставлены такие вопросы:

— Осуществлялась ли работа на представленном компьютере в указанное время?

— Не подвергалась ли информация, свидетельствующая об этом, фальсификации, а если да, то каким способом?

— Какое программное обеспечение использовались на представленном компьютере в указанное время?

— Какие файлы изменялись (создавались, редактировались) в указанное время на представленном компьютере?

— Какая хронологическая последовательность действий (операций) пользователя имела место в указанное время на представленном компьютере?

— Входил ли пользователь представленного компьютерного средства в сеть Интернет в указанное время?

— Имеются ли на представленном компьютере и какие электронные сообщения (электронной почты, сервисов обмена мгновенными сообщениями) полученные (отправленные) в указанное время через Интернет, по каким адресам они отправлены?

— Является ли пользователем, работавшим на представленном компьютере в указанное время, конкретное лицо, чье цифровое алиби проверяется?

Очевидно, что большая часть этих вопросов может быть разрешена путем назначения судебной компьютерно-технической экспертизы, общим предметом которой являются факты и обстоятельства, устанавливаемые на основе исследования закономерностей разработки и эксплуатации компьютерных средств, обеспечивающих реализацию информационных процессов, которые зафиксированы в материалах уголовного дела[1].

Родовая классификация судебной компьютерно-технической экспертизы организована на основе обеспечивающих компонент любого компьютерного средства – аппаратного (технического), программного и информационного обеспечения. В соответствии с этим в судебной компьютерно-технической экспертизе выделяют следующие направления исследований:

1) аппаратной составляющей компьютерных систем;

2) программной составляющей компьютерных систем;

3) данных программ и пользователей;

4) обстоятельств работы в компьютерной сети.

На основе указанных исследований могут быть получены данные, позволяющие с определенной степенью вероятности ответить на вопрос об идентификации пользователя, работавшего на представленном компьютере в определенное время. Возможности такой идентификации основаны в первую очередь на использовании динамических признаков, которые формируются у человека в процессе жизнедеятельности и обладают выраженными индивидуальными чертами.

Так, если компьютер использовался лицом как инструмент для создания различных документов, в целях идентификации могут быть применены специальные знания в области технико-криминалистической экспертизы документов.

---

[1] *См.: Россинская Е. Р.* Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе / Е. Р. Россинская. — 2-е изд., перераб. и доп. — М. : Норма, 2008. — С. 472–473.

Компьютер предоставляет автору или исполнителю документа обширный набор механизмов формирования текстов – специализированных программ. Причем каждый оператор (пользователь) компьютера владеет некоторой совокупностью этих механизмов. Навыки владения ими для каждого оператора индивидуальны и относительно устойчивы. Именно они отображаются в документе, являясь идентифицирующим признаком оператора (пользователя).

Например, каждый программист при редактировании кода программы, во-первых, пользуется определенными инструментами; во-вторых, определенными именами и последовательностью операторов; в-третьих, по своему усмотрению оформляет код. Совокупность указанных характеристик в ряде случаев позволяет идентифицировать автора.

Пользователь, редактирующий текстовые документы, например, в редакторе Microsoft Word, как правило, использует только те элементы форматирования, к которым он привык, или которые ему хорошо известны (автоматические переносы, автоматическое выравнивание текста, отступы, оглавление, сноски и т. п.)[1].

Кроме судебной технико-криминалистической экспертизы документов для решения задач идентификации лица, работавшего на компьютере в указанное время, возможно применение подходов и методов автороведческой экспертизы. Данный вид экспертиз производится с целью установления автора текста на основании анализа отобразившихся в нем особенностей письменной речи. При проверке криминалистической версии о цифровом алиби текстом-объектом автороведческой экспертизы могут выступать электронные документы, e-mail сообщения, записи в блогах и т. п., исполненные в бытовом, деловом, публицистическом и научном стилях письменной речи. Заметим, что решение вопроса об авторстве возможно, если исследуемый текст содержит не менее 500 слов[2].

Также следует обратить внимание на то, что компьютерная информация на машинных носителях может являться и файлом, содержащим звуковой ряд – живую речь или иные существенные для проверки цифрового алиби звуки. В таких случаях могут применяться специальные знания в области фоноскопии[3].

Необходимо упомянуть и о возможности проведения в целях

[1] См.: *Кукарникова Т. Э.* Возможности экспертных исследований электронных документов / Т. Э. Кукарникова // Воронежские криминалистические чтения : сб. науч. тр. / под ред. О. Я. Баева. — Воронеж: Изд-во Воронеж. гос. ун-та, 2007. — Вып. 8. — С. 198.

[2] См.: *Россинская Е. Р.* Указ. работа. — С. 385.

[3] См.: *Галяшина Е. И.* Идентификация личности по фонограммам речи на базе АРМа эксперта-фоноскописта / Е. И. Галяшина, М. И. Фомичева. — М. : ЭКЦ МВД России, 1995. — С. 45.

идентификации пользователя, работавшего на компьютере, экспертных исследований в области трасологии – на периферийном оборудовании компьютера, клавишах, других материальных объектах, участвующих в процессе работы пользователя на компьютере , на листах бумаги при распечатке текстов на принтере), остаются материальные следы – отпечатки пальцев, потожировые следы и т. д.

В данном случае, учитывая, что объектами экспертиз различных видов будут выступать одни и те же компьютерные средства, особое внимание следует уделить последовательности назначения экспертиз. При этом необходимо придерживаться такой рекомендации: в первую очередь назначаются экспертизы по тем следам, которые, более чем другие, подвержены различным внешним воздействиям и изменениям[1]. Иными словами, логично сначала провести трасологические исследования компьютерного средства как материального объекта, а затем его исследования как носителя компьютерной информации. Ведь материальные следы в виде потожировых следов и отпечатков пальцев в отличие от компьютерной информации «находятся на поверхности» и могут быть легко уничтожены.

Следует также учитывать, что решение любых идентификационных задач возможно лишь при наличии идентифицирующего и идентифицируемого объектов, и, следователю, на подготовительном этапе назначения экспертиз, необходимо будет получить образцы для сравнительного исследования.

Как известно, по результатам исследования эксперт составляет заключение, анализ которого играет решающую роль в ходе проверки криминалистической версии о цифровом алиби. В ходе такого анализа с учетом ответов эксперта на поставленные перед ним вопросы подтверждаются либо не подтверждаются необходимые и возможные последствия, вытекающие из рассматриваемой версии.

Так, отрицательный ответ на вопрос относительно наличия следов работы на компьютере в момент времени, зафиксированный как время преступления, означает, что версия о цифровом алиби не подтвердилась.

Положительный ответ на вопрос относительно наличия признаков фальсификации следов работы на компьютере в искомое время, как правило, указывает на то, что цифровое алиби является ложным и заранее подготовленным подозреваемым (обвиняемым) либо его сообщниками.

Однако для решения задач идентификации лица, работавшего на указанном компьютере в момент совершения преступления,

[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. 56.

может потребоваться применение специальных знаний в области технико-криминалистической экспертизы документов, автороведения, фоноскопии и т. д.[1]

Наличие в заключениях экспертов указанных ответов приводит к окончанию проверки версии о цифровом алиби, но обусловливает необходимость нового витка версионной деятельности: снова осмысливается информация, полученная или модифицированная в результате проверки неподтвердившейся версии[2].

[1] При этом пограничные вопросы должны исследоваться в рамках комплексной экспертизы, т. е. экспертизы, в производстве которой участвуют несколько экспертов различных специальностей или специализаций (профилей). В ее ходе решаются вопросы, как правило, смежные для различных родов судебных экспертиз (см. об этом: *Кукарникова Т. Э.* Указ. работа. — С. 193–202).

[2] См.: *Баев О. Я.* Основы криминалистики : курс лекций. — **С. 115.**