О Т З Ы В

на диссертацию Вражнова Алексея Сергеевича на тему: «Криминалистический риск при расследовании неправомерного доступа к компьютерной информации», представленную на соискание ученой степени кандидата юридических наук по специальности 12.00.12 - криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность

Развитие информационных технологий, автоматизация и компьютеризация различных, в том числе и производственных процессов, использование компьютерной техники в целях повышения оперативности деятельности правоохранительных органов - те тенденции, которые характерны для современного состояния практики раскрытия и расследования преступлений. В свою очередь эти тенденции выдвигают на передний план научных исследований в данной области проблемы, связанные с использованием всевозможных компьютерных устройств и новых информационно-обрабатывающих технологий в целях неправомерного доступа к охраняемой законом компьютерной информации и иных преступных деяний.

Учитывая сложность расследования таких преступлений, обусловленную необходимостью обладания субъектами расследования преступления определенными знаниями в области информационных технологий, а также тот факт, что деятельность следователя, как впрочем, и экспертов, специалистов, оперативных сотрудников и других лиц, привлекаемых следователем для оказания ему помощи, может происходить в условиях информационной неопределенности, нельзя исключить ситуации наступления криминалистического риска. Разработка практических рекомендаций для следователей, оперативных работников, специалистов, экспертов по данной проблематике становится залогом эффективности деятельности должностных лиц правоохранительных органов, служит показателем их профессиональной состоятельности, понимания и реализации растущих возможностей.

И хотя в литературе по проблемам криминалистики работы по вопросам практики раскрытия и расследования преступлений, связанных с использованием информационных технологий не редкость, далеко не все области информационного подхода исследованы на монографическом уровне достаточно глубоко. В связи с этим следует признать, что разработка научных положений о криминалистическом риске, направленных на повышение эффективности расследования преступлений данной категории,

включая и расследование неправомерного доступа к компьютерной информации, ставшая темой диссертационного исследования А.С. Вражнова, носит актуальный характер.

Не вызывает сомнений и научная новизна работы. Предпринятая автором попытка показать особенности расследования неправомерного доступа к компьютерной информации и выявить ошибки, допускаемые некоторыми из участников уголовного судопроизводства, приводящими к наступлению криминалистического риска, приведенные им ситуации, складывающиеся в стадии возбуждения уголовного дела, а также при проведении отдельных следственных действий, и ведущие к наступлению криминалистического риска - все это весьма весомый вклад в теорию и практику криминалистики и судебной экспертизы, где эти вопросы в предлагаемом аспекте рассмотрены явно недостаточно. Практическая значимость работы отчетливо выступает в публикациях автора по теме исследования, получила необходимую поддержку и подтверждение при его устных выступлениях в профессиональных аудиториях.

Теоретические выводы и практические рекомендации автора, обладая новизной и обоснованностью, представляют собой существенный вклад не только в криминалистическую науку, но и в следственную практику.

Успеху предпринятого диссертационного исследования в немалой степени способствовали признанная методология научных изысканий, обширный круг литературных источников по вопросам права, криминалистики, оперативно-разыскной деятельности, теории информации, систематике и автоматизации. Достаточной представляется и эмпирическая база исследования: автором проведен анализ и обобщение более 340 уголовных дел, возбужденных по ст. 272 УК РФ, опрос 50 лиц из числа руководящего персонала, а также 50 лиц, являющихся IT- специалистами коммерческих и некоммерческих организаций, использован личный опыт соискателя в проведении служебных проверок по фактам несанкционированного доступа к компьютерной информации.

Диссертант поставил перед собой целый ряд задач, среди которых: установление практической значимости определения криминалистического риска при производстве следственных действий, тактических операций и комбинаций вне зависимости от вида преступлений; выявление основных видов криминалистического риска в деятельности, следователя, сотрудников оперативно-разыскных органов, специалиста, эксперта, суда, прокурора, руководителя следственного органа, свидетеля, заявителя и представителя потерпевшего на стадиях возбуждения уголовного дела и предварительного расследования для деяния, предусмотренного статьей 272 УК РФ; разработка

методических рекомендаций, направленных на минимизацию негативных последствий основных видов криминалистического риска при расследовании неправомерного доступа к компьютерной информации и др. Как показало изучение диссертации, все эти задачи решены и решены успешно.

Убедительности выводов и рекомендаций автора способствует сама логика построения его работы, ее в целом хороший стиль изложения. Вслед за введением, включающим обоснование выбора данной темы, цель и задачи исследования, предмет, объект, научную и практическую значимость, положения, выносимые на защиту и т.д., он рассматривает в первой главе понятие «криминалистический риск»; показывает на примерах, как ошибки участников уголовного судопроизводства и иных субъектов процесса расследования могут привести к ситуации криминалистического риска; предлагает новые классификационные основания криминалистического риска (с.15-39); анализирует деятельность следователя, дознавателя при проведении ими следственных действий, тактических операций и комбинаций в условиях криминалистического риска (с. 39-49).

Диссертант абсолютно прав утверждая, что «риск через призму информационности зависит от объема тех сведений, которыми можно оперировать, и, следовательно, тесно связан с неопределенностью». Прав он и в том, что информационная составляющая может проявляться в двух аспектах: внешнем, который «всецело зависит от объема фактов… и иных сведений о предстоящем событии», и внутреннем, проявляющимся «в оценке всей информации определенным субъектом» (с. 18-19). Однако, точнее, на мой взгляд, следовало бы здесь вести речь не о внешних и внутренних аспектах информационной составляющей, а о влиянии на ее формирование субъективных и объективных факторов.

Заслуживает внимание попытка соискателя рассмотреть возможность возникновения криминалистического риска в деятельности следователя через призму таких факторов, как временной, пространственно-территориальный, личностный, непосредственно связанных с механизмом возникновения ошибки (с. 40-42). Диссертант достаточно подробно раскрывает содержание этих факторов (называя каждый из них, почему-то, криминалистическим), их влияние на возникновение криминалистического риска, перечисляет те негативные последствия, которые могут наступить в расследовании уголовного дела.

Во второй главе – «Анализ предкриминалистического и криминалистического рисков при обнаружении и расследовании неправомерного доступа к компьютерной информации», - речь идет об обнаружении неправомерного доступа к компьютерной информации на

примере деятельности субъектов корпоративно-трудовых отношений в условиях предкриминалистического риска (с. 50-63), подробно рассматривается возможность наступления криминалистического риска в деятельности участников уголовного судопроизводства в стадии возбуждения уголовного дела (с.64-97) и предварительного расследования (с. 98-123), предлагаются методические рекомендации, направленные на минимизацию криминалистического риска при расследовании преступлений, связанных с неправомерным доступом к компьютерной информации.

Глава написана интересно, хотя некоторые ее положения, вызывают обоснованные сомнения. Весьма туманными представляются рассуждения о возникновении предкриминалистического риска в деятельности лиц – участников корпоративно-трудовых отношений (с. 56-58). Мне непонятно, почему «руководитель организации как единственное уполномоченное лицо, которое в полной мере от имени организации может участвовать в уголовном процессе» связан с «криминалистической деятельностью» и что соискатель понимает под этой деятельностью? По смыслу рассуждений диссертанта следует, что к «криминалистической деятельности» руководителя он относит принятие решения об обращении (не обращении) в правоохранительные органы при обнаружении признаков неправомерного доступа к охраняемой законом компьютерной информации. Но при чем здесь «криминалистическая деятельность»? Конечно же, диссертант имеет полное право на свою позицию в этом вопросе. Я же вслед за Р.С Белкиным считаю, что нет, и не может быть никакой «криминалистической деятельности» ни в процессе расследования, помимо деятельности процессуальной, оперативно-розыскной или административно-правовой, ни в процессе служебного расследования. Любая из форм деятельности может лишь рассматриваться в криминалистическом аспекте постольку, поскольку она допускает применение для ее осуществления криминалистических средств и приемов.

Тем не менее, автор занимает правильную позицию, утверждая, что «для минимизации имеющегося у субъектов корпоративно-трудовых отношений предкриминалистического риска на законодательном уровне (или на уровне локальных актов) следует установить особый порядок обращения в правоохранительных органы, а также активно применять такой достаточно эффективный правовой инструмент, как служебное расследование» (с. 63).

Верной является его мысль о том, что привлечение на этапе проверки информации о возможном совершении деяния, предусмотренного ст. 272 УК РФ, специалиста (специалистов) лицом, производящим расследование, может предотвратить, с одной стороны, негативные последствия, с другой, - «возможные нападки представителей стороны защиты, касающиеся его

технической некомпетентности, которые они могут предъявлять, в том числе и на судебных стадиях уголовного процесса» (с. 69).

Не обошел диссертант вниманием и рассмотрение ошибок, ведущих к наступлению криминалистического риска, в деятельности следователя и иных лиц на стадии предварительного расследования.

Здесь же достаточно подробно и аргументировано изложены рекомендации по минимизации негативных последствий при расследовании неправомерного доступа к охраняемой законом компьютерной информации, адресованные следователю, специалисту, эксперту, заявителю, руководителю следственного органа, прокурору и суду, представителю потерпевшего и свидетелю (с. 124-154).

Заключение содержит основные выводы и предложения автора по результатам исследования.

Оценивая в целом диссертационное исследование А.С. Вражнова, представляющее собой определенный вклад в теорию и практику расследования преступлений, связанных с неправомерным доступом к компьютерной информации, считаю целесообразным отметить некоторые спорные и даже неверные, с моей точки зрения, положения диссертации.

1. Диссертант определяет предмет исследования как «криминалистический риск, распространяющийся на деятельность участников уголовного судопроизводства и иных субъектов процесса расследования деяния, указанного в статье 272 УК РФ» (с. 7).

Предметом научного исследования во всех случаях является группа объективных закономерностей действительности, специфичных для данной отрасли научного знания. И в этом случае предметом диссертационного исследования является не сам криминалистический риск, а те закономерности, которые лежат в основе деятельности участников уголовного судопроизводства и иных субъектов процесса расследования неправомерного доступа к охраняемой законом компьютерной информации, включая закономерности формирования ошибочных действий и суждений этих лиц, приводящие к возможному наступлению негативных последствий, в том числе и к наступлению криминалистического риска.

2. На стр. 32 автор пишет: «...криминалистический риск можно моделировать, т.е. заведомо достаточно достоверно предположить, каким образом он будет проявляться у различных лиц в рамках расследования и уголовного судопроизводства».

Я не представляю, как можно моделировать «криминалистический риск», а вот смоделировать ситуации, в результате которых может наступить этот риск, представить не сложно.

Здесь же, подводя итог рассуждениям о возможности моделирования ситуации возникновения криминалистического риска, соискатель отмечает: «Вместе с тем моделирование широко применяется не только в следственной деятельности, но и в оперативно-розыскной практике, встречается у иных лиц, *в обязанности которых входит познание закономерностей совершения уголовно наказуемых деяний*» (курсив мой – Т.А.).

Как известно, познание закономерностей – это задача науки, а изучение закономерностей совершения преступления относится к области криминалистики. Хотелось бы узнать, кто относится к лицам, в обязанности которых входит познание закономерностей совершения уголовно наказуемых деяний, какое отношение имеют эти лица к непосредственно практической деятельности и почему познание закономерностей совершения уголовно-наказуемых деяний является их обязанностью.

3. По мнению диссертанта, возникновение рисков в рамках осмотра места происшествия при расследовании преступлений о неправомерном доступе к компьютерной информации обусловлено рядом составляющих, среди которых он называет: «риск при обеспечении состава следственно-оперативной группы необходимыми техническими средствами («компьютерный чемодан»)», в содержимое которого автор вслед за В.Е. Козловым и И.Г. Ивановой, предлагает включить «технические средства выявления радиопередатчиков и закладок на физическом уровне (аппаратные сканеры)» и «дополнительный источник питания, источники бесперебойного питания UPS, соединительные шнуры, кабели сетевого питания, гибкие кабели, активные терминаторы шин…» (с. 69-70); риск, связанный «с непониманием лица, ведущего следствие, основных технических моментов, с которыми ему предстоит столкнуться в процессе осмотра места происшествия». При этом по мнению соискателя, «технические возможности современных устройств достигли такого уровня», что стало достаточно «просто уметь пользоваться компьютером, обращаться с определенными программами (в особенности с текстовыми редакторами, эмуляторами, преобразователями форматов и т.д.), что под силу и малолетнему ребенку…» (с. 72-73).

Во-первых, непонятно, о каком возникновении риска здесь идет речь. Отсутствие комплекта аппаратного и программного обеспечения у

следователя при осмотре места происшествия может привести (а может и не привести) лишь к невыявлению информации, но не к риску.

Во-вторых, довольно сомнительным выглядит утверждение, что снабжение следователя комплектом аппаратного и программного обеспечение в виде «компьютерного чемодана», позволит минимизировать потери компьютерной информации, поскольку недостаточно иметь в наличии те или иные технические средства, нужно еще и уметь ими пользоваться.

В-третьих, нельзя забывать, что деятельность по выявлению «радиопередатчиков и закладок на физическом уровне» жестко регулируется законодательством (регуляторы: Федеральная служба по техническому и экспортному контролю – ФСТЭК и Федеральная служба безопасности – ФСБ) и требует обязательного лицензирования.

В-четвертых, имея представление о количестве и размерах тех составляющих, которые соискатель, вслед за рядом авторов предлагает в качестве содержимого включить в «компьютерный чемодан», не трудно заметить, что многое из перечисленного наверняка имеется в наличии непосредственно на местах происшествия, да и вряд ли найдется чемодан достаточных размеров, в который поместится такое количество технических средств.

Наконец, в-пятых. По смыслу рассуждений соискателя следует, что, не смотря на то, что технические возможности современных устройств достигли достаточно высокого уровня, тем не менее, стало достаточно просто уметь пользоваться компьютером, обращаться с определенными программами, в частности с эмуляторами. Полагаю, что не многие специалисты, а тем более малолетний ребенок, способны воспользоваться эмуляторами, выполняющими имитацию работы одной системы средствами другой без потери функциональных возможностей и искажения результата. Для этого необходимо, по крайней мере, владеть определенными знаниями, касающимися характеристик эмулируемой системы, например, о потребляемых ею ресурсах (от данной характеристики зависят настройки эмулятора, что, в свою очередь, влияет на достигаемые результаты).

Попутно замечу, что «неознакомление следователя с наглядно-схематичной информацией, касающейся планов офисного помещения, локальной сети организации, систем электронного учета рабочего времени в фирме, либо непроверки ее на соответствие объективным данным, которые устанавливаются в ходе осмотра этого оборудования» (с. 73) – это не составляющая риска, а обычная безграмотность и халатность следователя.

4. Серьезные сомнения вызывает позиция диссертанта, утверждающего, что на месте предполагаемого преступления можно обнаружить не только материальные, но и виртуальные следы. При этом он пишет, что информацию о материальных следах следователь получает «при физическом осмотре сервера, и периферийных компонентов, а также при анализе иных объектов, в которых могут отображаться данные о совершенном деянии», а виртуальные следы «можно обнаружить благодаря анализу ... системных параметров и настроек» ряда разделов реестра и каталогов, секций в файлах, открытых портов для выявления имеющихся на данный момент подключений к компьютеру, директорий и файлов и т.д. (с. 74).

Вряд ли можно признать такое деление следов на материальные и виртуальные справедливым, хотя бы потому, что так называемые виртуальные следы тоже материальны. Их образование происходит путем создания, модификации, удаления информации на машинном носителе и отражается в системных, временных, специализированных файлах, свойствах и метаданных файлов данных и т.п., а восприятие – всегда опосредовано через аппаратно-программные средства.

Хотелось бы, также услышать, что понимает автор под физическим осмотром сервера. Понятие сервера – неоднозначно. Это или обычный системный блок, на котором может быть запущено программное обеспечение, обслуживающее или управляющее другими компьютерами, или, в большинстве случаев, это система серверов (файл-сервер, почтовый сервер, WEB-сервер, FTP-сервер и т.д.). В чем будет здесь заключаться физический осмотр такого сервера, и какие цели преследует данный осмотр?

5. Рассуждая о возникновении рисков при анализе виртуальных следов, соискатель приходит к выводу, что они «несоизмеримо выше, чем при исследовании материальных предметов и компонентов» поскольку, с одной стороны, «определенная часть компьютерной информации может быть защищена криптографическим способом» (Луценко В.А.), с другой - это, обусловлено «особым механизмом «следообразования» в операционных системах ЭВМ, при котором не только бывают случаи умышленного удаления или изменения определенных сведений в компьютере, но и не исключается вероятность искажения или «затирания» каких-либо данных в результате системных ошибок или неумелых действий пользователя» (с. 75).

Но в чем здесь заключается риск? Только в том, что следователь не сумел подобрать пароль для расшифровки защищенных файлов, или не нашел при осмотре никаких файлов? Я не вижу здесь никакого

криминалистического риска. Риск возникает тогда, когда следователь действует в условиях неопределенности и понимает, что последствия этого могут быть как положительными, так и отрицательными.

6. Рассматривая возможность совершения специалистом ошибки в ходе осмотра места происшествия, которая может привести к криминалистическому риску, диссертант пишет, что она (ошибка) «может им не осознаваться и быть обусловлена его недостаточной технической подготовкой в конкретной ситуации, не зависящей от наличия у данного субъекта определенного опыта и квалификации. Ключевым здесь является сам факт невосприятия совершения лицом своей ошибки…», и в качестве примера он приводит банальную, по его словам, ситуацию, когда специалист при осмотре места происшествия устанавливает на *исследуемый* (курсив мой – Т.А.) компьютер определенный антивирус, не проверив его на наличие иной системы защиты или на коллективную совместимость» (с. 87).

По-моему, автор здесь допускает существенную ошибку. Устанавливать на исследуемый компьютер антивирус нельзя ни при каких условиях! Как правило, специалист должен извлечь машинный носитель, скопировать с него информацию и только потом работать с копией этой информации, а не с самим машинным носителем. Конечно, встречаются такие объекты, исследование которых без их включения невозможно или экономически нецелесообразно, но и на такие объекты ни при каких условиях не должны устанавливаться антивирусы!

7. Неубедительно выглядит аргументация соискателя по поводу того, что «криминалистический риск у эксперта всецело обусловлен возможностью совершения им ошибки при проведении экспертизы, формулировании выводов по ней и оформлении (представлении) результатов», в качестве которых, среди прочих, он называет «ошибки в результате аппаратных и (или) программных сбоев в работе ЭВМ, которые произошли … по не зависящим напрямую от действий тех или иных лиц обстоятельствам», приводя в качестве примера ситуацию, «когда в ходе экспертизы «MAC-адрес сетевой карты представленного на исследование компьютера определить не представилось возможным из-за повреждений материнской платы», или «в случаях, когда представленные на изучение объекты были уничтожены или повреждены определенными субъектами ранее». Подводя итог, диссертант констатирует, что «криминалистический риск в деятельности эксперта … состоит в том, что он может совершить ошибку, состоящую в неправильном реагировании на имеющиеся

технические сбои, когда с одной стороны, можно попытаться осуществить ремонт аппаратных средств компьютера или восстановить необходимую информацию, что позволит получить дополнительные сведения об объектах, представленных на исследование, а с другой стороны, в результате таких процессов есть вероятность окончательно уничтожить (повредить) оборудование или данные» (с.119-121).

Вряд ли обосновано отнесение к ошибкам эксперта того факта, что в ходе экспертизы «MAC-адрес сетевой карты представленного на исследование компьютера определить не представилось возможным из-за повреждений материнской платы», или «в случаях, когда представленные на изучение объекты были уничтожены или повреждены определенными субъектами ранее». Риск здесь, конечно есть, только он далеко не всегда связан с ошибочными действиями эксперта. Более информативным примером риска эксперта может быть, на мой взгляд, следующая ситуация. Эксперту необходимо исследовать информацию, расположенную на неисправном накопителе на жестких магнитных дисках (НЖМД). Попытка получения доступа к информации на НЖМД может привести к ее необратимым изменениям. Неразрушающих методов получения сведений о месте расположения поврежденных кластеров, объеме повреждений не существует. Эксперт может отказаться от проведения исследования или, изучив ситуацию, взвесив свои возможности, посоветовавшись с коллегами, рискнуть и с помощью специализированных программно-аппаратных средств провести копирование той части информации, к которой он смог получить доступ, на другой машинный носитель. Другими словами, эксперт рискует и рисковать можно, если он понимает, что после совершения какого-либо действия могут быть разные результаты, но он не может учесть все факторы (имеется некоторая неопределенность, которую нет возможности учесть – нет других источников информации), при этом считает возможным совершить некие действия, несмотря на эту неопределенность.

В диссертации имеются и некоторые иные погрешности, например, автор по ходу диссертации ссылается на работы ученых и практиков, большинство из которых являются достаточно старыми для столь быстро развивающейся отрасли; использует в разъяснениях компьютерный сленг (винчестер - НЖМД), а также то аппаратное и программное обеспечение, которое уже давно не выпускается (накопители SCSI и IDE, ленточный накопитель на 20–40 гигабайт и т.д.).

Изложенные мною замечания носят дискуссионный характер и не влияют на общую положительную оценку диссертационного исследования.

Основные положения диссертации отражены в публикациях, перечисленных в автореферате, который соответствует диссертации.

Оценивая работу Алексея Сергеевича Вражнова на тему: «Криминалистический риск при расследовании неправомерного доступа к компьютерной информации», представленную на соискание ученой степени кандидата юридических наук по специальности 12.00.12 (криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность), прихожу к выводу, что она представляет собой оригинальное монографическое исследование, обладающее необходимыми качествами научной новизны и практической значимости, удовлетворяющее требованиям п. 9 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства РФ от 24 сентября 2013 г. № 842, а соискатель заслуживает присуждения искомой ученой степени кандидата юридических наук по специальности 12.00.12 (криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность).

Официальный оппонент:
Заслуженный деятель науки РФ
доктор юридических наук (12.00.09 - уголовный процесс; криминалистика; оперативно-розыскная деятельность), профессор,
профессор кафедры управления органами расследования преступлений
Федерального государственного казенного образовательного учреждения высшего образования
«Академия управления Министерства внутренних дел Российской Федерации»

Татьяна Витальевна Аверьянова

19.11.2015 г.

Почтовый адрес: 125171, г. Москва, ул. Зои и Александра Космодемьянских, д. 8
Тел.: (499) 745-95-73
E-mail: avers52@yandex.ru

Подпись Аверьянова Т.В. заверяю:
Заместитель начальника ОДиР
С.А. Мутолапова