## Раздел 7. Экспертно-криминалистическое обеспечение правоохранительной деятельности

АНТОНОВ О.Ю.,
доктор юридических наук, доцент,
antonov@udm.ru
Факультет подготовки криминалистов;
Московская академия
Следственного комитета
Российской Федерации,
125080, г. Москва, ул. Врубеля, 12

ANTONOV O.Yu.,
Doctor of Legal Sciences,
associate professor, antonov@udm.ru
Faculty of criminalists training;
Moscow Academy of the Investigative
Committee of the Russian Federation,
Vrubel St. 12, Moscow, 125080,
Russian Federation

СЕБЯКИН А.Г.,
quattro.sa@yandex.ru
Экспертно-криминалистический отдел;
Следственное управление
Следственного комитета
Российской Федерации
по Иркутской области,
664011, г. Иркутск, ул. Володарского, 11

SEBYAKIN A.G.,
quattro.sa@yandex.ru
Forensic division;
Investigation Department
of the Investigative Committee
of the Russian Federation
for the Irkutsk Region,
Volodarsky St. 11, Irkutsk, 664011

# ТАКТИЧЕСКИЕ КОМПЛЕКСЫ ПРИМЕНЕНИЯ ЗНАНИЙ В ОБЛАСТИ КОМПЬЮТЕРНОЙ ТЕХНИКИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

**Аннотация.** В статье рассмотрены вопросы применения знаний в области компьютерной техники при решении тактических задач, обусловленных типичными следственными ситуациями. Авторами проанализированы информационные компоненты типичных следственных ситуаций, выделены основные цели тактического воздействия, предложены тактические комплексы применения знаний в области компьютерной техники. Сделан вывод о том, что в типичных следственных ситуациях при применении знаний в области компьютерной техники возможно выделение типовых тактических комплексов действий, использующих как различные формы специальных знаний, так и профессиональные знания правоприменителя. Данные комплексы могут конкретизироваться в зависимости от специфики расследования того или иного вида преступления.

**Ключевые слова:** типичная следственная ситуация; тактико-криминалистическая рекомендация; специальные знания; тактическое решение; цель тактического воздействия; тактический комплекс.

Для цитирования: Антонов О.Ю., Себякин А.Г. Тактические комплексы применения знаний в области компьютерной техники при расследовании преступлений // Юридическая наука и правоохранительная практика. 2020. N 3 (53). С. 94-101.

# TACTICAL COMPLEXES OF APPLYING KNOWLEDGE IN THE FIELD OF COMPUTER TECHNOLOGY WHILE INVESTIGATING CRIMES

**Annotation.** The issues concerning the application of knowledge in the field of computer technology while solving tactical problems caused by typical investigative situations are analyzed in the article. The authors of the article analyzed the information components of typical investigative situations, identified the main objectives of tactical impact, and proposed tactical complexes for applying knowledge in the field of computer technology. It is concluded that, when applying knowledge in the field of computer technology in typical investigative situations, it is possible to identify typical tactical complexes of actions that involve both various forms of special knowledge and professional knowledge of the law enforcer. These complexes can be specified depending on the specifics of the investigation of a particular type of crime.

**Keywords:** typical investigative situation; tactical and forensic recommendation; special knowledge; tactical decision; purpose of tactical influence; tactical complex.

For citation: Antonov O.Yu., Sebyakin A.G. Tactical complexes of applying knowledge in the field of computer technology while investigating crimes // Legal Science and Law Enforcement Practice. 2020. No. 3 (53). P. 94-101.

Применение знаний в области компьютерной техники при расследовании преступлений можно отнести к одному из динамично развивающихся элементов различных отраслей юридической науки. Так, в УПК РФ в 2012 году были введены две поправки (п. 9.1 ст. 182 и п. 3.1 ст. 183), регулирующие изъятие электронных носителей при производстве обыска и выемки, которые, однако, просуществовали только 6 лет. Вместо указанных пунктов в декабре 2018 года введена отдельная статья 164.1 УПК РФ*, призванная унифицировать вопросы изъятия электронных носителей при производстве следственных действий.

Однако традиционной «площадкой» обсуждения вопросов, связанных с извлечением из электронных носителей значимой для следствия информации, является криминалистическая отрасль юридической науки. Предложенная А.Ф. Волынским система криминалистического обеспечения расследования преступлений, наряду с иными структурными элементами, включает в себя технико-криминалистическое обеспечение и тактико-криминалистическое обеспечение [1, с. 21]. В научной литературе больше внимания традиционно уделяется технико-криминалистическим аспектам, в том числе проблемам применения специальных знаний [2, с. 335; 3]. Это вызвано внедрением большого количества новых средств и методов выявления криминалистически значимой информации. Данная статья имеет целью рассмотрение способов решения именно тактических задач применения знаний в области компьютерной техники, обусловленных типичными следственными ситуациями.

Выделение в типичной следственной ситуации тактических задач, для решения которых требуются знания в области компьютерной техники, приводит к возможности выбора и применения комплексов тактических действий, облеченных в форму тактико-криминалистических рекомендаций, состоящих из следующих элементов:

– комплексная оценка информационного компонента следственной ситуации, требующей использования знаний в области компьютерной техники;

– определение цели тактического воздействия посредством формулирования ряда задач;

– определение приоритета, последовательности тактических действий, прогнозирование развития следственной ситуации.

Каждый элемент тактической рекомендации должен обязательно обладать свойством типичности, иначе снижается эффективность самой тактической рекомендации. Рассматривая следственную ситуацию как «совокупность условий, в которых осуществляется расследование в конкретный момент времени» [4, с. 133], можно выделить следующие типичные ситуации, требующие использования знаний в области компьютерной техники:

1) имеется информация о месте совершения преступления, в котором потенциально может быть обнаружен электронно-цифровой носитель, содержащий криминалистически значимую информацию (офис, жилище, адрес, по которому осуществляется незаконная деятельность);

2) имеется информация о лице (лицах), причастном к совершению преступления, пользующемся компьютерными, информационно-телекоммуникационными устройствами;

3) имеется информация о наличии в персональных компьютерных устройствах потерпевшего электронно-цифровых следов;

4) имеется информация о наличии в персональных компьютерных устройствах подозреваемого (обвиняемого) электронно-цифровых следов.

Возможны различные комбинации приведенных следственных ситуаций (например, информация о лицах, причастных к совершению преступления, может сочетаться с информацией о месте совершения преступления) или переход из одной

* О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 27 дек. 2018 г. N 533-ФЗ // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

следственной ситуации в другую (например, при наличии информации о лицах, причастных к совершению преступления, ожидаемой ситуацией будет являться существование информации о наличии в персональных устройствах подозреваемого (обвиняемого) электронно-цифровых следов). Каждая из указанных следственных ситуаций может конкретизироваться и детализироваться в зависимости от вида совершенного преступления.

При рассмотрении тактических задач, требующих применения знаний в области компьютерной техники, необходимо учитывать деление следственных ситуаций на конфликтные и бесконфликтные [5, с. 43]. Согласно определению, данному А.Р. Ратиновым, «бесконфликтная ситуация характеризуется полным или частичным совпадением интересов участников взаимодействия, отсутствием противоречий в целях, к достижению которых направлены их усилия на данном этапе расследования... Ситуации конфликтов различной длительности и остроты возникают тогда, когда между участниками процесса складываются отношения соперничества и противодействия» [6, с. 157].

Применительно к использованию знаний в области компьютерной техники бесконфликтная ситуация возникает при содействии следствию, выраженном в добровольном информировании о местонахождении электронных носителей, на которых содержится криминалистически значимая информация, их выдаче, сообщении аутентификационных данных. Противодействие же выражается в сокрытии указанной информации, а также в совершении попыток уничтожения криминалистически значимой информации, содержащейся на электронно-цифровом носителе.

Перечисленные типичные следственные ситуации (согласно Т.С. Волчецкой – ситуации познавательного типа) объединяют взаимосвязанные цели, для достижения которых необходимо применение знаний в области компьютерной техники. К основным целям следует отнести:

1) установление возможного носителя электронно-цифровых следов;

2) обнаружение на носителе электронно-цифровых следов, их изъятие и фиксацию;

3) анализ выявленных электронно-цифровых следов.

Как дополнительную цель использования знаний в области компьютерной техники можно выделить деятельность, направленную на преодоление противодействия расследованию, выражающееся в выявлении сокрытой криминалистически значимой информации на электронно-цифровом носителе и предотвращении попыток ее уничтожения.

С технической точки зрения в работе с электронно-цифровыми носителями А.В. Гончаров, например, выделяет следующие этапы:

1. Извлечение и копирование данных из электронно-цифрового носителя.

2. Преобразование (декодирование) полученной информации в вид, пригодный для дальнейшей обработки, анализа.

3. Анализ извлеченной информации [3, с. 187].

В данном случае необходимо отметить, что операции извлечения и преобразования (декодирования) информации в подавляющем большинстве случаев выполняются в едином технологическом цикле, поэтому с тактической точки зрения разделение указанных этапов, формирующих описанную выше вторую цель тактического воздействия, не имеет большого значения.

Что же касается анализа извлеченной информации, то, являясь этапом работы с электронно-цифровыми носителями, он может также рассматриваться и как цель тактического воздействия. Существует категория информации, наличие которой уже является для следователя криминалистически значимым фактом, например, информация, содержащаяся на сканированной копии экономического документа с необходимыми атрибутами (подписью, печатью). Другая категория информации, помимо ее обнаружения, требует анализа, сопоставления с уже имеющимися сведениями, дополнительного исследования. Соответственно, в зависимости от следственной ситуации, вида преступления анализ выявленных электронно-цифровых следов может выступать в качестве отдельной типичной цели тактического воздействия.

Достижение цели осуществляется посредством постановки соответствующих задач, решаемых путем проведения

тактических действий и их комплексов (комбинаций, операций). Т.С. Волчецкая в качестве основы подхода для разрешения следственных ситуаций познавательного типа выделяет комплексность, подразумевая под ней «единую систему следственных действий и оперативно-розыскных мероприятий, в которых имеет место взаимообусловленность, направленная на разрешение ситуации» [7, с. 44]. Таким образом, следственная ситуация разрешается посредством достижения целей тактического воздействия через постановку соответствующих задач, решаемых путем проведения тактических действий и их комплексов (комбинаций, операций).

Цель установления возможного носителя электронно-цифровых следов может быть достигнута путем решения двух задач – установления следов преступной деятельности и выявления следов присутствия конкретных лиц в определенном месте (точке) географического пространства.

Под следами преступной деятельности подразумеваются следы, свидетельствующие:

– об определенной активности лица в электронно-цифровом пространстве, совершении манипуляций с электронными вычислительными и (или) информационно-коммуникационными средствами, ведущих к достижению преступного умысла;

– о совершении физических действий, ведущих к достижению преступного умысла, запечатленных на электронно-цифровом носителе посредством электронно-оптических устройств (фотоаппаратов, видеокамер).

Абсолютное большинство следов преступной деятельности обнаруживается в трех категориях устройств:

– в служебных устройствах (устройства, предназначенные для выполнения определенных функций, обусловленных деятельностью лица);

– персональных устройствах (мобильные средства связи, домашние средства информационно-коммуникационной техники);

– различных системах видеофиксации (стационарных, мобильных, открытых, скрытых, внешних, внутренних).

Следы присутствия указывают на нахождение конкретного известного или неустановленного лица в определенном месте без оценки его действий, вне привязки к реализации преступного умысла.

На следы нахождения конкретного лица в определенном месте могут указывать:

– детализации телефонных соединений средств мобильной радиосвязи с обозначением базовой станции, осуществившей сервис;

– упомянутые выше системы видеофиксации.

Обнаружение на носителе электронных следов, их изъятие и фиксация – обобщенная цель, которую необходимо конкретизировать в зависимости от вида преступлений и типичной следственной ситуации.

В качестве типовых задач для достижения указанной цели можно выделить:

– обнаружение пользовательских файлов – текстовых, мультимедийных (графические изображения, видео-, аудиозаписи и пр.), а также иных файлов, созданных пользователем посредством различных прикладных программ. Необходимо учитывать, что криминалистическую значимость может иметь не только непосредственное содержимое файла (так называемый контент), но и метаданные (сведения о различных признаках и свойствах контента). К таковым можно отнести даты создания (изменения, печати, удаления) файла, источник получения (создания) файла и пр.;

– обнаружение специализированного программного обеспечения – любого коммерческого и свободно распространяемого программного обеспечения, которое может служить инструментом для осуществления преступного замысла (например, платформа 1С – для автоматизации финансовой деятельности организации, программы дистанционного банковского обслуживания, подачи деклараций, программы для организации игорной деятельности, программы анонимизации интернет-траффика и пр.);

– определение активности пользователя в сети Интернет. Составными частями данной задачи являются: обнаружение факта посещения интернет-ресурсов (в том числе социальных сетей), фиксация даты и времени посещения, наличие аккаунтов, выявление пользования услугами интер-

нет-банкинга, переписка посредством электронной почты или интернет-мессенджеров. В качестве отдельной подзадачи необходимо выделить обнаружение, декодирование и фиксацию аутентификационных данных пользователя: логинов и паролей, сохраненных в файлах cookie интернет-обозревателей;

– получение детализаций телефонных соединений известных участников уголовного дела или информации о телефонных соединениях, совершенных в конкретной точке (точках) местности, от операторов мобильной радиосвязи. Кроме того, в данную задачу входит получение служебной информации о базовых станциях операторов мобильной радиосвязи, осуществляющих соединения: координаты, высота и угол подвеса, азимут, сектор обслуживания.

Объектом анализа выявленных электронно-цифровых следов как отдельной типичной цели тактического воздействия является уже зафиксированная информация. Исследованию может быть подвергнуто содержимое пользовательских файлов на предмет соответствия каким-либо критериям. Обобщенным критерием выступает относимость содержащейся информации к совершенному преступлению. В зависимости от вида преступления указанный критерий может быть уточнен и конкретизирован (например, отнесение видеозаписи или графического контента к порнографии, отнесение записи в базе данных к конкретной финансовой сделке, совпадение искомого контекста в конкретном документе и пр.).

Анализ активности пользователя в сети Интернет может дать следствию информацию о ранее не установленных потенциальных потерпевших и, соответственно, привести к возникновению дополнительных эпизодов в расследовании уголовного дела. Выявление тематических групп или сообществ в интернет-пространстве может привести к установлению лиц, занимающихся аналогичной противоправной деятельностью. Кроме того, результатом анализа сведений о телефонных соединениях участников уголовного судопроизводства может стать решение круга задач: определение возможного нахождения участника уголовного дела в конкретное время в конкретном месте, оценка потенциальной возможности встречи двух (или более) участников уголовного дела, выявление иных участников, ранее не известных следствию, и пр.

Выявление электронно-цифровых следов преступной деятельности как тактической цели в рассматриваемых типичных следственных ситуациях требует совершения определенных тактических действий или их сочетаний (комбинаций, операций, комплексов). Соответственно, можно выделить универсальные (типичные) тактические комплексы, в основе которых лежит применение знаний в области компьютерной техники.

В случае развития исходной следственной ситуации в бесконфликтном русле при наличии информации о месте совершения преступного деяния представляется эффективным следующий тактический комплекс:

1) допрос участников уголовного дела с участием специалиста в области компьютерной техники. Присутствие на допросе указанного специалиста позволит выявить особенности образования электронно-цифровых следов в процессе осуществления преступной деятельности. В результате допроса достигается цель установления возможных носителей электронно-цифровых следов действий, получения аутентификационных данных: логинов, паролей от различных информационных ресурсов, в том числе облачных;

2) осмотр места происшествия с участием специалиста, присутствие которого может способствовать выявлению местонахождения электронных носителей электронно-цифровых следов действий и следов присутствия.

Далее исходная следственная ситуация развивается в ситуацию, в которой имеется информация о наличии в персональных устройствах потерпевшего или заподозренного лица электронно-цифровых следов. В этом случае необходим комплекс действий, в основе которого лежит осмотр электронно-цифровых носителей информации. С точки зрения выявления и фиксации электронно-цифровых следов данный этап является одним из важнейших и может осуществляться в рамках различных следственных действий с при-

менением различных форм специальных знаний;

3) осмотр электронных носителей в рамках осмотра места происшествия. Может осуществляться как с участием специалиста в области компьютерной техники, так и самостоятельно следователем, с использованием своих профессиональных знаний. Участие специалиста (или специалистов) на данном этапе позволит оценить степень риска (утраты следов), поможет принять решение о необходимости изъятия электронно-цифровых носителей (либо об отсутствии таковой). При осмотре подлежат решению задачи обнаружения пользовательских файлов, специализированного программного обеспечения, интернет-активности пользователей. В случае достижения позитивного результата (обнаружение искомых следов и их достаточность) изъятие электронно-цифрового носителя не является необходимым;

4) в случае негативного результата осмотра электронно-цифрового носителя следователем (невыявление следов) в рамках осмотра места происшествия лицо, осуществляющее следствие, может принять решение об изъятии указанного носителя для последующего исследования. Дальнейший осмотр может быть осуществлен в рамках осмотра предметов с участием специалиста. Участие специалиста на данном этапе повышает вероятность обнаружения искомых следов;

5) анализ выявленной информации по необходимым для дела критериям, в том числе для решения задачи выявления потенциальных потерпевших и лиц, занимающихся аналогичной противоправной деятельностью.

Если в рамках проведенного осмотра в соответствии с пунктами 3 и 4 не получена исчерпывающая информация, то следует выполнить следующие действия:

6) назначение компьютерно-технической экспертизы. Данное тактическое действие предусматривает совершенно иную форму применения специальных знаний – проведение судебной экспертизы. Необходимость назначения компьютерно-технической экспертизы обусловливается недостижением тактической цели в результате реализации ранее описанных частей тактического комплекса, хотя данный тезис и является спорным [8, с. 115]. Вообще, вопросы применения данной формы специальных знаний находятся в сфере научного интереса правового института судебной экспертизы и выходят за рамки проблем, рассматриваемых в настоящей статье.

Тем не менее с точки зрения тактики применения знаний в области компьютерной техники необходимо акцентировать внимание именно на месте судебной компьютерно-технической экспертизы в тактическом комплексе. Судебная компьютерно-техническая экспертиза не входит в перечень обязательных для назначения экспертиз, перечисленных в ст. 196 УПК РФ. Следовательно, назначение данной экспертизы в соответствии с ч. 1 ст. 195 УПК РФ происходит только в случае признания необходимости применения специальных знаний для решения тактической задачи. Для того чтобы оценить необходимость назначения судебной компьютерно-технической экспертизы, требуется реализация ранее описанных частей тактического комплекса, в которых свою положительную роль могут сыграть и профессиональные знания следователя. Потребность в назначении судебной компьютерно-технической экспертизы возникает только в случае, если тактическая цель не достигнута реализацией вышеуказанных этапов тактического комплекса.

В случае конфликтного развития следственной ситуации (противодействия) при наличии информации о месте совершения преступного деяния для достижения цели установления возможного носителя электронно-цифровых следов представляется более эффективным заменить допрос с участием специалиста следующим элементом тактического комплекса;

7) обыск с участием специалиста в области компьютерной техники. Планирование обыска с участием специалиста позволяет предусмотреть и осуществить блокирование возможности отключения сетевых соединений, совершения звонков и (или) операций с вычислительной техникой.

Следственная ситуация, характеризующаяся наличием информации о месте совершения преступления, часто требует решения таких тактических задач, как установление иных лиц, причастных к со-

вершению преступления, и возможного их местонахождения в момент совершения преступления, установление и анализ информационных связей участников уголовного дела (подозреваемых, потерпевших, свидетелей и пр.). В этом случае на практике находит подтверждение эффективность следующего тактического комплекса действий;

8) получение у операторов, оказывающих услуги сотовой связи, сведений о детализациях телефонных переговоров известных участников уголовного дела, а также сведений о месторасположении и направленности (азимуте) сервисных базовых станций;

9) оценка радиоэлектронной обстановки с участием специалиста в области компьютерной техники. Она обеспечивает получение информации о базовых станциях, осуществляющих сервис в конкретной географической или административной точке. Данное действие фиксируется в виде протокола осмотра местности или протокола осмотра места происшествия;

10) анализ полученных данных. В зависимости от задачи анализа он может быть осуществлен как самим следователем (с использованием профессиональных знаний), так и специалистом, в том числе с применением специализированных аппаратно-программных комплексов. В случае привлечения к анализу специалиста результат анализа, в зависимости от формы применения специальных знаний, может быть оформлен заключением специалиста либо заключением эксперта.

Любая следственная ситуация в отношении потерпевших чаще всего развивается бесконфликтно, поэтому в случае присутствия информации о наличии в персональных устройствах потерпевшего электронно-цифровых следов наиболее целесообразна последовательность действий, описанных в пп. 3-6. Соответственно, данную последовательность можно выделить как типовой тактический комплекс применения знаний в области компьютерной техники, который осуществляется в типичных следственных ситуациях, когда имеется информация о наличии электронно-цифровых следов на устройствах, эксплуатируемых потерпевшим или подозреваемым (обвиняемым, свидетелем).

В зависимости от степени конфликтности ситуации для выявления носителей электронно-цифровых следов возможно применение тактических действий, описанных в пп. 1 и 2 или в п. 7. Данные действия объединены в комплекс, применяемый в типичной следственной ситуации, когда имеется информация о месте совершения преступления.

Если получена информация о лице либо лицах, причастных к совершению преступления, а также оказывается противодействие расследованию, то применим типовой тактический комплекс, описанный в пп. 8-10.

Вышеизложенное позволяет сделать вывод о возможности выделения в типичных следственных ситуациях при применении знаний в области компьютерной техники типовых тактических комплексов действий, использующих как различные формы специальных знаний, так и профессиональные знания правоприменителя:

– в случае бесконфликтного развития следственной ситуации необходим допрос участников уголовного дела с участием специалиста в области компьютерной техники; осмотр места происшествия с участием специалиста;

– при наличии противодействия (конфликтное развитие следственной ситуации) предыдущий комплекс действий меняется на обыск с участием специалиста в области компьютерной техники (возможный вариант развития ситуации – одновременные обыски с участием специалистов в различных местах);

– в случае получения информации о наличии в персональных устройствах электронно-цифровых следов наиболее целесообразна такая последовательность действий: осмотр электронных носителей с возможным (необязательным) участием специалиста; анализ выявленной информации по необходимым для расследования критериям. Если в рамках проведенного осмотра не получена исчерпывающая информация, то необходимо изъятие электронно-цифровых носителей в рамках обыска или выемки и назначение по ним компьютерно-технической экспертизы;

– в следственной ситуации, когда имеется информация о лице либо лицах, причастных к совершению преступления, а

также оказывается противодействие расследованию, применим типовой тактический комплекс, состоящий из получения в порядке, установленном ст. 186.1 УПК РФ, у операторов сотовой связи сведений о детализациях телефонных переговоров известных участников уголовного дела, а также сведений о месторасположении и направленности базовых станций; оценки радиоэлектронной обстановки с участием специалиста в области компьютерной техники; анализа полученных данных. В зависимости от задачи анализа он может быть осуществлен как самим следователем, так и сведущим лицом (специалистом, экспертом).

Данные тактические комплексы могут быть конкретизированы в зависимости от специфики расследования того или иного вида преступления. Планирование конкретного тактического комплекса в конкретной следственной ситуации с участием специалиста в области компьютерной техники позволит как спрогнозировать развитие следственной ситуации в процессе реализации тактического комплекса, так и обозначить возможные «точки приложения» профессиональных знаний следователя и специальных знаний сведущего лица, тем самым определив форму их использования, а также рационально распределить имеющиеся ресурсы.

**Список литературы**

1. Волынский А.Ф. Криминалистическое обеспечение раскрытия и расследования преступлений: учеб. пособие. М.: Московский ун-т МВД России им. В.Я. Кикотя, 2016. 195 с.

2. Лавров В.П. Некоторые современные проблемы криминалистического обеспечения расследования преступлений // Оптимизация деятельности органов предварительного следствия и дознания: правовые, управленческие и криминалистические проблемы: сб. науч. ст. междунар. науч.-практ. конф. / под ред. И.П. Можаевой. М.: Акад. управления МВД России, 2017. С. 331-336.

3. Гончаров А.В. Использование возможностей современных инновационных технологий при исследовании цифровых устройств мобильной связи и компьютерных носителей информации при расследовании преступлений // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития: материалы междунар. науч.-практ. конф. М.: Московская акад. СК России, 2019. С. 186-201.

4. Белкин Р.С. Курс криминалистики: в 3 т. Т. 3. Криминалистические средства, приемы и рекомендации. М.: Юристъ, 1997. 538 с.

5. Драпкин Л.Я. Понятие и классификация следственных ситуаций // Следственные ситуации и раскрытие преступлений: науч. тр. Свердловск: Свердловский юрид. ин-т, 1975. Вып. 41. С. 26-44.

6. Ратинов А.Р. Судебная психология для следователей. М.: Юрлитинформ, 2008. 350 с.

7. Волчецкая Т.С. Ситуационный подход в практической и исследовательской криминалистической деятельности: учеб. пособие. Калининград: Изд-во Калининградского ун-та, 1999. 74 с.

8. Россинская Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия Тульского государственного университета. Экономические и юридические науки. 2016. N 3-2. С. 109-117.

**References**

1. Volynsky A.F. Forensic support for the disclosure and investigation of crimes. Moscow, Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V.Ya. Kikotya, 2016, 195 p. (In Russ.).

2. Lavrov V.P. Some modern problems of forensic support for the investigation of crimes. Optimization of the activities of the bodies of preliminary investigation and inquiry: legal, managerial and forensic problems. Moscow, Academy of Management of the Ministry of Internal Affairs of the Russian Federation, 2017. Pp. 331-336. (In Russ.).

3. Goncharov A.V. Using the capabilities of modern innovative technologies in the study of digital mobile communication devices and computer storage media in the investigation of crimes. Criminalistics – the past, present, future: achievement and development prospects. Moscow, Moscow Academy of the Investigative Committee of the Russian Federation, 2019. Pp. 186-201. (In Russ.).

4. Belkin R.S. Forensic course. In 3 volumes. Vol. 3. Forensic tools, techniques and recommendations. Moscow, Yurist Publ., 1997. 538 p. (In Russ.).

5. Drapkin L.Ya. Concept and classification of investigative situations. Investigative situations and crime detection. Sverdlovsk, Sverdlovsk Law Institute, 1975. Issue 41. Pp. 26-44. (In Russ.).

6. Ratinov A.R. Forensic psychology for investigators. Moscow, Jurlitinform Publ., 2008. 350 p. (In Russ.).

7. Volchetskaya T.S. A situational approach in practical and research forensic activity. Kaliningrad, Kaliningrad University Publishing House, 1999. 74 p. (In Russ.).

8. Rossinskaya E.R. On the question of the private theory of information and computer support of criminalistic activity. Bulletin of the Tula State University. Economic and legal sciences, 2016, no. 3-2, pp. 109-117. (In Russ.).