ПРОБЛЕМЫ КРИМИНАЛИСТИКИ

А.А. Топорков*, И.С. Сербин**

КРИМИНАЛИСТИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПНЫХ ПОСЯГАТЕЛЬСТВ НА КОММЕРЧЕСКУЮ ТАЙНУ

Аннотация. *В данной статье рассматриваются криминалистические и организационные особенности расследования незаконного получения сведений, составляющих коммерческую тайну. Рассмотрены: начальная стадия уголовного процесса, возбуждение уголовного дела, особенности этапа предварительной проверки, типичные следственные ситуации первоначального этапа расследования и программа действий по их разрешению. Отмечено, что наиболее важным элементом расследования по делам указанного вида является наличие инструментов, позволяющих повысить продуктивность мыслительной и организационной деятельности следователя, а использование информационных моделей и типовых программ действий следователя позволяет легче понять обстоятельства исходной ситуации расследования, осознать его цели, осуществлять целенаправленный поиск и распознавание, систематизацию и оценку значимой для расследования информации. Кроме того, значительно облегчается аналитическая обработка полученных фактических данных, выдвижение версий и планирование расследования конкретных дел.*

Ключевые слова: *юриспруденция, предварительная проверка, рекомендации, особенности расследования, следственные ситуации, сведения, программы действий, методика, ифнормационные модели, цели осмотра.*

Возбуждение уголовного дела — начальная стадия уголовного процесса.

Поводами для возбуждения уголовного дела служат: заявление о преступлении; явка с повинной; сообщение о совершенном или готовящемся преступлении, полученное из других источников.

Заявление о незаконном получении сведений, составляющих коммерческую тайну, поступают от собственника конфиденциальной информации, на которую совершено посягательство. Непосредственным исполнителем заявлений (и прилагающихся к ним документов), как правило, являются службы безопасности организаций.

© Топорков Анатолий Алексеевич
* Доктор юридических наук, профессор кафедры криминалистики Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
[toporkov2014@list.ru]
123995, г. Москва, ул. Садовая-Кудринская, д. 9.

© Сербин Игорь Сергеевич
** Кандидат юридических наук, адвокат
[advokat@serbin.ru]
119002, г. Москва, Сивцев Вражек, д. 43

В силу специфики системы защиты коммерческой тайны названные службы, как правило, первыми обнаруживают признаки противоправных деяний этого вида. Полученные этими службами сведения фиксируются в материалах служебных (процессуальных) расследований. Указанные материалы обычно состоят из объяснений работников организации, объектов — носителей информации, планов, схем, фотографий места происшествия; заключений по результатам расследования и некоторых других документов.

В случае обращения собственника информации за защитой в правоохранительных органы материалы служебного расследования используются следователем при решении вопроса о возбуждении уголовного дела. Кроме того, содержащиеся в них данные о месте, времени, причастных лицах и других обстоятельствах могут оказать существенную помощь следователю в выдвижении версий, организации и планировании расследования.

Вместе с тем необходимо учитывать, что выводы работников службы безопасности требуют тщательной проверки следственным путем, поскольку проводимые ими расследования не основываются на нормах процессуального закона и регулируются внутренними (локальными) нормативными актами: ведомственными инструкциями, положениями, методиками.

На стадии возбуждения уголовного дела исследуются как обстоятельства, влекущие за собой возбуждение уголовного дела, так и исключающие производство по делу, т.е. отказ в возбуждении уголовного дела. Исчерпывающий перечень обстоятельств, исключающих производство по делу, содержится в ст. 24 УПК. При исследовании названных обстоятельств по делам о противоправных посягательствах на коммерческую тайну в первую очередь следует обратить внимание на два специфических момента:

1) на наличие у предполагаемого предмета преступного посягательства трех обязательных признаков: материального, информативного и удостоверительного;
2) на включение предполагаемого предмета преступного посягательства в систему охранительных отношений, устанавливаемых режимом коммерческой тайны.

Это означает, что проверка сообщения о преступлении, проводящаяся в порядке ст. 144 УПК РФ, должна содержать ответы на следующие вопросы:

– имеет ли предполагаемый предмет преступного посягательства статус документа, установленный ст. 3 и 10 Федерального закона «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ;
– составляет ли содержащаяся в документе информация коммерческую тайну, имеющую действительную или потенциальную коммерческую ценность (в соответствии с ч. 2 ст. 3 ФЗ «О коммерческой тайне» и не относится ли она к сведениям, которые не могут составлять коммерческую тайну (в соответствии со ст. 5 названного Закона). После возбуждения уголовного дела следует назначить экспертизу по определению конфиденциальных сведений, содержащихся в документе;
– включен ли предполагаемый предмет преступного посягательства в систему охранительных отношений — в режим коммерческой тайны, имеет ли предусмотренные ч. 5 ст. 10 ФЗ «О коммерческой тайне» реквизиты: регистрационный номер, гриф «Коммерческая тайна» с указанием обладателя информации.

Отрицательный ответ на любое из указанных выше обстоятельств является основанием для отказа в возбуждении уголовного дела в связи с отсутствием предмета посягательства, а следовательно, с отсутствием в деянии состава преступления.

Для организации расследования фактов незаконного получения сведений, составляющих коммерческую тайну, существенное значение имеет наличие информации о связи этого противоправного деяния с другими преступлениями, к числу которых относятся:

1) незаконное разглашение сведений, составляющих коммерческую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе (ч. 2 ст. 183 УК);
2) неправомерный доступ к компьютерной информации в случаях, когда эта информация содержит сведения, составляющие коммерческую тайну (ст. 272 УК);
3) завладение носителем конфиденциальной информации (в частности, имеющим материальную ценность, например ноутбуком) путем кражи (ст. 158 УК), грабежа (ст. 161 УК), разбоя (ст. 162 УК);
4) действия лиц государственных организаций и органов местного самоуправления, ответственных за документ за надлежащую организацию работы участка конфиденциального делопроизводства; членов комиссии по проверке наличия конфиденциальных документов, маскирующих факт недостачи конфиденциальных материалов путем служебного подлога (ст. 292 УК РФ) и т.д.

Наиболее сложными в сфере расследования преступных посягательств на коммер-

ческую тайну представляются события, связанные с похищением конфиденциальных документов в условиях неочевидности, либо с перехватом конфиденциальной информации, циркулирующих в технических средствах и помещениях.

I. Для первоначального этапа расследования по фактам похищения конфиденциальных документов в условиях неочевидности характерны следующие *типичные следственные ситуации*:

Ситуация 1. Обнаружена недостача документа по месту хранения, обстоятельства выхода из законного владения неизвестны.

Ситуация 2. Документ обнаружен вне установленного места хранения с признаками возможного ознакомления посторонними.

Ситуация 3. Документ поступил в распоряжение законного обладателя или правоохранительных органов от посторонних лиц после выхода из законного владения при невыясненных обстоятельствах.

Для разрешения указанных ситуаций следователю предстоит решить ряд задач с целью получения ответов на следующие вопросы:

– что представляет собой документ, вышедший из законного владения (его характеристики, внешние признаки, наличие сведений, содержащих коммерческую тайну, соответствующего грифа и других реквизитов);
– кто является лицом, ответственным за сохранность документа (когда и в какой связи получен документ, как оформлено получение);
– какова причина выхода документа из законного владения;
– что произошло: похищение документа или его утрата;
– имеются ли признаки маскировки (сокрытия) нарушений правил хранения документа. Какие;
– имеются ли признаки маскировки отсутствия документа. Какие;
– кто маскировал отсутствие документа (лицо, утратившее его, или похититель);
– сколько человек участвовало в похищении документа;
– каким путем похититель (похитители) проник на место хранения документа (информации) и как покинул его;
– каковы мотив и цель действия похитителя;
– кто может сообщить сведения, необходимые для раскрытия существа события;
– какие обстоятельства способствовали совершению выхода документа из законного владения (его утрате или похищению).

Первая следственная ситуация

Обнаружена недостача документа по месту хранения, обстоятельства выхода из законного владения неизвестны.

Типичные следственные версии:

1. Документ похищен работниками организации.
2. Документ похищен лицами, не являющимися работниками организации, находившимися в хранилище в связи с выполнением каких-либо работ либо проводившими там время по приглашению лица, ответственного за документ.
3. Документ утрачен ответственным за него лицом.

Программа действий следователя при проверке первой следственной ситуации:

– Осмотр помещения (места) хранения документа.
– Осмотр сейфа (другого хранилища), в котором находился документ.
– Осмотр документа, аналогичного недостающему.
– Осмотр учетной документации участка конфиденциального делопроизводства.
– Назначение ревизии конфиденциального делопроизводства.
– Назначение экспертизы по определению конфиденциальности документа.
– Назначение экспертизы вещественных доказательств.
– Допрос лица, ответственного за документ.
– Допрос лиц, обнаруживших отсутствие документа.
– Подготовка поручения о производстве оперативно-розыскных (сыскных) действий.

Вторая следственная ситуация

Документ обнаружен вне установленного места хранения с признаками возможного ознакомления посторонними.

Типичные следственные версии:

1. Документом временно завладели работники организации с целью копирования либо ознакомления с содержащимися в нем конфиденциальными сведениями.
2. Документом временно завладели с указанной выше целью лица, не являющиеся работниками организации, находившиеся в хранилище в связи с выполнением каких-либо работ либо проводившими там время по приглашению лица, ответственного за документ.
3. Документ утрачен ответственным за него лицом.

Программа действий следователя при проверке второй следственной ситуации:

1. Осмотр места обнаружения документа.
2. Осмотр обнаруженного документа.

3. Осмотр упаковочного материала.
4. Осмотр места (сейфа) хранения документа.
5. Осмотр средств доставки документа.
6. Осмотр учетной документации по месту хранения документа, доставочной документации.
7. Назначение ревизии конфиденциального делопроизводства.
8. Назначение экспертизы по определению конфиденциальности документа.
9. Назначение экспертизы вещественных доказательств.
10. Допрос лица, ответственного за документ.
11. Допрос лиц, которые обнаружили отсутствие документа.
12. Подготовка поручения о производстве оперативно-розыскных (сыскных) мероприятий.

Третья следственная ситуация

Документ поступил в распоряжение законного обладателя или правоохранительных органов от посторонних лиц после выхода из законного владения при невыясненных обстоятельствах.

Типичные следственные версии:

1. Документ был похищен и возвращен собственнику информации похитителем с целью компрометации ответственного за него лица.
2. Документ был похищен с целью собирания конфиденциальной информации одним лицом и возвращен другим лицом, не причастным к похищению.
3. Документ был утрачен ответственным за него лицом и возвращен посторонним.

Программа действий следователя при проверке третьей следственной ситуации:

1. Допрос лиц, передавших документ в распоряжение законного обладателя или правоохранительных органов.
2. Осмотр поступившего документа либо его части.
3. Осмотр упаковочного материала.
4. Осмотр места хранения документа.
5. Осмотр сейфа, в котором хранился документ.
6. Осмотр учетной документации по месту хранения документа, доставочной документации.
7. Назначение ревизии конфиденциального делопроизводства.
8. Назначение экспертизы по определению конфиденциальности документа.
9. Назначение экспертизы вещественных доказательств.
10. Подготовка поручения о производстве оперативно-розыскных (сыскных) действий.

Лицам, осуществляющим оперативно-розыскные (сыскные) мероприятия, поручается выявление следующих сведений, имеющих отношение к утрате документа либо его похищению:

1. об обстоятельствах выхода документа из законного владения;
2. о деловых и личных качествах лица, ответственного за документ, возможно, связанных с утратой (похищением) последнего;
3. о возможно допускавшихся нарушениях правил обращения с документом;
4. о маскировке возможных нарушений правил конфиденциального делопроизводства;
5. о маскировке лицом, ответственным за документ, своей причастности к его утрате;
6. об организациях и лицах, которые могли быть заинтересованы в похищении документа;
7. о нераскрытых похищениях, совершенных аналогичным способом;
8. о лицах, вынашивавших намерение совершить похищение документа;
9. о лицах, имеющих орудие преступления, подобное примененному при похищении;
10. о фактах использования похищенного документа и содержащейся в нем информации;
11. о лицах (организациях), незаконно завладевших документом.

II. Для первоначального этапа расследования незаконного собирания сведений путем перехвата конфиденциальной информации, циркулирующей в технических средствах и помещениях, характерны следующие *типичные следственные ситуации:*

Ситуация 1. Сведения, составляющие коммерческую тайну, незаконно получены посторонним лицом (организацией). Обстоятельства выхода информации из законного владения неизвестны. Имеются основания полагать, что они собраны путем перехвата информации, циркулирующей в технических средствах и помещениях.

Типичные следственные версии

i. Перехват информации совершен с применением специально изготовленных технических средств, установленных вне помещения, где обрабатывается или циркулирует конфиденциальная информация.
ii. Перехват совершен с применением специально изготовленных технических средств, установленных в помещении, где обрабатывается или циркулирует конфиденциальная информация.
iii. Перехват совершен без применения специально изготовленных технических средств в помещении, где обрабатывается или циркулирует конфиденциальная информация.

iv. Перехват совершен без применения специально изготовленных технических средств за пределами помещения, где обрабатывается или циркулирует конфиденциальная информация.

Задачи, которые предстоит решить уполномоченным лицам в первой следственной ситуации, состоят в том, чтобы установить и удостоверить факт незаконного получения сведений, выявить способ перехвата информации и виновных лиц, установить размер ущерба, причиненного собственнику сведений, выявить обстоятельства, способствовавшие незаконному собиранию сведений путем перехвата информации.

Ситуация 2. В технических средствах или помещениях обнаружено электронное устройство перехвата информации, внедренное при невыясненных обстоятельствах.

Типичные следственные версии

1. Устройство перехвата информации внедрено работниками организации, имеющими доступ в помещение, где обрабатывается конфиденциальная информация.
2. Устройство перехвата информации внедрено лицами из других организаций, имевшими доступ в помещение, где обрабатывается конфиденциальная информация, в связи с выполнением договорных работ.
3. Устройство перехвата информации внедрено лицами, не являющимися работниками организации и не имеющими официального доступа в помещение, где обрабатывается конфиденциальная информация.

Во второй следственной ситуации необходимо установить способ и обстоятельства внедрения устройства перехвата информации причастных к этому лиц, объем и содержание перехваченных сведений, незаконного получателя информации, способ ее использования и размер ущерба, причиненного собственнику сведений, выявить обстоятельства, способствовавшие внедрению устройства перехвата информации.

В обеих ситуациях для организации расследования в целом допустимо применение изложенных выше программ расследования событий, связанных с похищением конфиденциальных документов. В то же время выполнение отдельных следственных действий по делам о перехвате информации, циркулирующей в технических средствах и помещениях, имеет определенную специфику. Она характеризуется спецификой предмета противоправного посягательсгва и способа совершения преступления. Обе описываемые ситуации:

Первая следственная ситуация

Сведения, составляющие коммерческую тайну, незаконно получены посторонним лицом (организацией). Обстоятельства выхода информации из законного владения неизвестны. Имеются основания полагать, что они собраны путем перехвата информации, циркулирующей в технических средствах и помещениях.

Программа действий следователя

1. Осмотр помещения, в котором обрабатывается конфиденциальная информация.
2. Осмотр технических средств и систем обработки и передачи информации.
3. Осмотр других технических средств, размещенных в помещениях, где обрабатывается конфиденциальная информация.
4. Осмотр средств вычислительной техники.
5. Осмотр типичных мест установки устройств перехвата информации и следов их использования.
6. Осмотр типичных мест обнаружения устройств перехвата информации, циркулирующей *в телефонной связи.*
7. Осмотр документов, регламентирующих организацию защиты информации.
8. Назначение экспертизы по определению конфиденциальности незаконно полученных (перехваченных) сведений.
9. Назначение экспертизы вещественных доказательств.
10. Дача отдельного поручения оперативным работникам о производстве оперативно-розыскных действий.
11. Следственный эксперимент.

Особенности и цели выполнения перечисленных выше следственных действий

1. Осмотр помещения, в котором обрабатывается конфиденциальная информация, включает в себя:

1. конструкции помещения и здания (стены, потолок, пол, окна, двери);
2. мебель и предметы интерьера.

Цели осмотра:

а) Выявление условий, создающих возможность перехвата вследствие нарушения требований инструкции по защите речевой информации, в числе которых следующие обстоятельства:

3. помещение (хранилище информации) расположено за пределами охраняемой территории либо на минимальном удалении от границ контролируемой зоны;
4. помещение имеет смежные конструкции (стены, полы, потолки) с помещениями, расположенными на неохраняемой территории;

5. окна помещения выходят на открытую для несанкционированного доступа территорию и не имеют штор (жалюзи);
6. ограждающие помещение конструкции не обеспечивают надежную звукоизоляцию и позволяют прослушивать хранилище (имеются трещины и щели);
7. помещение прослушивается через вентиляционные отверстия;
8. датчики охранной сигнализации, дверь, замки на двери и силовых щитах находятся в ненадлежащем техническом состоянии.

В процессе осмотра следует фиксировать наличие (либо отсутствие) тамбура с двойными дверьми, дополнительного слоя остекления рам в оконных проемах, уплотнительных прокладок в дверных и оконных притворах, применение надежных шумопоглотителей для вентиляционных отверстий.

б) Выявление возможности несанкционированного визуального просмотра обрабатываемых конфиденциальных материалов.

2. Осмотр технических средств и систем обработки и передачи информации включает в себя:

9. Средства вычислительной техники;
10. Средства связи и передачи данных вычислительной техники;
11. Средства телефонной связи, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, документов и другие технические средства обработки информации.

Цели осмотра:

а) Выявление внедренной «закладки», следов ее установки либо следов изъятия ранее установленной «закладки».

б) Выявление других специальных устройств, предназначенных для перехвата информации, либо следов их подключения.

3. Осмотр средств вычислительной техники (СВТ) включает в себя:

а) технические элементы системы обработки данных (терминалы, ЭВМ, узлы сети ЭВМ, каналы связи, внешние устройства ЭВМ);

б) технические элементы системы защиты информации;

в) программные элементы системы защиты информации (подсистемы управления доступом, механизмы идентификации, аутентификации, контроля доступа, управления потоками информации, подсистемы регистрации и учета, криптографической защиты, подсистемы обеспечения целостности);

г) защищаемые ресурсы, находящиеся в средствах вычислительной техники (программы; тома, каталоги, файлы, записи, поля записей; все виды памяти ЭВМ, в которых может находиться информация);

д) организационно-распорядительная и текущая документация подразделения защиты информации с отражением данных о смене паролей, ключей, об изменениях в составе лиц, допущенных к конфиденциальной информации, о регистрации и анализе действий пользователей по системному журналу.

Цели осмотра предполагают:

а) выявление встроенных электронных технических средств (либо следов их применения), позволивших осуществить несанкционированный доступ к информации;

б) обнаружение следов повреждений технических элементов системы защиты информации, позволяющих осуществить несанкционированный доступ к защищаемым сведениям;

в) обнаружение следов повреждений программных элементов системы защиты информации, позволяющих осуществить несанкционированный доступ к защищаемой информации;

г) выявление зарегистрированных системными и программными средствами СВТ сведений о наличии запрещенных связей между субъектами и объектами доступа, незаконном доступе к информационным ресурсам ЭВМ (дата и время, субъект, запрос на доступ, объект и тип доступа, исполнение запроса на доступ);

д) выяснение способа (вида) несанкционированного доступа:

12. доступ получен к файлам, программам, томам (информационным ресурсам), к которым субъект не допущен...
13. субъект вышел за пределы типов разрешенного ему доступа (читать, редактировать, писать, копировать) к конкретному документу или программе...
14. субъект не имеет права доступа к информации, содержащейся в СВТ...
15. субъект получил доступ к информационным ресурсам с использованием системных средств (паролей, ключей, принадлежащих другому пользователю)...
16. субъект получил доступ к информационным ресурсам с использованием собственных программ работы с устройствами...
17. субъект перенес конфиденциальную информацию на информационный носитель с открытым доступом.

е) Обнаружение следов копирования, повреждения либо изъятия документов (информации), находящихся в СВТ.

ж) Выявление обстоятельств, способствовавших незаконному собиранию сведе-

ний путем перехвата информации, находящейся в технических средствах и помещении. В том числе нарушений:

18. правил организации технической защиты охраняемой зоны помещения, линий и систем, обеспечивающих функционирование находящихся в нем технических средств;
19. порядка эксплуатации систем обработки и передачи конфиденциальной информации;
20. порядка ведения служебной информации системы защиты информации (генерацию и смену паролей, ключей, сопровождение правил разграничения доступа);
21. порядка оперативного контроля за функционированием системы защиты информации;
22. порядка регистрации и анализа действий пользователей;
23. порядка учета, хранения и выдачи пользователям носителей конфиденциальной информации, учтенной бумаги для распечаток, паролей и ключей;
24. порядка допуска в помещения, в которых производится автоматизированная обработка конфиденциальной информации.

4. Осмотр других технических средств, размещенных в помещениях, где обрабатывается конфиденциальная информация, включает в себя:

25. телефонные средства и системы;
26. средства радиосвязи;
27. средства охранной и пожарной сигнализации;
28. средства оповещения и сигнализации;
29. контрольно-измерительная аппаратура;
30. средства и системы кондиционирования;
31. средства проводной радиотрансляционной сети;
32. средства электронной оргтехники;
33. электрические часы.

Цели осмотра:

а) Выявление внедренной «закладки», следов ее установки либо следов изъятия ранее установленной «закладки».

б) Выявление других специальных устройств, предназначенных для перехвата информации, либо следов их подключения.

в) Выявление обстоятельств, способствовавших незаконному собиранию сведений путем перехвата информации:

v. Осмотр документов, регламентирующих организацию защиты информации, предполагает исследование:

а) паспорта защищаемого помещения, в котором отражаются: состав технических и программных средств вычислительной техники, планы размещения основных и вспомогательных технических средств; состав и схемы размещения средств защиты информации; перечень и план размещения оборудования и мебели (с указанием типа, учетного или инвентарного номера и даты установки и замены);

б) плана охраняемой зоны организации;

в) схемы прокладки линий передачи данных;

г) схемы и характеристики систем электропитания и заземления объекта информатизации.

Цели осмотра:

а) Проверка состояния работ и выполнения организационно- технических требований по защите информации.

б) Выявление в охраняемом помещении технических средств и систем, не прошедших сертификацию и специальную проверку на наличие возможно внедренных электронных устройств перехвата информации.

в) Обнаружение не зафиксированного в паспорте помещения факта замены либо перестановки технических средств и предметов мебели (признаков вероятного внедрения «закладки» либо применения иного способа перехвата информации).

г) Выявление обстоятельств, способствовавших незаконному собиранию сведений путем перехвата информации, находящейся в технических средствах и помещении. В том числе нарушений:

34. правил организации технической защиты охраняемой зоны помещения, линий и систем, обеспечивающих функционирование находящихся в нем технических средств;
35. порядка эксплуатации систем обработки и передачи конфиденциальной информации;
36. порядка ведения служебной информации системы защиты информации (генерацию и смену паролей, ключей, сопровождение правил разграничения доступа);
37. порядка оперативного контроля за функционированием системы защиты информации;
38. порядка регистрации и анализа действий пользователей;
39. порядка учета, хранения и выдачи пользователям носителей конфиденциальной информации, учтенной бумаги для распечаток, паролей и ключей;
40. порядка допуска в помещения, в которых производится автоматизированная обработка конфиденциальной информации.

vi. Назначение экспертизы по определению конфиденциальности незаконно полученных (перехваченных) сведений.

vii. Назначение экспертизы вещественных доказательств.

viii. Осмотр типичных мест обнаружения устройств перехвата информации и следов их использования включает в себя:

41. основные технические средства, расположенные в помещении;
42. вспомогательные технические средства, расположенные в помещении;
43. ограждающие конструкции защищаемого помещения (стены, полы, потолки);
44. окна, пожарные лестницы, водосточные труб, пристройки;
45. системы отопления, вентиляции, кондиционирования;
46. мебель и другие предметы интерьера;
47. линии и арматура систем связи, электропитания, освещения и сигнализации.

ix. осмотр типичных мест обнаружения устройств перехвата информации, циркулирующей в телефонной связи, предполагает исследование следующих объектов:

48. кабельные колодцы;
49. распределительные шкафы (коробки, ниши), кроссы, боксы;
50. пульты и стативы коммутаторов;
51. телефонные аппараты;
52. телефонные розетки.

10. Дача отдельного поручения оперативным работникам о производстве оперативно-розыскных действий;

11. Следственный эксперимент выполняется в следующих целях:

а) проверка выдвинутой версии о возможности (или невозможности) перехвата сведений, циркулирующих в конкретных технических средствах и помещении, с использованием известных специалистам способов и устройств;

б) проверка показаний обвиняемого, свидетеля или данных источника оперативно-розыскной информации об имевшем место перехвате сведений в конкретных условиях с использованием конкретного способа и устройства;

в) проверка параметров и возможностей «закладки» или иного технического устройства, программы ЭВМ, внедренных не установленным лицом, с целью незаконного перехвата конфиденциальной информации и выявленных в процессе следственных действий;

г) выявление причин и условий, способствовавших перехвату информации.

Вторая следственная ситуация

В технических средствах или помещениях обнаружено электронное устройство перехвата информации, внедренное при невыясненных обстоятельствах.

Программа действий следователя в значительной мере повторяет программу разрешения первой ситуации, однако имеет при этом следующие специфические особенности:

1. Осмотр электронного устройства перехвата информации («закладки»).

Осмотр производится с целью:

а) установления назначения и состояния устройства, его. пригодности для перехвата информации, способа перехвата информации и ее передачи, способа управления устройством, технических параметров устройства;

б) установления индивидуальных признаков устройства, свидетельствующих о том, по какому назначению он использовался, о связи устройства с расследуемым событием;

в) установления индивидуальных признаков устройства, свидетельствующих о принадлежности устройства конкретной организации или лицу (маркировка, способ изготовления, применение характерных деталей);

г) выявления следов, указывающих на связь устройства с конкретным лицом (следы пальцев рук, потожировые отложения, краска и другие вещества, имеющие сходство с обнаруженными на теле и одежде лица либо в его жилище).

a. Осмотр помещения, в котором обнаружено устройство перехвата информации.
b. Осмотр основных и вспомогательных технических средств, расположенных в помещении.

Указанные выше осмотры производятся с целью выявления других аналогичных устройств, следов их установки и изъятия, а также следов лиц, причастных к указанным действиям. При проведении этих следственных действий особое внимание обращается на типичные места обнаружения устройств перехвата информации и следов их использования, описанные в первой ситуации.

c. Следственный эксперимент.

Цель эксперимента: проверка выдвинутой версии о возможности (или невозможности) перехвата сведений, циркулирующих в конкретных технических средствах и помещении, с использованием обнаруженного устройства.

d. Назначение экспертизы устройства перехвата информации;
e. Дача отдельного поручение оперативным работникам о производстве оперативно-розыскных действий.

В условиях повышения значимости информации, имеющей действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам (коммерческой тайны), а также роста числа преступных посягательств, появления современных способов совершения и маскировки преступлений возрастает актуальность применения мер криминалистического обеспечении защиты коммерческой тайны.

Главным направлением совершенствования расследования в данном случае является оказание интеллектуальной поддержки следователю путем предоставления ему типовых информационных моделей, содержащих научно обоснованное описание процессов совершения преступлений и детального описания процедуры их расследования.

Использование информационных моделей и типовых программ действий следователя позволяет легче понять реальные обстоятельства исходной ситуации расследования, осознать его цели, осуществлять целенаправленный поиск и распознание, систематизацию и оценку значимой для расследования информации.

Библиография:

1. Криминалистика: учебник. Юридическая фирма «Контракт». — М., 2012. — 512 с.
2. Криминалистические и организационные особенности расследования преступлений «по горячим следам» // Lex Russica. №5, сентябрь 2012. Научные труды МГЮА имени О.Е. Кутафина. — С. 1095–1106.
3. «Особенности методики расследования коррупционных преступлений». Федеральное государственное казенное образовательное учреждение дополнительного профессионального образования «Институт повышения квалификации следственного комитета Российской Федерации»: сборник научных статей.
4. Противодействие преступлениям коррупционной направленности: актуальные проблемы и пути их решения, 2012. — С. 102, 120.

References (transliteration):

1. Uchebnik «Kriminalistika», yuridicheskaya firma «Kontrakt» — M., 2012.
2. «Kriminalisticheskie i organizatsionnye osobennosti rassledovaniya prestupleniy «po goryachim sledam»». Lex Russica №5, sentyabr' 2012. Nauchnye trudy MGYuA imeni O.E. Kutafina. — S. 1095–1106.
3. «Osobennosti metodiki rassledovaniya korruptsionnykh prestupleniy». Federal'noe gosudarstvennoe kazennoe obrazovatel'noe uchrezhdenie dopolnitel'nogo professional'nogo obrazovaniya «Institut povysheniya kvalifikatsii sledstvennogo komiteta Rossiyskoy Federatsii». Sbornik nauchnykh statey.
4. Protivodeystvie prestupleniyam korruptsionnoy napravlennosti: aktual'nye problemy i puti ikh resheniya». 2012. — S. 102, 120.

Материал получен редакцией 31 января 2013 г.