Вражнов Алексей Сергеевич. Криминалистический риск при расследовании неправомерного доступа к компьютерной информации : диссертация ... кандидата юридических наук: 12.00.12 / Вражнов Алексей Сергеевич;[Место защиты: Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный университет правосудия»].- Москва, 2015.- 218 с.

**Содержание к диссертации**

Введение

**Глава 1. Криминалистический риск как составляющая часть процесса расследования преступлений 15**

1. Понятие, значение и классификация категории «криминалистический риск» 15

2. Криминалистический риск при проведении следственных действий, тактических операций и комбинаций 39

**Глава 2. Анализ предкриминалистического и криминалистического рисков при обнаружении и расследовании неправомерного доступа к компьютерной информации 50**

1. Обнаружение неправомерного доступа к компьютерной информации в условиях предкриминалистического риска 50

2. Криминалистический риск в деятельности участников уголовного судопроизводства и иных субъектов процесса расследования при возбуждении уголовного дела, предусмотренного статьей 272 УК РФ 64

3. Деятельность следователя и иных лиц в условиях криминалистического риска на стадии предварительного расследования неправомерного доступа к компьютерной информации 98

4. Методические рекомендации, направленные на снижение криминалистического риска при расследовании неправомерного доступа к компьютерной информации 124

Заключение 155

Список использованных источников .

**Введение к работе**

**Актуальность темы исследования.** Понятие «криминалистический риск» было впервые сформулировано в 1990 году, однако и в настоящее время не прекращается научная дискуссия о значении данной категории для процесса раскрытия и расследования преступлений. Ряд ученых определяют криминалистический риск только как теоретическую категорию, не имеющую отношения к деятельности участников уголовного судопроизводства и иных лиц, способствующих расследованию того или иного преступления. Вместе с тем представляется, что данная категория имеет и практическую направленность, изучение которой позволит снизить вероятность совершения ошибок вышеназванными лицами и повысить эффективность расследования конкретных видов преступлений.

Предпочтение рассмотрения криминалистического риска на примере расследования деяния, указанного в статье 272 УК РФ, перед другими видами преступлений обусловлено следующими причинами.

Во-первых, внедрение современных информационных технологий в деятельность как физических, так и юридических лиц привело к увеличению количества и усложнению качественной составляющей совершаемых преступлений, предусмотренных главой 28 УК РФ, основное место среди которых занимает неправомерный доступ к компьютерной информации.

Во-вторых, учитывая специфику данного деяния, для осуществления которого необходимы специальные знания в области информационных технологий, появляется возможность не только исследовать «традиционные» ошибки, присущие следователю и сотрудникам оперативно-розыскных органов вне зависимости от вида преступления, но и установить особенности просчетов данных лиц, а также сведущих субъектов (эксперта, специалиста) в процессе выявления и расследования неправомерного доступа к компьютерной информации.

В-третьих, в отличие от ряда иных деяний, при расследовании неправомерного доступа к компьютерной информации, до настоящего времени мало внимания уделяется конкретным ситуациям, встречающимся в деятельности тех или иных субъектов, участвующих в производстве по данному преступлению.

Учитывая вышесказанное, представляется актуальным, рассмотреть теоретическое и практическое значение категории «криминалистический риск» в расследовании конкретного вида преступления - неправомерного доступа к компьютерной информации.

**Степень научной разработанности темы.** Теоретические основы криминалистического риска были заложены в трудах отдельных ученых: родоначальника данного понятия Г. А. Зорина, описавшего его природу, структуру, виды и критерии оценки, а также Н. П. Яблокова, указавшего на его применимость к деятельности следователя в сложных проблемных ситуациях. Ряд исследователей, в первую очередь, С. С. Арсентьева, О. А. Луценко и О. А. Нурутдинов, критически отнеслись к существованию криминалистического риска и (или) криминалистической ситуации, посчитав, что данные термины имеют только научную направленность и не присущи практической деятельности участников уголовного судопроизводства и иных субъектов, способствующих расследованию преступлений.

Методические рекомендации, посвященные расследованию

компьютерных преступлений в целом, и деяния, указанного в статье 272 УК РФ, в частности, широко представлены в современной научной и практической юридической литературе. В периодических трудах уделяется внимание особенностям производства отдельных следственных действий и оперативно-розыскных мероприятий (В. Б. Вехов, М. В. Гаврилов, А. Н. Иванов, В. И. Комиссаров, А. Л. Осипенко, Н. А. Подольный и др.). В монографиях и научно-практических пособиях исследуется криминалистическая характеристика деяния, указанного в статье 272 УК РФ и обсуждаются проблемы, возникающие у следователя и иных лиц в рамках

**5** первоначального и последующего этапов расследования неправомерного доступа к компьютерной информации (А. В. Варданян, Е. П. Ищенко, В. Е. Козлов, А. Н. Литвинов, В. А. Мещеряков, Е. В. Никитина, М. В. Салтевский, Н. Г. Чернец и др.). Отдельные работы посвящены судебной компьютерно-технической экспертизе и ее видам (Е. Р. Российская, А. И. Семикаленова, А. И. Усов и др.). Кроме этого имеется ряд диссертационных исследований: Ю. В. Гаврилин «Расследование неправомерного доступа к компьютерной информации» (Москва, 2000 г.),

A. С. Егорышев «Расследование и предупреждение неправомерного доступа к  
компьютерной информации» (Уфа, 2004 г.), И. Г. Иванова «Выявление и  
расследование неправомерного доступа к компьютерной информации»  
(Красноярск, 2007 г.).

Формированию целостного представления о криминалистическом риске способствовали работы отечественных ученых, рассматривающих аспекты информационной неопределенности, присущие деятельности различных участников судопроизводства, вопросы ситуалогии и моделирования (Т. С. Волчецкая, В. К. Гавло, Л. Я. Драпкин, Д. В. Ким, А. Ф. Облаков, Н. А. По дольный, А. Е. Шуклин и др.), особенности производства отдельных следственных действий, тактических операций и комбинаций (Т. В. Аверьянова, И. А. Макаренко, В. А. Образцов, М. В. Савельева,

B. В. Степанов, А. А. Чебурёнков, Л. Г. Шапиро, Н. Г. Шурухнов,  
А. А. Эксархопуло и др.), а также выделяющих те или иные виды рисков,  
существующих в криминалистике (Р. С. Белкин, И. Ф. Герасимов, А. Ф. Лубин,  
О. А. Нурутдинов, И. Н. Озеров, Ю. Ю. Осипов, А. Ю. Шумилов, Н. П. Яблоков  
и др.).

**Цели и задачи исследования.** Целью настоящей работы является развитие научных положений учения о криминалистическом риске (криминалистической рискологии), направленных на повышение эффективности расследования преступлений в общем, и неправомерного доступа к компьютерной информации в частности.

**6** Для достижения вышеназванной цели были поставлены следующие задачи:

- анализ категории «криминалистический риск», построение ее  
классификации и установление значения в процессе расследования  
преступлений;

- установление практической значимости определения  
криминалистического риска при производстве следственных действий,  
тактических операций и комбинаций вне зависимости от вида преступлений;

- исследование юридической природы риска в рамках процедуры  
обнаружения неправомерного доступа к компьютерной информации  
субъектами корпоративно-трудовых правоотношений;

- выявление основных видов криминалистического риска в деятельности,  
следователя, сотрудников оперативно-розыскных 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.

**Объект и предмет исследования.** Объектом исследования является преступная деятельность, направленная на неправомерный доступ к компьютерной информации, и деятельность участников уголовного судопроизводства и иных субъектов процесса расследования данного вида преступления, в условиях криминалистического риска.

Предметом исследования выступает криминалистический риск, распространяющийся на деятельность участников уголовного судопроизводства и иных субъектов процесса расследования деяния, указанного в статье 272 УК РФ.

**Методология и методы исследования.** Методологическую основу настоящей работы составляет всеобщий метод познания - диалектический материализм. В работе также использовались следующие общенаучные и частнонаучные методы: анализ, синтез, индукция, дедукция, аналогия, обобщение, системно-структурный, моделирование, формально-юридический, сравнительно-правовой, экспертный опрос, анализ документов.

**Правовая основа исследования** включает нормативные положения, закрепленные в Конституции Российской Федерации, УК и УПК РФ, иных законах и подзаконных актах (ТК РФ, ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства», «О государственной судебно-экспертной деятельности в Российской Федерации», «О коммерческой тайне», «Об адвокатской деятельности и адвокатуре в Российской Федерации», «Об оперативно-розыскной деятельности», Приказ МВД РФ, Минобороны РФ, ФСБ РФ, ФСО РФ, ФТС РФ, СВР РФ, ФСИН РФ, ФСКН РФ, СК РФ «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд»).

**Теоретическую основу исследования** составили фундаментальные научные труды и учебные пособия в области криминалистики и уголовного процесса под авторством Т. В. Аверьяновой, Р. С. Белкина, Т. С. Волчецкой, В. К. Гавло, И. Ф. Герасимова, Л. Я. Драпкина, Г. А. Зорина, Е. П. Ищенко, Д. В. Кима, В. И. Комиссарова, А. Ф. Облакова, Е. Р. Российской, А. И. Усова, А. Ю. Шумилова, Н. Г. Шурухнова, А. А. Эксархопуло, Н. П. Яблокова и других ученых.

Кроме этого, в диссертации использованы работы А. П. Альгина, В. Б. Вехова, А. Е. Войскунского, В. М. Гранатурова, Т. Кленовой, В. Е. Козлова, В. А. Копылова, Е. Никитина, О. Д. Ситковской, О. Б. Скородумовой, А. Сугано, Н. И. Тимофеева, Л. Н. Тэпмана и иных исследователей, выполненные в рамках отраслевых юридических наук, включающих уголовное,

**8** гражданское и трудовое право, а также криминологии, психологии, социологии, философии, экономической теории и защиты компьютерной информации. **Эмпирической основой исследования** выступили:

материалы более 300 уголовных дел, рассмотренных судами общей юрисдикции различных субъектов Российской Федерации за 2010-2013 годы по статье 272 УК РФ, изученные и обобщенные с помощью информационно-правовой системы «Актоскоп» (ИПС «Актоскоп»);

материалы более 40 уголовных дел Ленинского и Пролетарского районных судов г. Саранска Республики Мордовия за 2001-2010 годы по статье 272 УК РФ;

- результаты опроса 50 лиц из числа руководящего персонала  
(генеральные директора (директора), члены Совета директоров, акционеры  
(участники) компаний) коммерческих и некоммерческих организаций;

результаты опроса 50 лиц, являющихся 1Т-специалистами (операторы, программисты, иные лица, связанные с информационными технологиями) коммерческих и некоммерческих организаций;

личный опыт соискателя в проведении служебных проверок по фактам несанкционированного доступа к компьютерной информации.

**Научная новизна исследования** заключается в предложении авторского подхода к определению понятия «криминалистический риск» (с учетом его соотношения с тактическим риском); выявлении факторов криминалистического риска; определении возникновения ситуаций предкриминалистического и ситуаций собственно криминалистического риска; классификации ошибок допускаемых участниками уголовного судопроизводства и иными субъектами процесса расследования неправомерного доступа к компьютерной информации, как основы формирования криминалистического риска; разработке методических рекомендаций, направленных на снижение криминалистического риска на стадиях возбуждения уголовного дела и предварительного расследования деяния, указанного в статье 272 УК РФ.

**9** **Положения, выносимые на защиту**

1. Авторские определения понятий «криминалистический риск» и  
«ситуация информационной неопределенности в криминалистике»:

криминалистический риск - это вероятность совершения ошибки участником уголовного судопроизводства и иным субъектом процесса расследования преступлений в условиях выбора определенного решения, обусловленного сложившейся криминалистической ситуацией;

ситуация информационной неопределенности в криминалистике - это ситуация, при которой участник уголовного судопроизводства и иной субъект процесса расследования преступлений на любой стадии судопроизводства не располагает полным объемом сведений о каких-либо обстоятельствах расследуемого (рассматриваемого) дела, или не воспринимает их должным образом в силу своей самонадеянности, невнимательности, а также по причине отсутствия определенных знаний и вследствие этого в его деятельности присутствует криминалистический риск.

1. Вывод автора о различии понятий «тактический риск» и «криминалистический риск», которые соотносятся между собой как часть и целое, а также имеют разный круг подверженных им лиц и пределы распространения в рамках процесса раскрытия и расследования преступлений.
2. Выявленные автором факторы, влияющие на криминалистический риск, в деятельности следователя (дознавателя) при производстве следственных действий:

- временной криминалистический фактор (сокращение или расширение  
интервала сбора доказательственной информации в зависимости от вида  
преступления);

- пространственно-территориальный криминалистический фактор  
(возможность извлечения доказательственной информации из отдельных  
объектов окружающей действительности);

- личностный криминалистический фактор (опыт, профессиональное  
мастерство, уровень правосознания, свойства характера и особенности  
темперамента).

4. Сформулированное автором понятие «предкриминалистический риск»,  
под которым предложено понимать вероятность совершения ошибки  
участником корпоративно-трудовых отношений до обращения в  
правоохранительные органы с заявлением о совершенном преступлении в  
порядке статьи 23 УПК РФ в условиях выбора конкретного решения,  
обусловленного сложившейся ситуацией.

Диссертантом предложены меры для минимизации

предкриминалистического риска, заключающиеся в установлении на законодательном уровне (или на уровне локальных актов) особого порядка обращения в правоохранительные органы, а также в активном использовании служебного расследования.

5. Автором выработана классификация типичных видов ошибок,  
обусловленных криминалистическим риском, в зависимости от субъектного  
состава и стадии уголовного судопроизводства, применительно к процессу  
расследования неправомерного доступа к компьютерной информации:

- ошибки следователя при производстве следственных действий, при  
использовании результатов ОРД, при задержании лица, непричастного к  
совершенному деянию, при возбуждении уголовного дела, при вынесении  
постановления о привлечении определенного лица в качестве обвиняемого, при  
составлении обвинительного заключения в отношении определенного лица, при  
прекращении уголовного дела и (или) уголовного преследования;

- ошибки сотрудников, осуществляющих оперативно-розыскные  
мероприятия в ходе проведения опроса и наведения справок;

ошибки специалиста при использовании им специальных знаний;

ошибки эксперта при проведении судебной компьютерно-технической экспертизы (СКТЭ), формулировании выводов по ней и оформлении (представлении) результатов;

ошибки заявителя, обусловленные возможностью его представления следователю (сотрудникам оперативно-розыскных органов) ненадлежащего комплекта локальных документов, необходимого для установления деяния, подпадающего под неправомерный доступ к компьютерной информации;

ошибки представителя потерпевшего и свидетеля, которые вызваны непредставлением ими в правоохранительные органы сведений об имеющихся угрозах личной безопасности, сообщением информации, основанной на догадке, предположении или слухе, представлением доказательств и заявлением ходатайств;

- ошибки руководителя следственного органа, прокурора и суда,  
связанные с выполнением этими органами и должностными лицами  
контрольно-надзорных функций в отношении субъекта, производящего  
расследование и сотрудников, осуществляющих ОРД.

6. Разработанные автором методические рекомендации, направленные на снижение криминалистического риска при расследовании неправомерного доступа к компьютерной информации, наиболее важными из которых, наряду с положениями, применимыми к большинству иных преступлений, а также мерами, заключающимися в повышении образовательного уровня отдельных субъектов, являются следующие:

- выполнение следователем в ходе осмотра места происшествия и обыска  
комплекса мероприятий, заключающихся в получении и проверке информации  
об имеющейся в офисном помещении компьютерной техники, лицах,  
ответственных за ее использование, особенностях организации локальной сети  
и систем пропускного контроля, а также осуществлении действий,  
направленных на недопущение уничтожения злоумышленником определенных  
данных с ЭВМ и обнаружение материальных и виртуальных следов  
совершенного деяния;

- получение следователем при подготовке и производстве допросов  
подозреваемого (обвиняемого) информации о посещенных им web-порталах,  
имеющихся счетах в электронных платежных системах и движения по ним,

**12** функциональности найденного аппаратного (программного) обеспечения и принадлежности его определенным лицам;

- использование следователями, занимающимися расследованием  
неправомерного доступа к компьютерной информации, и специалистами,  
оказывающими им содействие в данной деятельности, специализированного  
аппаратного и программного обеспечения («компьютерный чемодан  
следователя» и «чемодан компьютерного специалиста»);

создание в каждом субъекте РФ «баз специалистов», которые, как свидетельствуют результаты проведенных опросов, можно формировать в том числе и из штатных 1Т-специалистов организаций;

проведение по определенному алгоритму служебных проверок в организациях, направленных на выяснение, действительно ли было совершено преступление, подпадающее под действие статьи 272 УК РФ.

**Теоретическая значимость работы** определяется содержанием сформулированных положений и выводов, которые могут быть использованы в ходе дальнейшей разработки учения о криминалистическом риске (криминалистической рискологии), в рамках общей теории криминалистики, и развития методики расследования неправомерного доступа к компьютерной информации, в рамках криминалистической методики.

**Практическая значимость работы** заключается в выявлении ошибок, влияющих на исход расследования правоохранительными органами преступлений, предусмотренных статьей 272 УК РФ, и разработке рекомендаций, направленных на их предотвращение; благодаря предложенному пошаговому алгоритму она будет полезна при внутренних проверках в организациях, когда есть сведения о возможном несанкционированном доступе к компьютерной информации; отдельные положения настоящего исследования могут использоваться в преподавании криминалистики и смежных с ней курсов в юридических учебных заведениях и в институтах (на факультетах) повышения квалификации.

**Степень достоверности и апробация результатов.**

Основные теоретические положения и практические рекомендации сообщались на международных научно-практических конференциях «Проблемы применения норм права в условиях модернизации российского общества и государства» (г. Челябинск, 2011 г.), «Европейская наука XXI века -2011» (г. Пшемысль, 2011 г.), «Актуальные проблемы современной криминалистики и судебной экспертизы» (г. Минск, 2011 г.), «Право и его реализация в XXI веке» (г. Саратов, 2011 г.), «Актуальные проблемы уголовного права, процесса и криминалистики» (г. Одесса, 2011 г.), «Эволюция государства и права: история и современность» (г. Курск, 2011 г.), «Перспективы развития уголовно-процессуального права и криминалистики» (г. Москва, 2012 г.), «Татищевские чтения: актуальные проблемы науки и практики» (г. Тольятти, 2012 г.), «Теория доказательств и практика расследования экономических и иных преступлений» (г. Нижний Новгород, 2012 г.) «Актуальные проблемы уголовного процесса и криминалистики» (г. Волгоград, 2012 г.), «Вопросы юриспруденции: история, теория, современность» (г. Краснодар, 2012 г.), «Криминалистические чтения, посвященные памяти заслуженного юриста Республики Беларусь, доктора юридических наук, профессора Г. И. Грамовича» (г. Минск, 2012 г.), «Актуальные проблемы совершенствования законодательства и правоприменения» (г. Уфа, 2013 г.); Всероссийских научно-практических конференциях «Проблемы реализации прав человека: история и современность» (г. Саранск, 2010 г.), «Юридическая наука и правоприменение» (г. Саратов, 2012 г.).

Результаты исследования, касающиеся методики расследования неправомерного доступа к компьютерной информации, используются в практической деятельности отдела уголовного розыска и следственного управления МУ МВД России «Мытищинское».

Положения диссертации в части рекомендаций при проведении служебных проверок в организациях в случае наличия данных о возможном несанкционированном доступе к компьютерной информации внедрены

**14** в практическую деятельность следующих юридических лиц: Ассоциация содействия развитию агротуризма «АгроТуризмАссоциация», Закрытое акционерное общество «Инжиниринговая компания «СтройМодернизация», Общество с ограниченной ответственностью «Компания ДЭЗ А» и т.д.

**Структура диссертации** обусловлена целью, задачами и ходом исследования. Настоящая работа состоит из введения, двух глав, включающих шесть параграфов, заключения и шести приложений.

## Криминалистический риск при проведении следственных действий, тактических операций и комбинаций

Так, например, согласно взглядам А. Ю. Шумилова, оперативный риск понимается через призму обстоятельства, исключающего преступность деяния, как «разновидность обоснованного профессионального риска»21. Автор указывает, что «риск оперативный признается правомерным при соблюдении следующих условий: он должен быть вызван необходимостью достижения социально полезной цели (предупреждение совершения преступления, угрожающего жизни человека, и т.п.); предполагаемая цель не может быть достигнута не связанными с риском оперативным действиями; участник ОРД (КРД), пошедший на риск (оперативник, агент и др.), обязан принять все необходимые меры для предупреждения вероятного вреда охраняемым оперативно-розыскным законом объектам (согласно ст. 1 ФЗ об ОРД – человек, собственность, общество и гос-во)»22.

Что касается следственного риска, то, по мнению Н. П. Яблокова, «это специфическое поведение следователя в ходе расследования, направленное на решение задач, отягощенных объективной вероятностью их недостижения и содержащее возможность наступления отрицательного результата или отрицательных последствий. Следственный риск по его значимости для расследования может быть тактическим и стратегическим. Первый распространяется на отдельные следственные действия, тактические операции и комбинации. Его возможные и наступившие отрицательные последствия чаще всего оказывают непродолжительное негативное влияние на ход расследования. Второй охватывает значительное число следственных действий и операций или расследование в целом. Поэтому его отрицательные результаты распространяются на длительный период расследования и даже могут привести его к неуспеху»23. Помимо монографий, в диссертационных исследованиях тактическому и оперативному рискам также было уделено внимание. Это подтверждается работами И. Н. Озерова «Категория риска в оперативно-розыскной деятельности»24 и Ю. Ю. Осипова «Деятельность следователя в условиях тактического риска» 25. Кроме этого, в научной литературе высказывается точка зрения, которая по своей сущности объединяет тактический, оперативный и следственный риски. Так, по мнению А. Ф. Лубина, Е. Е. Кондратьевой и О. А. Нурутдинова, «под риском понимается система следственных и оперативных действий, направленных на формирование системы обвинительных доказательств, с наличием прогнозных оценок по вероятности достижения поставленной цели» 26. Была предпринята попытка расширить круг субъектов, подвергающихся риску. Так, П. Кабанов в научной статье «Риск при расследовании преступлений» в их состав, помимо следователя и работника дознания, ввел еще и прокурора 27.

И, наконец, переходя непосредственно к термину «криминалистический риск», отметим, что он был впервые предложен в 1990 году Г.А. Зориным в монографии с одноименным названием, и понимался, как «действие или бездействие по поводу расследуемого преступления, направленное на цель, отягощенную объективной вероятностью недостижения, субъективированное определенным лицом, предполагающим альтернативный результат (успех-неуспех)»28. Схожее определение криминалистического риска было дано Н. П. Яблоковым, который понимал его как «специфическое поведение следователя в ходе расследования, направленное на разрешение задач, отягощенных объективной вероятностью их недостижения, и содержащее . возможность наступления отрицательного результата или отрицательных последствий»29. На наш взгляд, криминалистический риск – основная черта не только следственной, но и судебной, экспертной и иной практической деятельности всех основных участников уголовного судопроизводства и иных субъектов процесса расследования преступлений, за исключением в подавляющем большинстве случаев защитника и подозреваемого (обвиняемого, подсудимого, осужденного, оправданного)30. Данный риск возникает с момента обнаружения следователем (дознавателем, органом дознания, руководителем следственного органа) определенного деяния, которое содержит признаки преступления. Моментом окончания криминалистического риска можно считать вступление приговора (определения, постановления) суда в законную силу, и его исполнение надлежащим государственным органом, кроме случаев, предусмотренных разделом Уголовно-процессуального кодекса Российской Федерации31. Криминалистический риск присутствует при расследовании и уголовном судопроизводстве абсолютно по всем категориям дел, независимо от их сложности, распространенности и иных факторов. Принимая во внимание, что следственные, экспертные, оперативно-розыскные и иные ситуации являются динамическими моделями, нужно отметить, что любое «простое» уголовное дело может в определенный момент стать «трудноразрешимым» в силу неопытности следователя, иных лиц, уполномоченных производить расследование, выполнять исследования, или участвовать в следственных действиях и иных мероприятиях, или, наоборот, в связи с излишней самоуверенностью данных субъектов в своих действиях, оставлением без внимания личностных качеств подозреваемого (обвиняемого), несовершенством технической базы, нарушением уголовного и уголовно-процессуального законодательства и другими причинами. В связи с этим ошибочной представляется точка зрения С. С. Арсентьевой, которая отрицательно относится к допустимости риска при простых криминалистических ситуациях, аргументируя тем, что это «снижает критерии требовательности к деятельности следователя, поскольку любые его непродуманные и явно ошибочные действия можно объяснить тем, что следственная деятельность всегда сопряжена с риском и потому “неуспех” – один из вполне закономерных результатов»32.

## Криминалистический риск в деятельности участников уголовного судопроизводства и иных субъектов процесса расследования при возбуждении уголовного дела, предусмотренного статьей 272 УК РФ

В соответствии с Уголовно-процессуальным кодексом, до момента возбуждения уголовного дела могут производиться лишь отдельные следственные действия, а также осуществляется сбор справочно информационной, документальной и иной информации о произошедшем событии. Цель всех этих мероприятий – выяснить, имеются ли достаточные данные, дающие основание полагать, что совершено преступление и соответственно есть ли основание для возбуждения уголовного дела или нет.

Вместе с тем деяние, указанное в статье 272 УК РФ, имеет свою специфику, заключающуюся в том, что «факт неправомерного доступа к информации в компьютерной системе или сети обычно первыми обнаруживают сами же пользователи информационной системы»83.

Учитывая это, следует напомнить, что, помимо общего порядка возбуждения дела в рамках УПК РФ, существует статья 23, которая регулирует специфическую процедуру привлечения к уголовному преследованию за отдельные преступления, предусмотренные в главе 23 УК РФ. Суть данной статьи заключается в том, что руководитель юридического лица должен оценить целесообразность подачи заявления о преступлении, совершенном в отношении фирмы, которую он возглавляет, в условиях, когда вред был причинен исключительно интересам данной организации. А так как руководитель организации, являющийся единоличным исполнительным органом, не всегда может в полной мере объективно и всесторонне осознавать тактические и стратегические последствия данного заявления в правоохранительные органы для репутации юридического лица или, напротив, не реагировать на совершаемые преступные действия против интересов компании в силу различных обстоятельств, то в научной литературе неоднократно поднимался вопрос о наличии недостатков в конструкции статей 201 УК РФ (примечания 2 и 3) и 23 УПК РФ и предлагались различные варианты их разрешения: от введения единообразия юридической терминологии уголовного и уголовно процессуального права по данной проблеме84 до исключения вышеназванных норм из кодексов85. По нашему мнению, наиболее обоснованной, являлась точка зрения А. Ю. Федорова, который систематизировал информацию предыдущих исследователей и предложил новые редакции вышеназванных статей в уголовном и уголовно-процессуальном кодексе86, в которых рекомендовал расширить круг субъектов, уполномоченных подавать заявление о возбуждении уголовного дела (включив в данный перечень акционеров, членов совета директоров, наблюдательного совета)87. Однако исследователь не учел нескольких моментов. Первый из них касается сообщения о согласии на возбуждение уголовного дела. В российском законодательстве не определен сам порядок дачи в правоохранительные органы такого согласия, отсутствует перечень документов, которые необходимо истребовать от заявителя, не указывается круг лиц, уполномоченных на данное обращение. Соответственно, может возникнуть ситуация, когда руководитель организации поручил какому-нибудь ее сотруднику обратиться в правоохранительные органы, а потом заявил, что не наделял данными полномочиями работника, сообщившего о произошедшем преступлении. В связи с этим представляется целесообразным совсем исключить из текста статьи 23 УПК РФ словосочетание «или с его согласия». Второй момент заключается в круге субъектов, уполномоченных заявлять о совершении преступления. По нашему мнению, предложенный А. Ю. Федоровым перечень является неполным, так как нужно помнить, что, помимо руководящих сотрудников организации, имеются и иные работники, которые также заинтересованы в нормальной и стабильной работе компании по различным причинам: материального характера, организационного плана, общих идей и целей и т.д.

В связи с этим необходимо отметить отдельные нормативно-правовые гарантии для членов рабочего коллектива, в данной сфере которые имеются в Трудовом кодексе Российской Федерации. Например, статьей 21 ТК РФ закреплено право работников на «участие в управлении организацией в предусмотренных настоящим Кодексом, иными федеральными законами и коллективным договором формах». Перечень основных форм участия работников в данной деятельности имеется в статье 53 ТК РФ и не является исчерпывающим. В рамках нашего исследования сосредоточим научный интерес на праве работников на управление организацией в непосредственной форме через общие собрания, минуя деятельность профсоюзов и иных представительных органов. Соответственно из перечисленных в статье 53 Трудового кодекса форм участия с учетом предложенных нами рамок остаются следующие: 1) получение от работодателя информации по вопросам, непосредственно затрагивающим интересы работников; 2) обсуждение с работодателем вопросов о работе организации, внесение предложений по ее совершенствованию; 3) участие в разработке и принятии коллективных договоров. Данную форму отдельные ученые, например О. В. Смирнов, считают «наиболее ярким примером непосредственного участия работников в установлении условий труда и управлении организацией»88, с чем вполне можно согласиться.

Кроме этого, в рамках отдельно взятой компании могут предусматриваться локальные акты, дающие дополнительные полномочия работникам.

Вместе с тем одним расширением их правового статуса нельзя обойтись. Современное уголовно-процессуальное законодательство нуждается в некоторых изменениях в части увеличения групп преступлений, подпадающих под условия статьи 23 УПК РФ89. В частности, кроме деяний, предусмотренных главой 23 Уголовного кодекса Российской Федерации, к ним следует отнести компьютерные преступления, закрепленные статьями 272 и 274 УК РФ90.

## Деятельность следователя и иных лиц в условиях криминалистического риска на стадии предварительного расследования неправомерного доступа к компьютерной информации

В предыдущем параграфе настоящей главы отмечалось, что криминалистическому риску при возбуждении уголовного дела по статье 272 УК РФ подвергаются такие лица, как следователь, сотрудники оперативно-розыскных органов, специалист, эксперт, заявитель, прокурор, руководитель следственного органа и суд. В свою очередь на стадии предварительного расследования неправомерного доступа к компьютерной информации возможностям совершения ошибок, обусловленных криминалистическим риском, подвергается большее количество субъектов, к числу которых, помимо лиц, указанных при возбуждении уголовного дела, следует отнести также свидетеля. В рамках настоящего параграфа раскроем проявления криминалистического риска у представителей обозначенного нами круга участников и опять начнем с лица, производящего расследование.

Ранее нами были рассмотрены три основных вида криминалистического риска в деятельности следователя на стадии возбуждения уголовного дела по статье 272 УК РФ, которые касались возможности совершения ошибок данным субъектом при осмотре места происшествия, при использовании результатов ОРД, а также при возбуждении уголовного дела. В рамках предварительного расследования деятельность лица, ведущего следствие, также подвержена такому явлению, как криминалистический риск, который может проявляться в большем числе видов: 1) риск задержания лица, непричастного к совершенному деянию; 2) риск при избрании меры пресечения в отношении подозреваемого (обвиняемого); 3) риск при производстве следственных действий, тактических операций и комбинаций; 4) риск при использовании результатов оперативно-розыскной деятельности (статья 89 УПК РФ); 5) риск при вынесении постановления о привлечении определенного лица в качестве обвиняемого; 6) риск при составлении обвинительного заключения в отношении определенного лица; 7) риск прекращения уголовного дела и (или) уголовного преследования. Первый вид криминалистического риска, касающийся задержания лица179, по нашему мнению, заключается в возможности применения данной меры процессуального принуждения к субъекту, который непричастен к произошедшему деянию, содержащему признаки преступления, предусмотренного статьей 272 УК РФ, однако обладает специальными знаниями в компьютерной сфере, имеет (имел, мог иметь) доступ к локальной сети, серверу или сайту организации и не исключено, что, возможно, был заинтересован (по различным причинам) в несанкционированном доступе к соответствующей информации. В роли таких субъектов может выступать широкий круг участников: сотрудники компании (как непосредственно IT-специалисты, так и иные работники, обладающие навыками системного администрирования и программирования, о чем известно их коллегам в фирме); родственники и друзья кого-либо из персонала организации, которые часто заходят в офисные помещения и считаются уже как бы «своими» на данном предприятии; недавно уволенные лица, имеющие несданные карты доступа к пропускным системам, и т.д. Указывая на вышеназванных лиц как на субъектов, которые совершили неправомерный доступ к компьютерной информации, руководитель организации (или иной уполномоченный сотрудник фирмы) может как действительно ошибаться в своих выводах180, так и сознательно, в силу личной неприязни к определенному человеку, сообщить в правоохранительные органы информацию о его безусловном участии в совершенном противоправном деянии181. Учитывая, что в сложившихся условиях субъект, производящий расследование, сразу не имеет возможности проверить достоверность информации, полученной от таких уполномоченных представителей потерпевшего, он, скорее всего, примет решение о задержании лица, на которого было указано как на совершившее неправомерный доступ к компьютерной информации, собственником которой является юридическое лицо, и вплотную сосредоточится на проведении комплекса процессуальных действий с этим подозреваемым, прекратив или резко уменьшив при этом активность разработки иных возможных версий совершенного преступления.

Второй вид криминалистического риска обусловливается возможностью подачи в суд ходатайства о необходимости назначения или непосредственном применении следователем по отношению к подозреваемому (обвиняемому) определенной меры пресечения, которая не отвечает требованиям сложившейся ситуации. Это может, в частности, выражаться в избрании несоразмерно более строгой или, наоборот, слишком мягкой меры пресечения, а также в применении ее вообще (в том числе к непричастному субъекту) или отказе в таковом. В рамках настоящего диссертационного исследования в связи с тем что единственной мерой пресечения, применяемой к субъекту, подозреваемому или обвиняемому в неправомерном доступе к компьютерной информации, в исследованных нами уголовных делах являлась подписка о невыезде 182, ограничивающая права и свободы лица, в отношении которого она была избрана, в наименьшем объеме183, и принимая во внимание степень общественной опасности деяния, предусмотренного статьей 272 УК РФ, данный вид криминалистического риска, а в дальнейшем и меры по его минимизации рассматриваться не будут.

Третий вид криминалистического риска заключается в возможности совершения ошибок лицом, производящим расследование неправомерного доступа к компьютерной информации, в ходе следственных действий, тактических операций и комбинаций. В настоящей работе по причине того, что в научной литературе до сих пор не разработаны тактические операции и комбинации, применяемые только при расследовании деяния, предусмотренного статьей 272 УК РФ184, будем изучать вышеназванный вид криминалистического риска, ограничиваясь лишь таким компонентом, как следственные действия, в роли которых, учитывая особенности предмета доказывания неправомерного доступа к компьютерной информации, на данной стадии уголовного судопроизводства чаще всего выступают осмотр места происшествия, обыск, допрос, а также судебная экспертиза.

## Методические рекомендации, направленные на снижение криминалистического риска при расследовании неправомерного доступа к компьютерной информации

В итоге после анализа опросов данных лиц сотрудники оперативно-розыскных органов будут располагать более системной и структурированной информацией, чем только при получении объяснений от технических специалистов в организации. Содержание полученных сведений заключается в следующем: 1) будет ориентировочно выяснен круг субъектов (внешний и внутренний), у которых имеется заинтересованность в неправомерном доступе к компьютерной информации в отношении данной компании по различным мотивам; Хотя и процесс получения объяснений от данного сотрудника нельзя проводить формально, в ходе него рекомендуется перепроверить политику подбора кадров в фирму, в частности выяснить, имеются ли в компании лица, трудоустроенные на определенные должности, не имея при этом соответствующего профессионального образования или стажа работы, которые являются обязательными требованиями для них, а также другую информацию, зависящую от конкретной обстановки. 2) определятся лица, в чью компетенцию входит обеспечение информационной безопасности в организации исходя как из документальных составляющих, так и из реальных поручений, которые перед ними были поставлены руководством; 3) обозначатся должности, которые занимали сотрудники фирмы на прежних местах работы249; 4) с определенной долей вероятности выяснится возможность совершения деяния группой лиц (т.е. в том случае, если какой-либо сотрудник организации был принят на должность IT-специалиста по протекции администрации, несмотря на его низкую квалификацию, явно не соответствующую требованиям, предъявляемым к данной категории работников); 5) обнаружится иная информация, с помощью которой сотрудники ОРО смогут сделать промежуточный вывод о возможности совершения преступления и выявить лиц, к нему причастных.

В свою очередь криминалистический риск у сотрудников оперативно-розыскных органов при таком ОРМ, как наведение справок, также выражается в двух моментах, обозначенных нами ранее, которые мы считаем целесообразным напомнить: 1) совершение ошибки, обусловленной получением документов, не соответствующих действительности, повлекшим за собой непроведение сопоставления между информацией, содержащейся в истребованных справках, и объективными данными изучаемого субъекта; 2) совершение ошибки, обусловленной получением отказа в предоставлении запрашиваемой информации, повлекшим за собой прекращение дальнейших попыток по ее истребованию. Для минимизации негативных последствий данного вида криминалистического риска (включая первый и второй моменты), как и в случае

В особенности служащих оперативно-розыскных органов должны заинтересовать случаи, когда отдельные работники фирмы прежде были IT-специалистами (системными администраторами и операторами, программистами, наладчиками сетевого оборудования и т.д.), а у данного работодателя выполняют совсем иные функции (являются инженерами, логистами, бухгалтерами и т.д.). со следователем при использовании результатов ОРД, а также при возбуждении уголовного дела, считаем обоснованным использование сотрудниками оперативно-розыскных органов общеизвестных рекомендаций, состоящих в личном посещении физических и юридических лиц, которым были направлены запросы, обращении в официальные архивы, где могут дублироваться искомые сведения, и информирования субъекта, производящего расследование обо всех случаях игнорирования их требований. Специалист

Для снижения криминалистического риска в деятельности еще одного участника уголовного судопроизводства, указанного в статье 58 УПК РФ, предлагаем придерживаться следующих рекомендаций.

Во-первых, целесообразно создать в каждом субъекте РФ «базы специалистов», которые можно формировать в том числе из штатных IT-специалистов организаций. Как показали проведенные нами опросы250, 46 % IT-работников компаний согласны в свое рабочее время выступать в уголовном процессе в качестве специалистов, 48 % руководящего персонала также не возражают против участия их штатных системных администраторов, операторов, программистов и иных лиц, связанных с информационными технологиями, в данном виде судопроизводства251.

Применительно к нашему случаю, представляется желательным, чтобы лицо, привлекаемое к расследованию неправомерного доступа к компьютерной информации в роли специалиста, отвечало следующим критериям:

1) среднее профессиональное или высшее образование, полученное в учебных заведениях с государственной аккредитацией по таким направлениям, как «Компьютерная безопасность» (090301), «Информационная безопасность автоматизированных систем» (090303), «Компьютерные сети» (230111),

Участники опросов делились на 2 состава: руководящий персонал (единоличные исполнительные органы компаний, члены совета директоров, акционеры (участники) фирм) и IT-специалисты организаций (системные администраторы (операторы), программисты и т.д.). Общее количество респондентов – 50 человек в каждой из представленных групп. В качестве субъектов в которых происходил данный опрос, выступили город федерального значения – Москва, Липецкая область, Московская область, Нижегородская область, Новосибирская область, Республика Мордовия и т.д. 251 Более подробно результаты опросов продемонстрированы в Приложениях 3 и 4. 138 «Автоматизированные системы обработки информации и управления (по отраслям)» (230103); 2) имеющийся стаж по специальности (специализации) не менее 5 лет252; 3) наличие сертификатов «Cisco», «Microsoft» и других, полученных в центрах обучения и тестирования; участие в международных, российских или региональных практических конференциях, касающихся отдельных аспектов развития современных информационных технологий; прохождение специализированных курсов (в том числе участие в виртуальных семинарах253) и т.д.

Во-вторых, следует расширить практику привлечения к участию в следственных действиях специалистов, обладающих комплексными знаниями в области, как аппаратного, так и программного обеспечения. Так, например, при осмотре места происшествия, видится правильным, чтобы лицо привлекаемое в порядке статьи 58 УПК РФ, было сведущим не только в сфере использования различных видов операционных систем, и иных программных продуктов, что позволит ему фиксировать и изымать определенные компьютерные данные, но и имело опыт работы с аппаратной средой технических устройств, в общем, и со специализированным оборудованием защиты информации, в частности254.