DOI: 10.17803/1994-1471.2024.158.1.166-178

Е. Ю. Герасимова*

Следственные ситуации, возникающие на первоначальном и последующем этапах расследования создания, распространения и использования вредоносных компьютерных программ

Аннотация. Статья посвящена анализу следственных ситуаций, которые могут возникнуть на разных этапах расследования преступления, предусмотренного статьей 273 УК РФ, — создания, распространения и использования вредоносных компьютерных программ. На основании приведенных данных, мнений ученых и научной литературы была выявлена необходимость более точечного изучения обстоятельств, при которых рассматривается та или иная следственная ситуация на первоначальном и последующем этапах расследования, поскольку комбинаций обстоятельств огромное множество. В связи с этим мы предлагаем выделить отдельные виды обстоятельств следственных ситуаций, возникающих на первоначальном и последующем этапах расследования, описать возможные варианты их форм и затем, исходя из возникающих перед следователем и правоохранительными органами в связи с ними задач, описать рекомендуемые действия, которые могли бы позволить решить задачи в ходе предварительного следствия и достигнуть принятия правового решения в рамках предварительного расследования.

Ключевые слова: следователь; следственные действия; следственные ситуации; первоначальный этап расследования; последующий этап расследование; криминалистика; вредоносные компьютерные программы; преступления; ситуалогия; планирование.

Для цитирования: *Герасимова Е. Ю.* Следственные ситуации, возникающие на первоначальном и последующем этапах расследования создания, распространения и использования вредоносных компьютерных программ // Актуальные проблемы российского права. — 2024. — Т. 19. — № 1. — С. 166–178. — DOI: 10.17803/1994-1471.2024.158.1.166-178.

* *Герасимова Елена Юрьевна*, заместитель начальника курса факультета подготовки сотрудников полиции для подразделений по охране общественного порядка Московского университета МВД России имени В.Я. Кикотя
ул. Академика Волгина, д. 12, г. Москва, Россия, 117997
gerasimova.eu@bk.ru

Investigative Situations Arising at the Initial and Subsequent Stages of Investigating the Creation, Distribution and Use of Malicious Software

Elena Yu. Gerasimova, Deputy Head of Year Director, Faculty of Police Officers Training for Public Order Units, Kikot Moscow University of the Ministry of the Interior of Russia
12, Akademika Volgina St., Moscow 117997, Russian Federation
gerasimova.eu@bk.ru

Abstract. The paper is devoted to the analysis of investigative situations that may arise at different stages of the investigation of a crime under Article 273 of the Criminal Code of the Russian Federation: creation, distribution and use of malicious software. Based on the data presented, the opinions of scientists and scientific literature, the need for a more precise study of the circumstances under which this or that investigative situation is considered at the initial and subsequent stages of the investigation was identified, since there are a huge number of combinations of circumstances. In this regard, we propose to highlight certain types of circumstances of investigative situations that arise at the initial and subsequent stages of the investigation, describe possible options for their forms and then, based on the tasks that arise for the investigator and law enforcement agencies in connection with them, describe recommended actions that could allow you to solve problems during the preliminary investigation and achieve a legal decision within the framework of the preliminary investigation.
Keywords: investigator; investigative actions; investigative situations; initial stage of investigation; subsequent stage of investigation; criminology; malicious computer programs; crimes; situationology; planning.
Cite as: Gerasimova EYu. Investigative Situations Arising at the Initial and Subsequent Stages of Investigating the Creation, Distribution and Use of Malicious Software. *Aktual'nye problemy rossijskogo prava*. 2024;19(1):166-178. (In Russ.). DOI: 10.17803/1994-1471.2024.158.1.166-178.

Рекомендации, разрабатываемые в процессе формирования частной методики расследования отдельного вида преступления, могут быть применимы только при определенных условиях. Данный тезис имеет прямую аналогию с классической конструкцией правовой нормы, имеющей диспозицию, применимую в случае наступления условий, предусмотренных гипотезой. Отличие заключается только в юридической силе предписываемой модели поведения. Принятие следователем решения о выборе направления всего расследования в целом или о выборе того или иного приема для достижения положительного результата при производстве отдельного следственного действия, безусловно, зависит прежде всего от того, какие обстоятельства сложились к определенному моменту расследования, что́ стало известно ему о тех или иных обстоятельствах, имеющих значение для принятия решения. Такой неоспоримый и элементарный тезис лежит в основе криминалистического учения, называемого ситуалогией[1].

И прежде чем представить результаты наших изысканий о следственных ситуациях, возникающих на первоначальном и последующем этапе расследования создания, распространения и использования вредоносных компьютерных программ, мы бы хотели вкратце обозначить свою позицию по ряду важных для нас положений, имеющих дискуссионный характер в научных кругах.

В первую очередь мы бы хотели определить границы первоначального и последующего этапа. В своей работе мы не рассматриваем закономерности деятельности следователя или иного лица, участвующего в расследовании создания, распространения и использования вредоносных компьютерных программ, на заключительном этапе по вполне понятным причинам. Процессуальные действия, выполняемые в этот период, не имеют особенностей,

[1] *Волчецкая Т. С.* Криминалистическая ситуалогия : монография / под ред. проф. Н. П. Яблокова. Москва ; Калининград, 1997. С. 134.

существенно связанных с характером расследуемого преступления. Сбор дополнительного характеризующего материала, объявление об окончании производства следственных действий, комплекс мероприятий в порядке ст. 217 УПК РФ и другие действия следователя, традиционно включаемые в заключительный этап, при расследовании преступлений рассматриваемого нами вида не будут существенно отличаться по своему порядку от выполняемых на таком же этапе при расследовании какого-либо коррупционного, корыстного, насильственного или другого преступления. Наиболее ярким отличием в частных методиках расследования преступлений отдельных видов всегда является перечень обязательных следственных действий и видов экспертиз, проводимых в целях доказывания объективной стороны состава преступления, или, как это выражено в законе, события преступления (время, место способ и другие обстоятельства). Всё это принято включать в первоначальный и последующий этапы.

Первоначальный этап расследования начинается с момента возбуждения уголовного дела. Наличие достаточных данных, указывающих на признаки преступления, с которым необходимо связывать данное событие, совсем не исключает существенного дефицита значимых для расследования сведений о нем. Возбуждение уголовного дела как юридический факт, хотя и меняет состояние сложившейся ситуации, формируя новый статус участников отношений, сам по себе не может повлиять на состояние информированности следователя об обстоятельствах расследуемого преступления. Рассматриваемый нами первоначальный этап расследования и следственные ситуации в этот период традиционно характеризуются неочевидностью и неопределенностью во множестве вопросов. Как и на стадии возбуждения уголовного дела, следователю всё еще приходится принимать множество решений на основании наиболее вероятных предположений, в том числе сделанных на базе знаний об особенностях элементов криминалистической характеристики и взаимосвязях ее элементов. Об этой характерной особенности первоначального этапа расследования преступлений, связанных с компьютерной информацией, часто упоминают ученые в своих публикациях, к примеру О. С. Бутенко и А. Н. Голодный[2], В. В. Поляков[3].

Мы считаем целесообразным связывать отправную точку первоначального этапа расследования с возбуждением уголовного дела. Но если с началом первоначального этапа расследования всё более-менее понятно, хотя и не совсем однозначно, то с моментом его окончания и перехода на последующий этап мнения ученых существенно разделяются. М. В. Кардашевская в своих публикациях, проведя анализ вариантов периодизации расследования, предлагаемых разными авторами, приходит к вполне обоснованному, по нашему мнению, решению характеризовать первоначальный, последующий и завершающий этапы расследования по приоритетным задачам, стоящим перед следователем в эти периоды. Данные задачи ставит УПК России. После того, как первоначальная задача уже решена и данных собрано достаточно для принятия решения о наличии всех необходимых признаков преступления, главным становится вопрос о наличии оснований для предъявления виновному обвинения в его совершении. Решение этого вопроса следует связать с первоначальным этапом расследования; следовательно, окончание этого этапа необходимо сопрягать с моментом окончания процедуры привлечения в качестве обвиняемого или выполнения всех необходимых действий для обеспечения этой процедуры, если место нахождения лица, подлежащего привлечению, еще не установлено. С этого момента первоначальный этап перехо-

[2] *Бутенко О. С., Голодный А. Н.* Некоторые следственные ситуации при расследовании преступлений, совершаемых с использованием компьютерной техники // Массовые коммуникации на современном этапе развития мировой цивилизации : материалы Всероссийской научной конференции с международным участием, Гуманитарно-социальный институт. Ростов н/Д, 2015. С. 272–276.

[3] *Поляков В. В.* Следственные ситуации по делам о неправомочном удаленном доступе к компьютерной информации // Доклады ТУСУРа. 2010. № 1 (21), ч. 1, июнь. С. 46–50.

дит в последующий, приоритетной задачей на котором будет, в свою очередь, получение достоверных сведений, достаточных для принятия решения об окончании предварительного следствия[4]. По данному принципу мы бы и хотели представить отдельные периоды расследования для описания складывающихся в эти промежутки следственные ситуации для выделения некоторых возникающих перед следствием задач и рекомендуемых алгоритмов их решения.

Как справедливо указывает Е. Р. Россинская, «следственная ситуация в общем виде — это условия (обстановка), в которых находится процесс расследования по уголовному делу на данный определенный момент времени»[5]. Р. С. Белкин также лаконично определил эту категорию подобным образом: «совокупность условий, в которых осуществляется расследование в конкретный момент времени»[6]. Все обстоятельства, в которых происходит процесс расследования, могут иметь значение для получения результата, однако очевидно, что следователь или иное лицо, участвующее в расследовании, может учитывать их при планировании, только если ему стало о них известно. Именно поэтому при рассмотрении следственных ситуаций часто принято включать в них только обстоятельства, отвечающие такому условию. «Особенность следственной ситуации обусловлена тем, что она сама является результатом познавательной деятельности по расследованию преступлений»[7]. Думается, именно поэтому в приведенном выше определении, предлагаемом Е. Р. Россинской, сделана оговорка «в общем виде». Далее в своих рассуждениях мы будем придерживаться мнения, согласно которому, чтобы ситуационный подход к выбору разрабатываемых рекомендаций имел положительный эффект, следователь должен иметь возможность примерить рекомендуемую модель к условиям, с которыми он столкнулся в своей практической деятельности, то есть к тому, что он знает о ситуации, сложившейся в объективной действительности. Так, и профессор В. К. Гавло предлагает характеризовать подобным образом следственную ситуацию с точки зрения информационной осведомленности следователя о расследуемом событии преступления и его отдельных обстоятельствах в так называемом узком смысле. Обращаясь к мнению немецких криминалистов, мы можем увидеть, что они определяют следственную ситуацию, как «совокупность обстоятельств, условий и развития событий, которые обуславливают действия полиции и влияют на них»[8]. Очевидно, что действия полиции не могут быть детерминированы обстоятельствами, о которых полиции ничего не известно.

Несмотря на отсутствие сведений о многих значимых для расследования обстоятельствах после принятия решения о возбуждении уголовного дела, у следователя, как правило, имеется достаточно данных о том, чтобы оценить следственную ситуацию и определить, к какому типичному виду она относится. Одной из задач криминалистической методики как раздела криминалистической науки является выделение и описание типичных следственных ситуаций («объективно повторяемых положений»[9]), складывающихся при расследовании отдельных видов преступлений, и разработка рекомендуемой для них программы действий следователя.

К настоящему времени в научно-криминалистических источниках уже наработан значитель-

---

4 *Кардашевская М. В., Шипилова Е. С.* Этапы процесса расследования и их характеристика // Таврический научный обозреватель. 2015. № 2 (октябрь). С. 8.

5 *Россинская Е. Р.* Криминалистика : учебник М. : Норма : Инфра-М, 2012. С. 140.

6 *Белкин Р. С.* Курс криминалистики : в 3 т. М. : Бристъ, 1997. Т. 3 : Криминалистические средства, приемы и рекомендации. С. 133.

7 Судебно-следственные ситуации: психолого-криминалистические аспекты : монография / В. К. Гавло, В. Е. Клочко, Д. В. Ким ; под ред. проф. В. К. Гавло. Барнаул : Изд-во Алт. ун-та, 2006. С. 68.

8 Криминалистический словарь. 2-е изд., перераб. / под ред. В. Бугхарда [и др.]. М., 1993. С. 43.

9 *Корноухов В. Е.* Основные положения методики расследования отдельных видов преступлений. Красноярск : Красноярский гос. ун-т, 1972. С. 93.

ный объем рекомендаций подобного характера, относящихся к расследованию компьютерных преступлений. Узкоориентированных рекомендаций для поведения следователя в следственных ситуациях при расследовании создания, распространения и использования вредоносных компьютерных программ нам встретить не удалось, однако в более широком плане, например для компьютерных преступлений или преступлений в сфере IT-технологий, мы нашли немалое количество теоретического материала, который может представлять интерес в контексте нашего исследования. Первое, на что можно обратить внимание при изучении научных изысканий, — это традиционное для науки криминалистики отсутствие единого общепринятого мнения авторов на главное основание для классификации следственных ситуаций.

Профессор С. Г. Еремин выделяет три типичные следственные ситуации, возникающие при расследовании компьютерных преступлений:

1) нарушение целостности и конфиденциальности в информационной системе и данные о виновном лице выявлены силами ее собственника, который обратился с заявлением;

2) нарушение выявлено собственником информационной системы, но сведения о нарушителе отсутствуют;

3) факт нарушения и данные о нарушителе стали «общеизвестными или непосредственно обнаружены органом дознания», в том числе в ходе осуществления оперативно-розыскной деятельности, связанной с другим делом[10].

О. С. Бутенко и А. Н. Голодный в своей публикации о следственных ситуациях при расследовании преступлений, совершаемых с использованием компьютерной техники, также подобным образом рассмотрели три вида следственных ситуаций. Первая из них характеризуется тем, что нарушение целостности или конфиденциальности информации в информационной системе было выявлено ее собственником, им же было установлено виновное лицо и сообщено в правоохранительные органы.

С. Г. Еремин предлагает рассмотреть такое обстоятельство для дополнительной классификации следственных ситуаций, возникающих при расследовании компьютерных преступлений, как мотив совершения компьютерных преступлений. Так, из мотивов совершения преступлений рассматриваемой нами категории можно выделить следующие: 1) хулиганские действия; 2) корыстная цель или иная личная заинтересованность посторонних лиц, не имеющих отношения к лицу или организации, подвергшейся противоправному посягательству; 3) корыстная цель работников самой организации, компьютерная информация которой была несанкционированно уничтожена, модифицирована, скопирована или заблокирована.

Такое обстоятельство, как характер лица, чья информация подверглась противоправному посягательству, также может выступать основанием для классификации следственных ситуаций, складывающихся на первоначальном и последующем этапах расследования создания, распространения и использования вредоносных компьютерных программ. От этого во многом зависит перечень обязательных процессуальных действий и тактика проведения отдельных следственных действий. Например, в случае противодействия расследованию со стороны лица, подвергшегося воздействию вредоносной программы, если это лицо является коммерческой организацией, для производства обыска по месту его нахождения, скорее всего, не потребуется разрешение суда.

Особого внимания, на наш взгляд, заслуживает мнение О. Ю. Антонова и А. Г. Себякина, предложивших рассматривать следственные ситуации в контексте применения знаний в области компьютерной техники при расследовании преступлений. Предложенная ими система видов типичных следственных ситуаций построена в зависимости от наличия и характера информации об электронно-цифровом носителе криминалистически значимой информации. Первый предлагаемый авторами вид

[10] *Еремин С. Г.* Возбуждение уголовного дела о преступлениях в сфере дистанционно-банковского обслуживания, следственные ситуации, версии, планирование и расследование на первоначальном этапе // Вестник Волгоградской академии МВД России. 2019. № 2 (49). С. 79.

следственной ситуации характеризуется наличием сведений о месте, в котором преступником выполнялись действия по совершению преступления. В ситуации второго вида имеющаяся информация указывает на лицо, причастное к его совершению, пользовавшееся при этом электронными устройствами компьютерного или информационно-телекоммуникационного характера. В третьем случае следователю известно о существовании электронно-цифровых следов в компьютерных устройствах лиц, подвергшихся преступному посягательству. И четвертый вид следственных ситуаций отличается осведомленностью следователя о наличии электронно-цифровых следов в компьютерных устройствах преступника[11]. Нетрудно заметить, что указанные отличительные признаки предлагаемых видов следственных ситуаций не являются взаимоисключающими, что не соответствует правилам построения классификационных систем, о которых достаточно подробно говорит А. Ю. Головин в трудах, посвященных криминалистической систематике[12].

Р. А. Дерюгин и М. А. Шергин в результате изучения деятельности по расследованию преступлений, совершаемых с использованием информационных технологий и в сфере компьютерной информации, приходят к выводу о том, что типичными будут такие следственные ситуации: 1) бесконфликтная следственная ситуация (самая простая, по мнению авторов), когда расследуемое преступление очевидно, его характер и обстоятельства установлены, пострадавший самостоятельно выявил факт воздействия на информационную систему, вредоносное программное обеспечение и способ его использование преступником; 2) о совершенном преступлении правоохранительным органам стало известно, однако «механизм полностью не установлен, преступник не задержан, но есть сведения, указывающие на причастность определенных лиц»; 3) о преступлении известны только последствия его совершения. Отсутствие сведений о способе совершения и о личности преступника делают такую ситуацию достаточно сложной.

Приводя подобную классификацию, авторы обращают внимание на то, что ими перечислены не все вероятные варианты типичных следственных ситуаций первоначального этапа расследования. Кроме того, как видно из текста публикации, их исследование ориентировано прежде всего на мошенничество в сфере компьютерной информации[13], то есть предмет только частично совпадает с предметом нашего исследования. Но с учетом того, что мошенники часто используют вредоносные программы при совершении такой формы хищения, результаты научных изысканий этих авторов во многом являются справедливыми для нас.

В своем анализе результатов научных исследований, проводимых в целях классификации следственных ситуаций, складывающихся при расследовании компьютерных преступлений, мы исходили прежде всего из того, что выводы авторов о характере предлагаемых ими видов следственных ситуаций можно отнести к расследованию преступлений интересующей нас категории. При этом большинство описанных выше признаков следственных ситуаций могут вполне сочетаться с другими, то есть часто авторы в одной классификации нарушают требования к формированию такого рода систем. Таким образом, выделяя группы следственных ситуаций, они не обособляют эту группу, а описывают некоторый значимый для планирования работы следователя признак. Следственная же ситуация является достаточно сложной много-

[11] *Антонов О. Ю., Себякин А. Г.* Тактические комплексы применения знаний в области компьютерной техники при расследовании преступлений // Юридическая наука и правоохранительная практика. 2020. № 3 (53). С. 95.

[12] *Головин А. Ю.* Теоретические основы и актуальные проблемы криминалистической систематики на современном этапе развития криминалистики : дис. … д-ра юрид. наук : 12.00.12. М., 2003.

[13] *Дерюгин Р. А., Шергин М. А.* О некоторых особенностях расследования преступлений, совершаемых с использованием IT-технологий и в сфере компьютерной информации // Вестник Уральского юридического института МВД России. 2021. № 3. С. 101–102.

аспектной системой, даже если ее как систему (совокупность) обстоятельств сократить, поставив такое условие, как осведомленность о них следователя. И по одному признаку их классифицировать, думается, нецелесообразно, особенно если мы имеем в виду такое многообразное по механизму преступление, как создание, распространение и использование вредоносных компьютерных программ. В своей работе мы решили не столько классифицировать следственные ситуации по отдельному признаку, сколько выделить эти признаки и определить алгоритм действий следователя при наличии признака в конкретной следственной ситуации. Классификация следственных ситуаций в нашем случае может быть определена по приоритетной задаче или по этапу расследования, на котором она сформировалась.

Выбранное нами основание для периодизации процесса расследования имеет обратный эффект для рассуждений о видах следственных ситуаций, возникающих на том или ином этапе. Так, если исходить из приоритетной задачи отдельного этапа, то, когда она заключается в получении достаточных данных для привлечения лица к уголовной ответственности, некоторые особенности следственной ситуации будут иметь не столь существенное значение, как на последующем. При этом приоритетная задача не позволяет пересекаться видам следственных ситуаций на том или ином этапе, даже при совпадении характера некоторых из составляющих их обстоятельств.

Исходя из этих рассуждений, мы приходим к выводу о том, что наиболее целесообразным будет вести речь о классификации не следственных ситуаций, а обстоятельств, которые могут в них присутствовать. Число вариантов этих обстоятельств в формируемой классификации следственных ситуаций будет увеличиваться в геометрической прогрессии по мере увеличения учитываемых обстоятельств. Именно поэтому, думается, во многих, в том числе в приведенных выше, классификациях авторами сделана оговорка о том, что возможны различные сочетания тех или иных названных ими обстоятельств. Для этого мы должны выделить отдельные виды обстоятельств следственной ситуации, описать возможные варианты их форм и затем, исходя из возникающих перед следователем в связи с ними задач, описать рекомендуемые действия, которые могли бы позволить решить эти задачи. Такой подход позволяет нам представить следующие результаты.

1. Обстоятельство: имеются сведения о конкретной вредоносной программе или иной вредоносной компьютерной информации.

1.1. Цели и задачи:

1.1.1. Получить экземпляр попавшей в поле зрения следствия вредоносной программы (компьютерной информации).

1.1.2. Проверить (подтвердить) факт использования или распространения имеющейся компьютерной информации.

1.1.3. Определить, какое воздействие (какие воздействия) оказала программа на компьютерную информацию (программное обеспечение): уничтожение, блокирование, копирование, модификация, нейтрализация средств защиты.

1.1.4. Определить, какие воздействия (уничтожение, блокирование, копирование, модификация, нейтрализация средств защиты) фактически возможно осуществить при использовании программы.

1.2. Рекомендуемые действия:

1.2.1. Изъятие экземпляра вредоносной программы (компьютерной информации) одним из предусмотренных законом способов в зависимости от конкретных обстоятельств (выемка, осмотр, ОРМ и др.).

1.2.2. Консультация с экспертом (специалистом).

1.2.3. Компьютерная экспертиза.

1.2.4. Поручение проведения ОРМ.

2. Обстоятельство: имеются сведения о нарушении целостности и конфиденциальности в информационной системе или об иных проявлениях, возникших в результате противоправного посягательства с использованием вредоносной компьютерной информации.

2.1. Задачи:

2.1.1. Установить причинно-следственную связь между выявленными последствиями и использованием вредоносной компьютерной информации.

2.1.2. Определить размер ущерба (характер вреда), причиненного использованием вредоносной компьютерной информации.

2.2. Рекомендуемые действия:

2.2.1. Консультация со специалистом.

2.2.2. Компьютерная экспертиза.

2.2.3. Технико-криминалистическая экспертиза компьютерного оборудования.

2.2.4. Допрос заявителя или собственника информационной системы, подвергшейся вредоносному воздействию.

2.2.5. Допросы в качестве свидетелей лиц, занимавшихся разработкой компьютерного программного обеспечения, подвергшегося воздействию вредоносной программы.

2.2.6. Допрос осуществлявших сопровождение (установка, настройка, обслуживание, обновление и пр.) подвергшегося воздействию программного обеспечения.

3. Обстоятельство: имеются признаки корыстного мотива в выявленном противоправном посягательстве на информационную систему с использованием вредоносной компьютерной информации.

3.1. Задачи:

3.1.1. Установить причинно-следственную связь между выявленными последствиями и использованием вредоносной компьютерной информации.

3.1.2. Определить размер ущерба (характер вреда), причиненного использованием вредоносной компьютерной информации.

3.1.3. Осуществить поиск «денежного следа».

3.1.4. Проверить версию системы преступной деятельности (системы участников, системы неоднократного совершения эпизодов преступной деятельности).

3.2. Рекомендуемые действия:

3.2.1. Компьютерная экспертиза.

3.2.2. Экономическая экспертиза.

3.2.3. Допрос лиц, связанных с обеспечением работы информационной компьютерной системы.

4. Обстоятельство: использование вредоносной компьютерной информации было совершено из мотивов личной заинтересованности некорыстного характера.

4.1. Задачи:

4.1.1. Установление преимуществ, которые возможно получить при использовании или распространении вредоносной программы или компьютерной информации.

4.1.2. Определение фактического результата, полученного в ходе использования вредоносной программы или компьютерной информации.

4.2. Рекомендуемые действия:

4.2.1. Консультация со специалистом (экспертом) в области информационных технологий.

4.2.2. Компьютерная экспертиза.

4.2.3. Допрос работника организации, чья профессиональная деятельность относится к информации, подвергшейся преступному посягательству.

5. Обстоятельство: лица, на которых падает подозрение в совершении использования вредоносной компьютерной информации, сопряженного с противоправным посягательством на информационную систему организации, являются ее действующими или бывшими сотрудниками либо иным образом связаны с ней.

5.1. Задачи:

5.1.1. Определить круг лиц, имевших реальную физическую возможность совершить преступные действия (физический доступ, отсутствие алиби и др.).

5.1.2. Определить круг компетенций, необходимых для выполнения преступных действий.

5.1.3. Определить круг лиц, имеющих компетенции, необходимые для выполнения действий.

5.1.4. Проверить версии о преследовании мотивов мести, корысти, получения преимуществ по службе, ревности, иной личной заинтересованности и др.

5.1.5. Установить конкретных лиц.

5.2. Рекомендуемые действия:

5.2.1. Консультации с экспертом, специалистом.

5.2.2. Осмотр со специалистом компьютерного оборудования и программного обеспечения.

5.2.3. Допросы лиц, которые могут обладать соответствующими сведениями.

5.2.4. Поручение проведения ОРМ.

6. Обстоятельство: лица, заподозренные в противоправном посягательстве на информационную систему, не имеют отношения к организации, которой она принадлежит.

6.1. Задачи:

6.1.1. Проверка версии о преследовании мотива мести бывших работников организации.

6.1.2. Проверка версии о соучастии действующих сотрудников («инсайдеров»).

6.2. Рекомендуемые действия:

6.2.1. Консультация со специалистом (экспертом) в области информационных технологий с целью определения компетенций, необходимых для совершения преступления.

6.2.2. Допрос руководителя и сотрудника организации, в чьи обязанности входит организация учета кадров.

6.2.3. Изъятие и осмотр личных дел или иных баз данных в зависимости от организации учета уволенных сотрудников.

7. Обстоятельство: противоправное посягательство на компьютерную информацию было совершено из хулиганских побуждений.

7.1. Задачи:

7.1.1. Проверка версии о дополнительных нехулиганских преступных мотивах совершения, которые могут преследоваться наряду с хулиганскими.

7.1.2. Проверка версии о сокрытии истинных мотивов, включая экстремистские, под маскировкой их под хулиганские.

7.1.3. Получение сведений о возможных результатах использования вредоносной программы.

7.1.4. Определение круга лиц, получивших пользу от использования вредоносной программы.

7.2. Рекомендуемые действия:

7.2.1. Консультация со специалистом (экспертом) в области информационных технологий.

7.2.2. Поручение провести ОРМ по проверке преступных связей лица, принадлежности его к неформальным объединениям.

8. Обстоятельство: факт использования вредоносной компьютерной информации был выявлен собственником или пользователем информационной системы самостоятельно.

8.1. Задачи:

8.1.1. Установить круг лиц, обладающих полезными сведениями (свидетелей), и получить от них необходимые сведения в зависимости от выясненных обстоятельств.

8.1.2. Установить принципы работы компьютерной информационной системы, подвергшейся противоправному посягательству, и способ воздействия (проникновения) вредоносной информации.

8.1.3. Обнаружить и зафиксировать электронные следы противоправного посягательства на информационную систему.

8.1.4. Определить характер и размер вреда, который мог быть причинен действием вредоносной информации.

8.1.5. Определить вред, фактически причиненный в результате воздействия вредоносной информации.

8.2. Рекомендуемые действия:

8.2.1. Консультация со специалистом в области информационных технологий.

8.2.2. Осмотр компьютерной техники и программного обеспечения.

8.2.3. Компьютерная экспертиза.

8.2.4. Допрос лица, выявившего факт использования вредоносной программы.

8.2.5. Допрос лица или лиц, чья профессиональная деятельность связана с функционированием системы, подвергшейся преступному посягательству.

9. Обстоятельство: факт использования вредоносной компьютерной информации был выявлен в результате осуществления оперативно-розыскной деятельности.

9.1. Задачи:

9.1.1. Сведениям, полученным в ходе осуществления оперативно-розыскной деятельности, необходимо придать статус доказательств, соответствующий требованиям УПК РФ.

9.1.2. Проверить наличие у органа дознания иных интересующих следствие материалов ОРМ, кроме тех, что уже были предоставлены.

9.1.3. В порядке взаимодействия с органами дознания совместно обсудить направления дальнейшего оперативного сопровождения расследования.

9.2. Рекомендуемые действия:

9.2.1. Получение доступа к работе с документами, представляющими тайну, и изучение еще не легализованных результатов оперативно-розыскной деятельности.

9.2.2. Поручение органу дознания на предоставление результатов ОРМ.

9.2.3. Комплекс мероприятий, указанный в п. 8.2.

10. Обстоятельство: эпизод использования вредоносной компьютерной информации был выявлен в результате расследования другого аналогичного факта.

10.1. Задачи:

10.1.1. Собрать материалы (доказательства), достаточные для увеличения объема обвинения.

10.2. Рекомендуемые действия:

10.2.1. Если эпизод аналогичный, то комплекс мероприятий повторяет предусмотренный для уже расследуемого.

11. Обстоятельство: для противоправного посягательства на информационную систему использовалось коммуникационное устройство (смартфон, планшет-коммуникатор, мобильный телефон и т.п.).

11.1. Задачи:

11.1.1. Задачи, возникающие при наличии такого обстоятельства, в общем не будут иметь существенных отличий от задач, возникающих в иных рассматриваемых разделах.

11.2. Рекомендуемые действия:

11.2.1. Мероприятия, рекомендуемые при возникновении такого обстоятельства в следственной ситуации, необходимо определить в зависимости от иных рассматриваемых в настоящем разделе обстоятельств следственных ситуаций.

12. Обстоятельство: установлено настоящее место нахождения лица, подпадающего под подозрение, или следователь обладает реальной возможностью вызвать его для проведения следственных действий с его участием.

12.1. Задачи:

12.1.1. Привлечение к уголовной ответственности и изобличение установленного лица в полной мере.

12.1.2. Установление контактов установленного лица, круга знакомых, друзей, лиц, с которыми он имел общение в период совершения преступления и предшествующий этому.

12.2. Рекомендуемые действия:

12.2.1. Проведение допроса подозреваемого и комплекса связанных с этим процессуальных действий (избрание меры пресечения или процессуального принуждения, сбор характеризующего материала и т.д.).

12.2.2. Проведение личного обыска.

12.2.3. Проведение обыска по месту жительства.

12.2.4. Проведение обыска по месту работы.

12.2.5. Поручение на проведение ОРМ с целью установления возможных мест нахождения компьютерного оборудования, которое установленное лицо могло использовать в процессе осуществления преступной деятельности.

12.2.6. Поручение проведения ОРМ для выявления дополнительных эпизодов расследуемого преступления, иной преступной деятельности, установления соучастников, получения дополнительных улик.

13. Обстоятельство: место нахождения лица, совершившего создание, распространение и использование вредоносных компьютерных программ, не установлено, следствие не обладает возможностью с ним связаться.

13.1. Задачи:

13.1.1. Розыск и задержание преступника.

13.2. Рекомендуемые действия:

13.2.1. Процессуальные меры и организация разыскной работы, направленной на установление места нахождения преступников, при неочевидности такого характера широко освещена в методиках расследования преступлений, совершенных в условиях неочевидности.

14. Обстоятельство: установлено конкретное лицо или группа соучастников, совершивших создание, распространение и использование вредоносных компьютерных программ.

14.1. Задачи:

14.1.1. Определение характера участия в преступлении и степени вины совершивших преступные действия.

14.1.2. Установление места нахождения всех участников преступления.

14.1.3. Привлечение к уголовной ответственности виновных.

14.2. Рекомендуемые действия:

14.2.1. Разработка, организация и проведение оперативно-тактической операции по задержанию (доставлению) к следователю участников группы с проведением комплекса мероприятий, указанных в п. 13.2.

14.2.2. При взаимодействии с органом дознания определить наиболее целесообразный алгоритм совместных действий по документированию преступной деятельности, установлению контактов между участниками группы.

15. Обстоятельство: установлен круг лиц, среди которых может (могут) быть совершивший (совершившие) создание, распространение и использование вредоносных компьютерных программ.

15.1. Задачи:

15.1.1. Выявление среди круга установленных лиц совершившего преступление.

15.1.2. Установление контактов установленного лица, круга знакомых, друзей, лиц, с которыми он имел общение в период совершения преступления и предшествующий этому.

15.2. Рекомендуемые действия:

15.2.1. Поручение на проведение ОРМ с целью проверки на предмет причастности лиц, входящих в круг установленных.

15.2.2. Проведение допросов.

15.2.3. Осмотр со специалистом рабочих мест установленных лиц.

15.2.4. Поручение на проведение ОРМ с целью установления возможных мест нахождения компьютерного оборудования, которое установленное лицо могло использовать в процессе осуществления преступной деятельности.

16. Обстоятельство: круг лиц, которые могли совершить создание, распространение и использование вредоносных компьютерных программ, неопределенно широк.

16.1. Задачи:

16.1.1. Установление круга лиц или лица, причастных к совершению преступления.

16.2. Рекомендуемые действия:

16.2.1. Круг рекомендуемых мероприятий имеет также неограниченные пределы и их перечень и последовательность зависят от имеющейся информации о механизме преступления, включая те, что указаны нами в настоящей системе рекомендаций.

17. Обстоятельство: место, откуда осуществлялось противоправное посягательство на компьютерную информацию с использованием вредоносной компьютерной программы, установлено.

17.1. Задачи:

17.1.1. Обнаружение, фиксация и изъятие в установленном месте следов и улик.

17.1.2. Определение круга лиц, имевших доступ к установленному месту в период совершения преступления.

17.1.3. Определение конкретного лица или группы лиц, которые находились в установленном месте при совершении преступления.

17.1.4. Установление лиц, совершивших преступление.

17.2. Рекомендуемые действия:

17.2.1. Проведение следственного действия для обнаружения и изъятия следов и улик, находящихся в установленном месте.

17.2.2. Производство экспертиз изъятого (компьютерная, техническая экспертиза компьютерной техники, дактилоскопическая, геномная и др.) в зависимости от характера обнаруженных и изъятых следов.

17.2.3. Допрос собственников помещения лиц, имевших доступ к установленному месту.

18. Обстоятельство: не установлено место, где находилось подпадающее под подозрение лицо и откуда оно осуществляло противоправное посягательство с использованием вредоносной компьютерной информации.

18.1. Задачи:

18.1.1. Определение требований и характеристик места, с которого могло быть осуществлено противоправное посягательство на компьютерную информацию.

18.1.2. Определение круга подобных мест.

18.1.3. Поиск следов, по которым возможно определить путь, проделанный электронной информацией к точке оказания ее вредоносного воздействия.

18.1.4. В зависимости от результатов определения электронных следов определить конкретное место или круг таких локаций, откуда вероятнее всего осуществлялось посягательство или проникновение.

18.2. Рекомендуемые действия:

18.2.1. Консультация со специалистом в области информационных технологий для определения возможных способов установления места осуществления посягательства на компьютерную информацию с предварительным анализом

имеющихся данных о механизме расследуемого преступления.

18.2.2. Поручение на проведение ОРМ с целью установления места на котором находилось попадающее под подозрение лицо, и откуда оно осуществляло противоправное посягательство с использованием вредоносной компьютерной информации.

19. Обстоятельство: лицо, попадающее под подозрение в совершении создания, распространения и использования вредоносных компьютерных программ, занимает бесконфликтную позицию, не намерено оказывать противодействия или даже расположено к оказанию содействия расследованию.

19.1. Задачи:

19.1.1. Выяснение всех обстоятельств, подлежащих доказыванию, предусмотренных УПК РФ.

19.1.2. См. п. 15.1.

19.2. Рекомендуемые действия:

19.2.1. Круг следственных действий и иных мероприятий может быть неограниченно широким в зависимости от выясняемых обстоятельств и механизма расследуемого преступления.

19.2.2. См. п. 15.2.

Представленная нами система рекомендаций в зависимости от сложившегося отдельного обстоятельства в следственной ситуации должна позволить синтезировать комплекс рекомендуемых действий, зависящий от варианта совокупности конкретных условий, с которыми столкнулся следователь. Сто́ит признать, что один из законов теории систем, смысл которого заключается в том, что свойства системы больше суммы свойств ее элементов, в полной мере будет действовать и в формируемой по предложенному нами методу системе рекомендаций. При комбинации двух и более приведенных нами обстоятельств рекомендуемых действий должно быть более суммы рекомендованных нами для каждого из этих обстоятельств, так как возникнет необходимость проведения дополнительных действий, детерминированных сочетанием множества. Однако в рамках объема настоящего исследования рассмотреть такого рода многоуровневую систему рекомендаций не представляется возможным. В дальнейшем мы намерены продолжить работу в этом направлении, так как она представляет для нас достаточно сильный интерес.

БИБЛИОГРАФИЯ

1. *Антонов О. Ю.*, *Себякин А. Г.* Тактические комплексы применения знаний в области компьютерной техники при расследовании преступлений // Юридическая наука и правоохранительная практика. — 2020. — № 3 (53). — С. 95. — С. 94–101.
2. *Белкин Р. С.* Курс криминалистики : в 3 т. Т. 3. Криминалистические средства, приемы и рекомендации. — М. : Бристъ, 1997. — 538 с.
3. *Бутенко О. С.*, *Голодный А. Н.* Некоторые следственные ситуации при расследовании преступлений, совершаемых с использованием компьютерной техники // Массовые коммуникации на современном этапе развития мировой цивилизации : материалы Всероссийской научной конференции с международным участием, Гуманитарно-социальный институт. — Ростов н/Д, 2015. — С. 272–276.
4. *Волчецкая Т. С.* Криминалистическая ситуалогия : монография / под ред. проф. Н. П. Яблокова. — М., Калининград, 1997. — 248 с.
5. *Головин А. Ю.* Теоретические основы и актуальные проблемы криминалистической систематики на современном этапе развития криминалистики : дис. … д-ра юрид. наук : 12.00.12. — М., 2003.
6. *Дерюгин Р. А.*, *Шергин М. А.* О некоторых особенностях расследования преступлений, совершаемых с использованием IT-технологий и в сфере компьютерной информации // Вестник Уральского юридического института МВД России. — 2021. — № 3. — С. 100–104.
7. *Еремин С. Г.* Возбуждение уголовного дела о преступлениях в сфере дистанционно-банковского обслуживания, следственные ситуации, версии, планирование и расследование на первоначальном этапе // Вестник Волгоградской академии МВД России. — 2019. — № 2 (49). — С. 78–85.

8. *Кардашевская М. В.*, *Шипилова Е. С.* Этапы процесса расследования и их характеристика // Таврический научный обозреватель. — 2015. — № 2 (октябрь).
9. *Корноухов В. Е.* Основные положения методики расследования отдельных видов преступлений. — Красноярск : Красноярский гос. ун-т, 1972. — 98 с.
10. *Поляков В. В.* Следственные ситуации по делам о неправомочном удаленном доступе к компьютерной информации // Доклады ТУСУРа. — 2010. — № 1 (21), ч. 1, июнь. — С. 46–50.
11. *Россинская Е. Р.* Криминалистика : учебник — М. : Норма : Инфра-М, 2012. — 464 с.

Материал поступил в редакцию 8 июня 2023 г.

REFERENCES (TRANSLITERATION)

1. Antonov O. Yu., Sebyakin A. G. Takticheskie kompleksy primeneniya znaniy v oblasti kompyuternoy tekhniki pri rassledovanii prestupleniy // Yuridicheskaya nauka i pravookhranitelnaya praktika. — 2020. — № 3 (53). — S. 95. — S. 94–101.
2. Belkin R. S. Kurs kriminalistiki: v 3 t. T. 3 Kriminalisticheskie sredstva, priemy i rekomendatsii. — M.: Brist, 1997. — 538 s.
3. Butenko O. S., Golodnyy A. N. Nekotorye sledstvennye situatsii pri rassledovanii prestupleniy, sovershaemykh s ispolzovaniem kompyuternoy tekhniki // Massovye kommunikatsii na sovremennom etape razvitiya mirovoy tsivilizatsii: materialy Vserossiyskoy nauchnoy konferentsii s mezhdunarodnym uchastiem, Gumanitarno-sotsialnyy institut. — Rostov n/D, 2015. — S. 272–276.
4. Volchetskaya T. S. Kriminalisticheskaya situalogiya: monografiya / pod red. prof. N. P. Yablokova. — M.; Kaliningrad, 1997. — 248 s.
5. Golovin A. Yu. Teoreticheskie osnovy i aktualnye problemy kriminalisticheskoy sistematiki na sovremennom etape razvitiya kriminalistiki: dis. … d-ra yurid. nauk: 12.00.12. — M., 2003.
6. Deryugin R. A., Shergin M. A. O nekotorykh osobennostyakh rassledovaniya prestupleniy, sovershaemykh s ispolzovaniem IT-tekhnologiy i v sfere kompyuternoy informatsii // Vestnik Uralskogo yuridicheskogo instituta MVD Rossii. — 2021. — № 3. — S. 100–104.
7. Eremin S. G. Vozbuzhdenie ugolovnogo dela o prestupleniyakh v sfere distantsionno-bankovskogo obsluzhivaniya, sledstvennye situatsii, versii, planirovanie i rassledovanie na pervonachalnom etape // Vestnik Volgogradskoy akademii MVD Rossii. — 2019. — № 2 (49). — S. 78–85.
8. Kardashevskaya M. V., Shipilova E. S. Etapy protsessa rassledovaniya i ikh kharakteristika // Tavricheskiy nauchnyy obozrevatel. — 2015. — № 2 (oktyabr).
9. Kornoukhov V. E. Osnovnye polozheniya metodiki rassledovaniya otdelnykh vidov prestupleniy. — Krasnoyarsk: Krasnoyarskiy gos. un-t, 1972. — 98 s.
10. Polyakov V. V. Sledstvennye situatsii po delam o nepravomochnom udalennom dostupe k kompyuternoy informatsii // Doklady TUSURa. — 2010. — № 1 (21), ch. 1, iyun. — S. 46–50.
11. Rossinskaya E. R. Kriminalistika: uchebnik — M.: Norma: Infra-M, 2012. — 464 s.