Костомаров Кирилл Валерьевич
Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков
12.00.09 – уголовный процесс, криминалистика; оперативно-розыскная деятельность
юридические науки
Д 212.298.12
ФГБОУ ВПО «Южно-Уральский государственный университете» (НИУ)
454080, г. Челябинск, ул. Коммуны, 149
Тел.: (351) 267-92-30
E-mail: darsvet@mail.ru
Предполагаемая дата защиты диссертации - 26 апреля 2012 г.

На правах рукописи

КОСТОМАРОВ КИРИЛЛ ВАЛЕРЬЕВИЧ

ПЕРВОНАЧАЛЬНЫЙ ЭТАП РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ДОСТУПОМ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ БАНКОВ

Специальность

12.00.09 – уголовный процесс, криминалистика;

оперативно-розыскная деятельность

Автореферат

диссертации на соискание ученой степени

кандидата юридических наук

Челябинск – 2012

Диссертация выполнена на кафедре уголовно-правовых дисциплин Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Уральский институт – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации»

Научный руководитель: доктор юридических наук, профессор, заслуженный юрист РФ

Карагодин Валерий Николаевич

Официальные оппоненты:

Драпкин Леонид Яковлевич
доктор юридических наук, заслуженный деятель науки РФ, профессор кафедры криминалистики Уральской государственной юридической академии;

Арсентьева Светлана Степановна
кандидат юридических наук, доцент кафедры прокурорского надзора и организации правоохранительной деятельности Челябинского государственного университета

Ведущая организация:

ФГБОУ ВПО «Алтайский государственный университет», г. Барнаул

Защита диссертации состоится 26 апреля 2012 г. в 10-00 на заседании диссертационного совета Д 212.298.12 при ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет) по адресу: 454080, г. Челябинск, ул. Коммуны, 149, ауд. 208.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет) по адресу: 454080, г. Челябинск, пр. Ленина, д. 87, корп. 3/д.

Автореферат разослан __ марта 2012 г.

Ученый секретарь диссертационного совета
доктор юридических наук, доцент Даровских Светлана Михайловна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования в значительной степени определяется распространенностью и качеством расследования компьютерных преступлений, связанных с незаконным доступом к компьютерной информации банков. К сожалению, обобщенные статистические данные о количестве подобных преступлений, совершаемых в России, отсутствуют. В 2011 году в нашей стране совершено 2698 компьютерных преступлений. В то же время в некоторых исследованиях отмечается, что в 2010 году объем средств, похищенных с помощью компьютерных технологий из банков России, стран СНГ и Балтии, составлял 1,3 млрд долларов, а в 2013 году составит до 7,5 млрд долларов.

По сведениям департамента казначейства США по борьбе с финансовыми преступлениями (FinCEN), во всем мире наблюдаются высокие темпы роста киберпреступности в банковской сфере. Так, только в 2010 году количество этого вида посягательств увеличилось на 115 %.

Негативная динамика этого вида преступности объясняется стремительным распространением средств вычислительной техники и современных компьютерных технологий не только в различных отраслях, но и в быту. Банковские учреждения наиболее восприимчивы к различного рода инновациям, позволяющим привлекать клиентов и сокращать расходы, наращивая тем самым собственные прибыли. Поэтому компьютерные технологии и средства используются в настоящее время практически во всех банковских учреждениях мира.

Поскольку в банках концентрируются значительные материальные ценности, они во все времена привлекали внимание представителей преступности. Внедрение современных информационных технологий не только не останавливает, но и стимулирует интерес субъектов посягательств. Возможности оперирования компьютерной информацией без вступления в

непосредственный физический контакт с управомоченными сотрудниками банка, по мнению субъектов посягательств, представляет большие возможности для безнаказанной реализации преступных замыслов.

Компьютерные преступления вообще и совершаемые в сфере банковской деятельности в частности характеризуются высокой степенью латентности. По различным оценкам экспертов, до 90 % такого рода преступлений остаются невыявленными.

В процессе расследования таких преступлений нередко возникают трудности, которые не всегда успешно преодолеваются следователями.

Основные проблемы возникают именно на первоначальном этапе расследования, в процессе которого формируется основная доказательственная база, зачастую определяющая эффективность всего производства по уголовному делу. Такое положение в известной степени обусловлено отсутствием научных исследований и методик расследования преступлений рассматриваемого вида. Все это и обусловило выбор темы настоящего диссертационного исследования.

Степень научной разработанности темы. Исследования преступлений в сфере компьютерной информации были начаты в России в 90-х гг. XX века на основе анализа зарубежных источников (Ю. М. Батурин, В. Б. Вехов, Б. Х. Толеубекова). В дальнейшем исследования продолжили В. В. Крылов, В. А. Мещеряков и другие ученые уже с учетом изменений отечественного уголовного закона. Среди зарубежных исследований необходимо выделить пособие по борьбе с компьютерными преступлениями Д. Айкова, К. Сейгера и У. Фонсторха, «Руководство по реагированию на внешнее вторжение» К. Мандиа и К. Просиса, «Технику компьютерных преступлений» Л. Джеймса.

Тактика проведения отдельных следственных действий по уголовным делам о незаконном доступе к компьютерной информации освещалась в работах А. Д. Волеводза, В. Д. Курушина, В. А. Минаева, Е. И. Панфиловой, Е. Р. Россинской, К. С. Скоромникова, Н. Т. Шурухнова, а также в

диссертационных исследованиях Ю. В. Гаврилина, О. Г. Григорьева, А. В. Касаткина, Т. Э. Кукарниковой, А. В. Остроушко, В. Ю. Рогозина, Л. Н. Соловьева, А. И. Усова, В. П. Хомколова, Г. М. Шаповаловой и др.

Исследования всех вышеперечисленных авторов посвящены общим проблемам расследования компьютерных преступлений. Вопросы же выявления и расследования компьютерных преступлений именно в сфере деятельности банков до настоящего времени изучению на монографическом уровне не подвергались.

При проведении настоящего диссертационного исследования были выявлены особенности элементов криминалистической характеристики данного вида преступлений, с учетом которых были предложены соответствующие практические рекомендации по выявлению и расследованию такого рода посягательств.

Целью исследования являются выявление проблем первоначального этапа расследования преступлений, связанных с незаконным доступом к компьютерной информации банков, и разработка практических рекомендаций по их преодолению и повышению его эффективности.

Для достижения поставленной цели поставлены следующие задачи:

1) на основе обобщения данных судебно-следственной практики уточнить содержание криминалистической характеристики преступлений, связанных с незаконным доступом к компьютерной информации банков;

2) выделить типичные ситуации, формирующиеся на этапе доследственной проверки сообщений о преступлениях данного вида и подготовить предложения об основных путях их разрешения;

3) с учетом результатов исследования и систематизации судебно-следственной практики подготовить рекомендации по выдвижению следственных версий и разрешению ситуаций первоначального этапа расследования данного вида преступления;

4) выявить основные сложности, возникающие при проведении отдельных следственных действий, определить пути и средства их

преодоления;

5) подготовить научно обоснованные предложения и методические рекомендации по оптимизации первоначального этапа расследования преступлений, связанных с незаконным доступом к компьютерной информации банков.

Объектом исследования являются преступная деятельность, связанная с незаконным доступом к компьютерной информации банков, а также деятельность правоохранительных органов по раскрытию, расследованию данного вида преступлений.

Предметом исследования являются объективные закономерности возникновения информации о незаконном доступе к компьютерной информации банков, субъектах данного доступа, а также деятельности по выявлению и расследованию данной категории преступлений.

Границы объекта и предмета исследования ограничены рамками досудебного производства в стадии возбуждения уголовного дела и на первоначальном этапе предварительного расследования, поскольку именно в этот период формируется основная доказательственная база, обеспечивается возможность выполнения целей и задач производства по уголовному делу.

Первоначальный этап расследования понимается как производство от возбуждения уголовного дела до сбора доказательств, достаточных для предъявления обвинения или принятия решения о прекращении уголовного дела без предъявления обвинения.

Методологическую основу исследования составляют диалектический подход к анализу социально-правовых процессов и явлений. При его проведении использованы принципы системного, сравнительного и комплексного анализа проблем, а также системно-структурный, логический, статистический, контент-анализ, наблюдение, измерение, описание, сравнение и другие методы исследования.

Теоретической базой работы послужили труды Т. В. Аверьяновой, О. Я. Баева, Л. В. Бертовского, Ю. М. Батурина, А. А. Белякова, Р. С. Белкина,

В. Б. Вехова, С. И. Винокурова, И. А. Возгрина, А. Г. Волеводза, Т. С. Волчецкой, В. К. Гавло, Ю. В. Гаврилина, И. Ф. Герасимова, В. Н. Григорьева, Г. А. Густова, Л. Я. Драпкина, Г. Г. Зуйкова, Е. П. Ищенко, В. Н. Карагодина, В. Я. Колдина, В. В. Крылова, В. А. Мещерякова, В. А. Образцова, В. Ю. Рогозина, Е. Р. Россинской, Н. А. Селиванова, Л. Н. Соловьева, В. Г. Танасевича, Д. А. Турчина, А. И. Усова, Г. М. Шаповаловой, Н. Г. Шурухнова, Н. П. Яблокова и других ученых.

Использовались труды таких зарубежных ученых по вопросам расследования компьютерных преступлений, как Д. Айков, Ю.-П. Граф, Л. Джеймс, Д. Крег, К. Мандиа, К. Просис, К. Сейгер, У. Фонсторх и др.

Эмпирическая база исследования. При проведении диссертационного исследования были изучены 105 уголовных дел о преступлениях, связанных с незаконным доступом к компьютерной информации банков, рассмотренных судами г. Москвы (21 уголовное дело), Свердловской (53 уголовных дела) и Нижегородской (31 уголовных дела) областей, а также 47 материалов об отказе в возбуждении уголовного дела.

Кроме того изучалась опубликованная практика федеральных судов Российской Федерации и ряда иностранных государств.

Было проведено анкетирование 86 следователей и сотрудников органов, осуществляющих оперативно-розыскную деятельность, имеющих опыт расследования преступлений, связанных с незаконным доступом к компьютерной информации, а также 26 сотрудников отделов информационной безопасности различных банков.

Научная новизна диссертационного исследования определяется его целями, задачами, объектом и предметом.

В работе на основе изучения судебно-следственной практики уточнена криминалистическая характеристика незаконного доступа к компьютерной информации банков. В частности выявлена и описана специфика обстановки, типичных свойств личности субъекта преступления и особенности способов совершения.

В диссертации анализируются типичные ситуации, формирующиеся при поступлении сообщений о совершении данного вида преступлений, предлагаются пути и средства их разрешения.

Особое внимание при этом уделяется изученным в теории проблемам выдвижения и проверки версий о личности субъекта и обстоятельствах преступлений рассматриваемых категорий, проведения качественного осмотра места происшествия. В ранее опубликованных работах содержались в основном рекомендации по исследованию средств компьютерной техники, каналов и конфигураций их соединений. В диссертации даны рекомендации по осмотру таких мест происшествия, как служебные и жилые помещения, в которых расположены компьютеры, использовавшиеся для незаконного доступа; территории, на которых производилось задержание с поличным; помещения банков, где дислоцированы средства хранения и использования компьютерной информации, подвергшиеся посягательству.

В диссертации подробно исследуются тактические аспекты задержания с поличным, ранее не затрагивавшиеся в работах, посвященных расследованию компьютерных преступлений.

На основе ситуационного подхода в диссертации сформулированы предложения по оптимизации планирования первоначального этапа расследования преступлений рассматриваемого вида, поиска субъектов причастных к его совершению и проверки обоснованности возникшего подозрения.

С учетом специфики механизма следообразования данного вида преступлений соискателем установлено значение судебных экспертиз для достижения названных задач. При этом соискатель не ограничивается, как другие авторы, рассмотрением возможностей только компьютерно-технической экспертизы. В диссертации содержится предложение о производстве иных видов экспертиз, в том числе бухгалтерских, с целью установления содержания, времени и процедуры выполнения субъектами преступления банковских операций.

Анализируя деятельность по проверке обоснованности подозрения, диссертант не сводит ее только к допросу подозреваемых, а предлагает рекомендации по получению и установлению достоверности показаний названных лиц, предположительно причастных к совершению преступлений.

Результатом исследования обозначенных проблем являются следующие основные положения, которые выносятся на защиту:

1. Суждения о том, что содержание криминалистической характеристики незаконного доступа к компьютерной информации банков специфично и отличается от аналогичных характеристик других видов компьютерных преступлений.

2. Авторская трактовка структуры обстановки незаконного доступа к компьютерной информации банков, в которой доминирующее значение имеют не пространственно-временные элементы, а сложившийся порядок, режим, средства и технологии накопления, хранения и использования компьютерной информации банков.

3. Выводы о специфических корреляционных связях между свойствами личности субъектов преступления и применяемыми ими способами незаконного доступа к компьютерной информации банков. Среди лиц, совершающих преступления рассматриваемого вида, выделяются следующие субъекты: внутренние (сотрудники банка) и внешние, реализующие соответственно непосредственные или удаленные (опосредованные) способы незаконного доступа к компьютерной информации.

Внешние субъекты вынуждено осуществляют достаточно сложные подготовительные мероприятия по подготовке к совершению незаконного доступа к компьютерной информации банков, что нередко требует от них достаточно глубоких специальных познаний.

Внутренние субъекты находятся в более благоприятных условиях, имеют возможности использования служебных ЭВМ, данных о правилах и процедурах доступа к компьютерной информации банков, что существенно

упрощает содержание избираемых ими способов совершения преступлений рассматриваемого вида.

4. Классификация типичных исходных ситуаций, возникающих на этапе доследственной проверки сообщений о незаконном доступе к компьютерной информации банка, и предложения по их разрешению. Выделяются прежде всего сложные проблемные ситуации, характеризующиеся дефицитом информации о личности субъекта, реализовавшего непосредственный, удаленный или комбинированный способы незаконного доступа к компьютерной информации. Соответственно этому предлагаются пути выявления внутренних или внешних субъектов посягательств.

5. Предложения о проведении операций по задержанию с поличным внешних и внутренних субъектов преступлений рассматриваемого вида.

6. Разработаны практические рекомендации по планированию первоначального этапа расследования с учетом типичных ситуаций, характеризующихся различными информационными, психологическими и управленческими факторами. Предлагаются различные направления, средства и методы расследования в зависимости от того, выявлены или не установлены субъекты посягательства, применявшиеся ими удаленные, непосредственные, комбинированные способы незаконного доступа.

7. Обобщенные рекомендации по использованию возможностей различных судебных экспертиз для решения задач первоначального этапа расследования.

8. Типичные алгоритмы проверки обоснованности подозрения в причастности к незаконному доступу к компьютерной информации банка. Демонстрируется, что содержание, последовательность и тактика оперативно-розыскных мероприятий и следственных действий, проводимых в этих целях, обуславливается объемом, качеством и источником информации, послужившей основанием для подозрения, а также позицией подозреваемого.

Анализируются возможные варианты преодоления противодействия подозреваемых из числа внешних и внутренних субъектов, исполнявших разные роли при совершении преступлений исследуемого вида.

Теоретическая и практическая значимость исследования определяется актуальностью рассмотренных проблем, решением важных научно-практических и теоретических аспектов расследования преступлений исследуемой категории. Результаты исследования, теоретические положения и практические рекомендации могут быть использованы в следственной и оперативно-розыскной деятельности, при обучении студентов юридических вузов, для повышения квалификации следователей и в последующих научных изысканиях по данной проблематике.

Апробация результатов исследования. Результаты диссертационного исследования отражены в материалах Международной научно-практической конференции «Актуальные проблемы уголовного процесса и криминалистики России и стран СНГ» (Челябинск, 2009).

По теме диссертационного исследования опубликовано шесть научных статей, две из них – в изданиях, рекомендованных ВАК Минобрнауки России. Одна статья опубликована в международном криминалистическом журнале «International Journal of Criminal Investigation». Положения и выводы проведенного исследования использовались на юридическом факультете Уральской академии государственной службы при чтении курса «Криминалистика».

Объем и структура работы. Диссертация состоит из введения, трех глав, заключения, списка использованной литературы и приложения. Объем работы – 212 страниц.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность избранной темы исследования, определяются цели, задачи и методология исследования, раскрываются его теоретическая и практическая значимость, научная новизна

исследования, формулируются основные положения, выносимые на защиту.

Первая глава «Криминалистическая характеристика преступлений, связанных с незаконным доступом к компьютерной информации банков» состоит из трех параграфов.

В первом параграфе «Содержание криминалистической характеристики преступлений, связанных с незаконным доступом к компьютерной информации банков» рассматривается понятие этой научной категории, определяется ее структура.

Анализ элементов криминалистической характеристики преступления данного вида начинается с анализа предмета посягательства – компьютерной информации банков.

Компьютерная информация банков может быть классифицирована по содержанию на сведения: о вкладчиках и клиентах банка; о финансовом состоянии и операциях банка; о сотрудниках банка; о программных средствах, используемых для производства финансовых операций, а также для хранения, обработки и использования других банковских данных.

В зависимости от объема компьютерной информации, подвергшейся посягательству, могут быть выделены преступления, направленные на всю хранящуюся, используемую банковским учреждением информацию или только на часть таких данных.

Важным элементом криминалистической характеристики преступлений, связанных с незаконным доступом к компьютерной информации банков, являются сведения об обстановке совершения таких деяний. Доминирующее положение в ней занимают не пространственно-временные элементы, а информационная обстановка. Ее содержание и структура отличаются от аналогичных условий учреждений, осуществляющих иные виды деятельности.

Компонентом обстановки данного вида преступлений является сложившийся порядок хранения, обработки, использования и защиты компьютерной информации банков. Кроме этого, в нее включаются

программные и технические средства, обработки, использования и защиты информации.

Информационная обстановка банковского учреждения в значительной степени характеризуется его структурой. Внутреннее взаимодействие банка и информации обусловлено наличием либо отсутствием сети филиалов, а также единых информационных центров. Наличие разветвленной сети подразумевает активное обращение информации между филиалами и головной организацией. Такого рода удаленное взаимодействие компьютерной информации требует соответствующего увеличения качества средств защиты. Так, в 8 % изученных нами уголовных дел преступления были совершены в отношении информации банков, имеющих представительства и филиалы. При этом 36 % таких преступлений были направлены на информацию представительств и филиалов.

Место совершения преступлений рассматриваемой категории также характеризуется определенной спецификой. Например, часть таких посягательств совершается сотрудниками банка во время выполнения ими служебных полномочий, когда они находятся на рабочих местах. Такие преступления составили 32 % от общего числа изученных уголовных дел.

В то же время в 68 % изученных уголовных дел преступления совершались субъектами, находившимися за пределами банковских учреждений. В большинстве случаев субъекты использовали жилые помещения, в которых они проживали. В 93 % изученных нами уголовных дел преступления были совершены в областных центрах, 7 % - в малых городах и поселках. Такое положение, на наш взгляд, обусловлено превосходящими темпами информатизации и компьютеризации крупных городов по сравнению с периферией.

Время совершения преступлений анализируемого вида также отличается определенной спецификой. Оно представляет собой временной отрезок разной продолжительности. Достаточно сказать, что по 34 % изученных уголовных дел установить точно дату, часы совершения

преступлений не представилось возможным. В этих случаях в процессуальных документах указывался приблизительный промежуток времени, в который совершалось расследуемое деяние. Около 20 % всех изученных нами преступлений были совершены в рабочее время (с 10 до 18 часов). Однако сотрудники банков, использовавшие непосредственный доступ к компьютерной информации, совершали 96 % такого рода преступлений именно в указанное время.

Во втором параграфе «Свойства личности субъектов преступлений, связанных с незаконным доступом к компьютерной информации банков» рассматриваются взаимосвязь и влияние таких элементов криминалистической характеристики личности, как возраст, пол, образование, участие в группе или единоличный характер преступной деятельности, судимость.

Возраст субъектов посягательств колеблется в широких границах от 15 до 45 лет. В момент совершения преступления возраст 23 % субъектов не превышал 20 лет, 13 % - были старше 40 лет и 64 % - в возрасте 20-40 лет. При изучении уголовных дел были выявлены различия в возрасте субъектов, применявших способы удаленного или непосредственного доступа к компьютерной информации банков. Около 63 % субъектов первой из названных групп на момент совершения преступления находились в возрасте до 25 лет. Это можно объяснить тем, что становление личности к этому моменту еще не завершилось, сильно желание самоутвердиться, а удаленность от места происшествия и абстрактное восприятие жертвы психологически облегчают совершение подобных посягательств.

При обобщении уголовных дел было установлено, что субъекты рассматриваемого вида преступления обладают достаточно высоким уровнем образования: 74 % имели высшее либо неполное высшее образование (36 % и 38 % соответственно).

Около 9 % субъектов ранее привлекались к уголовной ответственности, в том числе 7 % - за совершение неправомерного доступа к компьютерной

информации, что фактически свидетельствует об отсутствии криминального прошлого у большинства лиц, совершающих рассматриваемый вид преступления.

В научно-методической литературе предлагаются классификации субъектов компьютерных преступлений по различным основаниям. Однако большинство из них носят чисто теоретический характер, поскольку не могут быть использованы в практической деятельности органов расследования. В связи с этим в диссертации предлагается классификация субъектов преступлений, связанных с незаконным доступом к компьютерной информации банков, на внешних и внутренних, являющихся сотрудниками банковского учреждения.

Внутренние субъекты изученных нами преступлений занимали различное служебное положение: в обслуживании работали 35 % из них, на руководящих должностях – 23 %, в профильных подразделениях – 19 % и в технических службах – 23 %. В столь же широком диапазоне колеблется возраст внутренних преступников: от 18 до 59 лет. Одиноких людей больше, чем семейных (54 % против 31 %). Свыше 80 % внутренних субъектов совершали преступления из корыстных побуждений. При этом лишь 27 % преступников испытывали материальные трудности. Внутренние субъекты имеют более широкие возможности доступа к компьютерной информации банков по сравнению с внешними субъектами, не работающими в банковских учреждениях.

Внутренние субъекты изученных нами преступлений не обладали глубокими знаниями компьютерных технологий, при совершении преступления использовали умения, присущие рядовому пользователю.

Внешние субъекты, не работающие в банке, - это чаще всего мужчины (порядка 98 %), обычно в возрасте до 25 лет.

В 23 % изученных уголовных дел преступления рассматриваемого вида совершались группами. Из них 12 % посягательств было совершено группами, состоящими только из сотрудников банка, 62 % - смешанными

группами, состоящими из сотрудников банка и посторонних лиц, 26 % - только из числа посторонних лиц.

В третьем параграфе «Способы совершения преступлений, связанных с незаконным доступом к компьютерной информации банков» рассматриваются особенности подготовки, совершения и сокрытия преступлений рассматриваемого вида.

Способ совершения преступления понимается как система действий по подготовке, совершению и сокрытию преступления, детерминированная условиями внешней среды и психофизическими качествами личности, связанными с избирательным использованием соответствующих средств и условий места и его времени.

Основным элементом способа совершения компьютерного преступления является незаконный доступ к компьютерной информации, получение возможности знакомиться и осуществлять неправомерные операции с данными, находящимися в информационной системе в ЭВМ и на машинных носителях.

Следует отметить, что незаконный доступ к компьютерной информации банка сам по себе нередко является элементом преступной деятельности, включающей в себя деяния, охватываемые составами нескольких (чаще всего корыстных) преступлений.

В теории криминалистики и следственной практике выделяются способы непосредственного и опосредованного (доступа) к компьютерной информации. Они отличаются по объему, содержанию подготовки, операций по совершению и сокрытию преступлений рассматриваемого вида.

Под способом опосредованным (удаленным) понимается незаконный доступ к компьютерной информации банка, совершенный с помощью средств вычислительной техники, находящихся вне банковского учреждения. При расследовании 68 % изученных нами уголовных дел было установлено, что незаконный доступ к банковской информации осуществлялся опосредованно субъектом, удаленным от места хранения желаемых сведений.

Для осуществления удаленного доступа к компьютерной информации выполняются удаленное подключение с использованием неисправности в системе защиты банка; проникновение посредством подбора паролей (программный или интеллектуальный подбор); подключение к телекоммуникационному оборудованию; использование незаконно полученных авторизационных данных, необходимых для доступа к компьютерной информации банков; хищение аппаратных средств (вплоть до банкоматов) для изучения механизма защиты; вовлечение в преступную деятельность сотрудников банка; внедрение в банк соучастника.

Применение способов непосредственного доступа к компьютерной информации банков было доказано при расследовании 32 % изученных нами уголовных дел. Главной отличительно особенностью этой группы способов является то, что проникновение в систему осуществляется без удаленного присоединения к компьютерной сети банка, а непосредственно к рабочей станции банковского учреждения.

При изучении уголовных дел было установлено, что данные способы применялись только внутренними субъектами преступления.

В 81 % изученных случаев внутренние субъекты преступления заранее планировали свои действия. В содержание 35 % изученных способов включались подготовительные действия по изучению структуры базы данных; поиску конкретной ЭВМ, где располагался необходимый объем информации; выявлению слабых мест в защите информационной системы, позволяющих получить доступ к ней.

При реализации почти одной трети таких способов (31 %) субъекты пытались организовать общий пароль; создать необязательную общую запись авторизации; получить авторизованный доступ к информации за пределами своей ответственности; обойти средства защиты; получить пароли административного уровня; копировать информацию с домашнего компьютера в систему учреждения; использовать помощь бывших сотрудников и т.п.

В большинстве случаев субъекты названных посягательств включали сокрытие в способ преступления. Содержание операций по сокрытию существенно различается в зависимости от того, осуществляется ли опосредованный или непосредственный доступ к компьютерной информации банков.

Сотрудники банков, скрывая готовящееся или совершаемое ими преступление, прежде всего стремятся избрать такое место и время, которые исключают появление людей, способных помешать реализации преступного замысла. Внешние субъекты в основном используют специальные программы и операции по сокрытию, одновременно или последовательно позволяющие получать доступ к информации банка и скрывать совершаемое преступление.

Вторая глава «Проверка заявлений и сообщений о преступлениях, связанных с незаконным доступом к компьютерной информации банков» состоит из трех параграфов.

В первом параграфе «Типичные исходные ситуации и основные направления их разрешения» на основании обобщения уголовных дел выделены типичные условия, формирующиеся в стадии возбуждения уголовного дела.

В сложных проблемных ситуациях дефицита информации об обстоятельствах и субъектах предполагаемого посягательства основным направлением проверки является установление действий по незаконному доступу к компьютерной информации банка и дислокации ЭВМ, с помощью которой они совершались. Для этого производится опрос заявителей и других лиц, наблюдавших признаки и операции по незаконному доступу, проводятся специальные компьютерно-технические исследования, дается поручение уполномоченным органам о проведении оперативно-розыскных мероприятий.

Содержание проверочных мероприятий существенно различается в зависимости от того, располагают ли органы расследования сведениями о реализации непосредственного или удаленного доступа к компьютерной

информации банков.

В ситуациях, когда имеющиеся данные не позволяют сделать однозначного вывода о способе доступа, необходимо проверять версии о применении в ходе посягательства как удаленного, так и непосредственного доступа.

При обнаружении признаков непосредственного доступа принимаются меры к установлению рабочего места извлечения информации и зоны входа в информационную систему. В этих целях проводятся специальные компьютерно-технические исследования; оперативно-розыскные мероприятия; осмотры мест происшествия, изучение документов и материалов видеонаблюдения, технической регистрации, в которых фиксируются все операции и перемещения сотрудников банков, опросы заявителей и свидетелей.

В условиях наличия сведений о реализации удаленного способа неправомерного доступа также актуальна задача установления компьютера, использовавшегося для совершения преступления. Для его обнаружения требуется проверка всех элементов компьютерной системы, в которых могли отразиться информационные следы (ЭВМ банка, провайдер, промежуточные узлы связи). Целесообразно обращение к данным учета ранее судимых по способу преступления. Существенную помощь могут оказать и аналогичные сведения из криминалистического учета нераскрытых преступлений.

Параллельно следует проводить проверочные мероприятия в банковском учреждении, в котором обналичивались денежные средства, переведенные посредством незаконного использования информационной системы. В месте получения денежных средств опрашиваются лица, выдававшие денежные средства. У них подробно выясняются обстоятельства выдачи и признаки внешности получателя. В ходе опроса рекомендуется использование изображений выясняемых признаков. По возможности составляется композиционный портрет субъекта.

Осуществляется проверка лиц, на имя которых открывались счета, и

документов, которые предоставлялись для получения денежных средств. Нередко для этого используются похищенные, случайно найденные или позаимствованные паспорта. В этих случаях проверяются обстоятельства и очевидцы утраты названного документа.

Некоторые субъекты посягательств рассматриваемого вида пытаются реализовать полученные сведения через сеть Интернет. Иногда они сообщают об успешном использовании определенных приемов и способов незаконного доступа в сети, обсуждают их с другими лицами, занимающимися подобной деятельностью. Поэтому целесообразно изучение сайтов, блогов, файлов в сети Интернет, на которых могут располагаться подобные сведения.

В ситуациях, характеризующихся наличием информации, дающей основания полагать, что посягательство совершалось внутренним субъектом синхронно с действиями внешнего, целесообразна проверка всех соединений аппаратов мобильной связи, находившихся в банковском учреждении. Такие операции дают положительный эффект, например, в случаях, когда после электронного перевода денежных средств на другой счет они сразу же обналичиваются.

В данном разделе диссертации рассматриваются также ситуации, характеризующиеся наличием данных о субъектах посягательства, и даются рекомендации по проверке их причастности к предполагаемому преступлению.

Во втором параграфе «Тактико-организационные особенности осмотра места происшествия» даются рекомендации по проведению этого следственного действия. В данном разделе отмечаются, что осмотру обязательно подлежат помещения банковского учреждения.

Отличительной особенностью корпоративных компьютерных банковских сетей является то, что их построение осуществляется, как правило, на протяжении нескольких лет. В такого рода сетях наличествует оборудование разных производителей, в том числе и из разных поколений технологий. Поэтому следует заблаговременно получить сведения о

средствах вычислительной техники в структуре информационной сети банка, технических способах их объединения, особенностях функционирования. Рекомендуется изучать планы помещений, подлежащих осмотру, с нанесенными на них схемами электроснабжения и элементов компьютерных сетей банков. С учетом этих сведений намечается последовательность осмотра помещений банка и расположенных в них объектах.

В ситуациях, характеризующихся наличием информации о помещении банка, в котором дислоцируется ЭВМ, использовавшаяся для незаконного доступа, осмотр целесообразно начинать с исследования этой территории. Далее исследуются те элементы информационной системы, в которых могут быть обнаружены другие следы незаконного доступа – линии проводной связи, коммутаторы, серверы, документы, отражающие выполнение операций с использованием компьютерной техники и т.п.

В условиях отсутствия информации о конкретном месте, откуда осуществлялся непосредственный доступ, рекомендуется сплошной осмотр помещений банка и всех находящихся в них элементов компьютерной сети. При подготовке к осмотру выясняется, какой установлен порядок, режим работы в помещениях, намеченных для осмотра и т.д.

Представляется, что количество привлекаемых к осмотру лиц зависит от условий реальной следственной ситуации, площадей и числа объектов, подлежащих исследованию, сложности и объема запланированных операций. В случае проведения осмотра больших площадей с большим количеством объектов число привлекаемых специалистов увеличивается.

Определенными особенностями характеризуется осмотр локальных вычислительных сетей ЭВМ (ЛВС). Они могут занимать значительные площади и состоять из нескольких сотен узлов, что необходимо учитывать при подготовке и проведении осмотра.

При подготовке к осмотру мест незаконного удаленного доступа также необходимо получить сведения об условиях обстановки, подлежащей обследованию. Эти действия чаще всего совершаются в жилых помещениях,

в которых проживают субъекты посягательства. Осмотр необходимо проводить во время, когда предполагаемый субъект находится в подлежащем обследованию помещении. Поэтому важно изучить распорядок дня указанных лиц. Иногда целесообразно установление наблюдения за ними.

Следует отметить, что в большинстве изученных случаев подобные осмотры проводились в ситуациях, когда такие субъекты уже были осведомлены о возникших в отношении них подозрениях. Они задерживались при попытках получения денежных средств в банке, после электронного перевода их со счетов владельцев либо при реализации информации, добытой из компьютерных сетей и баз данных банка. В таких случаях время на подготовку к проведению осмотра места происшествия очень ограниченно.

В структуре осматриваемого жилого помещения могут быть выделены два основных узла. Первый представляет собой стол, на котором расположена ЭВМ, и прилегающая к нему территория. Кроме компьютера и его соединений рекомендуется осматривать документы, носители электронной информации. Необходимо обращать внимание на любые бумажные носители с текстами, исполненные с помощью печатных устройств или от руки. Среди них могут быть записи паролей, кодов, программ, использовавшихся для осуществления незаконного доступа, данные вкладчиков, распечатки данных, полученных в результате совершения преступлений. Особое внимание следует уделять банковским документам: уведомлениям об открытии счета, выпискам из него, квитанциям на получение денежных средств.

В качестве другого узлового элемента подобных мест происшествия могут быть названы участки хранения специальной учебно-методической и справочной литературы по вопросам компьютерного программирования.

В третьем параграфе «Задержание с поличным субъектов преступлений, связанных с незаконным доступом к компьютерной информации банков» рассматриваются возможности проведения этого действия в форме тактической операции.

В диссертации предлагаются конкретные рекомендации по проведению описываемых тактических операций по задержанию внутренних субъектов в служебных помещениях и внешних – по месту жительства, во время выполнения ими действий по незаконному доступу к компьютерной информации или непосредственно после этого.

В структуру этих тактических операций включаются оперативно-розыскные действия по установлению наблюдения за названными лицами, а также за местами предполагаемого продолжения преступной деятельности, по установлению контроля за использованием определенных средств компьютерной техники и фиксации выполняющихся действий, захвату названных субъектов операций. Возможно также проведение следственных действий – осмотр места происшествия, освидетельствование задержанного.

Субъекты таких посягательств могут задерживаться во время выполнения операций по неправомерному доступу к компьютерной информации банков; получения денежных средств, похищенных с использованием незаконного доступа к компьютерной информации; реализации данных, извлеченных в результате незаконного доступа; непосредственно после окончания операций, образующих объективную сторону преступлений рассматриваемого вида.

Проведение анализируемой операции возможно при обнаружении неудачных попыток непосредственного или удаленного доступа или неудавшихся попыток перевода денежных средств, извлечения информации, ставшей предметом посягательства, или признаков неоконченных, неожиданно прекращенных действий. Информация о таких фактах поступает, как правило, из учреждений банка. По данным фактам производится подробный опрос сотрудников технических подразделений и служб безопасности банка, выявивших признаки преступления.

В диссертации предлагаются рекомендации по задержанию субъекта преступления в момент получения наличных денежных средств, незаконно переводимых с помощью компьютерных технологий со счетов клиентов

банка на специально созданные счета.

Выделяются варианты проведения подобных операций в условиях ситуаций, характеризующихся наличием сведений: а) о предполагаемом месте получения денежных средств неустановленным субъектом; б) о намерении конкретного субъекта получить деньги в банковском учреждении.

В стадии возбуждения уголовного дела могут проводиться операции по задержанию с поличным субъектов, реализующих данные, полученные в результате неправомерного доступа к компьютерной информации. В этих ситуациях проводится такое оперативно-розыскное мероприятие, как проверочная закупка.

На этапе подготовки проверочной закупки необходимо получить и зафиксировать выраженное желание, инициативу субъекта реализовать добытые преступным путем сведения, чтобы избежать обвинений в подстрекательстве к совершению преступных действий. Непосредственный захват продавца осуществляется после передачи носителей указанных данных и получения за них денег.

Все материалы подготовки и проведения этого оперативно-розыскного мероприятия должны представляться в соответствии с правилами, установленными инструкцией о порядке предоставления результатов оперативно-розыскной деятельности дознавателю, следователю, прокурору и в суд.

Третья глава «Особенности первоначального этапа расследования преступлений, связанных с незаконным доступом к компьютерной информации банков» состоит из трех параграфов.

В первом параграфе «Планирование первоначального этапа расследования» предлагаются практические рекомендации по осуществлению этой деятельности с учетом условий типичных следственных ситуаций.

Ситуации первоначального этапа расследования в 67 % изученных нами уголовных дел являлись сложными, проблемными, характеризовались

существенной неполнотой информации о способе и субъектах совершения преступления.

В подобных ситуациях деятельность следователя осуществляется в тех же направлениях, что и в аналогичных условиях, формирующихся в стадии возбуждения уголовного дела. Однако в ходе расследования для проверки выдвинутых версий проводятся не только организационно-проверочные и оперативно-розыскные мероприятия, но и следственные действия. В работе предлагаются рекомендации по проверке версий о совершении выявленного преступления непосредственным или удаленным способами, внутренними или внешними субъектами.

Анализируются также особенности планирования и проведения в рассматриваемых ситуациях отдельных следственных действий: допросов различных категорий свидетелей, выемок и осмотров предметов, документов, проведения специальных исследований компьютерной техники и информационных сетей банков.

В тупиковых следственных ситуациях, когда проверка выдвинутых версий не дает желаемого результата, предлагается проанализировать всю проделанную работу. В этих условиях рекомендуется «мозговой штурм», осуществляемый в процессе обсуждения сложившейся ситуации следователем совместно с сотрудниками оперативно-розыскных органов, специалистами и экспертами. Все данные оцениваются с позиций полноты выдвинутых версий.

Для полноты и объективности оценки информационного компонента ситуации рекомендуется составлять письменную таблицу, в одних графах которой предлагается выделять содержание и источник имевшихся сведений, а в других – выводы об обстоятельствах и субъектах неправомерного доступа, которые можно было сделать на основе указанных данных. В отдельной графе целесообразно указывать краткое изложение механизма построения указанных выводов.

На основе обобщения и анализа полученных материалов, практики

расследования в аналогичных ситуациях, тактических и методических рекомендаций по разрешению подобных ситуаций составляется новый план расследования. В нем может быть предусмотрено проведение дополнительных или повторных мероприятий по проверке ранее выдвигавшихся версий, а также по отработке новых предложений об обстоятельствах и субъектах расследуемого события.

Типичным результатом разрешения проблемных ситуаций является получение данных, позволяющих привлечь конкретных субъектов в качестве подозреваемых в совершении преступлений рассматриваемого вида. Основной задачей расследования в подобных ситуациях является доказывание умысла подозреваемого, его действительных намерений.

В этом разделе также сформулированы предложения по планированию расследования, осуществляемого после выявления подозреваемых.

Во втором параграфе «Особенности назначения и производства судебных экспертиз» рассматриваются проблемы проведения на первоначальном этапе расследования названных процессуальных действий.

Основной экспертизой, назначаемой по уголовным делам рассматриваемой категории, является судебная компьютерно-техническая (далее – СКТЭ). Эти экспертизы назначались при расследовании 60 % изученных уголовных дел. Объектами экспертного исследования при этом являлись средства компьютерной техники, при помощи которых осуществлялся незаконный доступ, - в 74 % случаев; средства компьютерной техники, к которым был совершен незаконный доступ, - в 31 % случаев; аппаратные средства, программное обеспечение, информационные следы - в 15 % случаев.

В работе рассматриваются возможности проведения различных видов исследований при проведении СКТЭ. По большинству изученных уголовных дел проводились информационно-компьютерные исследования. В то же время для выявления места расположения ЭВМ, с помощью которой осуществлялся удаленный доступ, требуется проведение компьютерно-

сетевых исследований. При расследовании почти половины (47 %) изученных автором уголовных дел при производстве СКТЭ решались диагностические задачи становления вида и характера изменений, внесенных в информационные системы банков в результате совершения преступлений.

В работе рассматриваются особенности подготовки и назначения СКТЭ для решения различных задач.

По уголовным делам анализируемой категории нередко возникает необходимость назначения и проведения судебно-бухгалтерских экспертиз. При проведении этих экспертиз устанавливается, какие банковские и кассовые операции совершались подозреваемыми, как они отразились в бухгалтерской документации, какой материальный ущерб был причинен преступными действиями и т.д. В распоряжение эксперта кроме обычной документации необходимо предоставлять заключения СКТЭ об операциях, проводившихся с использованием незаконного доступа к компьютерной информации банков.

В наиболее сложных ситуациях рекомендуется проведение комплексной судебно-бухгалтерской и компьютерно-технической экспертизы.

В работе рассматриваются возможности назначения и производства названных и иных экспертных исследований для решения задач первоначального этапа расследования преступлений указанного вида.

В третьем параграфе «Проверка обоснованности подозрения в совершении преступления, связанного с незаконным доступом к компьютерной информации банков» указывается, что содержание этой деятельности не ограничивается только допросом подозреваемых. Она включает в свое содержание проведение оперативно-розыскных мероприятий и следственных действий по установлению относимости, допустимости, достоверности и достаточности доказательств причастности подозреваемого к расследуемому преступлению.

В ходе этой деятельности исследуются не только уже имеющиеся, но и собираются новые доказательства. В результате проверки могут быть

получены доказательства достаточные для прекращения уголовного дела в отношении подозреваемого, предъявления ему обвинения в совершении расследуемого преступления.

Проверка обоснованности подозрения начинается еще при подготовке к допросу подозреваемого. На этой стадии рекомендуется как можно более полно оценить сложившуюся ситуацию и разработать прогноз возможного поведения подозреваемого на допросе. Для этого проводятся отбор и систематизация материалов уголовного дела, содержащих сведения о причастности подозреваемого к преступлению. Следует подобрать и систематизировать данные, не только подтверждающие подозрение, но и те, которые могут быть использованы подозреваемым для аргументации своей защиты.

При прогнозировании поведения подозреваемого на допросе следует учитывать и свойства его личности, в том числе отразившиеся в способе совершения инкриминируемого деяния. Так, если подозреваемый прибегал к сложным операциям по сокрытию совершенного (совершаемого) деяния, можно предполагать, что он продолжит свою деятельность и в ходе допроса.

С учетом содержания указанных сведений избираются приемы допроса подозреваемых. В основном в ходе допроса подозреваемых используются приемы предъявления доказательственной информации.

Наиболее сложные ситуации складываются к моменту первоначального допроса подозреваемых, установленных спустя продолжительное время после совершения ими преступления, связанного с незаконным доступом к компьютерной информации банков. При расследовании 23 % изученных нами уголовных дел такие подозреваемые первоначально полностью отрицали свою причастность к расследуемому преступлению.

В работе предлагаются различные рекомендации по опровержению ложных показаний об этих обстоятельствах в зависимости от того, исходят ли они от подозреваемых из числа внешних или внутренних субъектов преступления.

Некоторые подозреваемые не отрицают выполнение действий по незаконному доступу к компьютерной информации банков, но скрывают истинные цели и мотивы содеянного. Противодействие таких подозреваемых преодолевается путем предъявления им доказательств неправомерного доступа к компьютерной информации банков, тщательной подготовки этой деятельности, перевода, получения денежных средств со счетов банка, извлечения и реализации незаконно полученной банковской информации.

В данном разделе диссертации исследуются проблемы проверки показаний подозреваемых, задержанных с поличным. С учетом типичных доводов таких подозреваемых даются рекомендации по проверке их показаний.

В этом же параграфе рассматриваются особенности проверки показаний при установлении и задержании группы подозреваемых.

При выборе и реализации приемов предъявления доказательственной информации рекомендуется учитывать свойства личности допрашиваемых. Так, при допросе подозреваемых упрямых по характеру, не склонных к даче объективных показаний, рекомендуется предъявлять с нарастающей силой совокупность фактических данных.

Подозреваемым, испытывающим неуверенность в занимаемой позиции, могут предъявляться единичные доказательства, наиболее сильные и значимые с точки зрения допрашиваемого.

Приемы предъявления доказательственной информации различным категориям допрашиваемых могут варьироваться в ходе одного или нескольких допросов.

В завершающей части параграфа содержатся предложения о проверке показаний подозреваемых, не отрицающих свою причастность к преступлению.

В заключении диссертации сформулированы основные выводы, предложения и рекомендации для их реализации в дальнейшей научной и практической деятельности.

В приложении приведена анкета по изучению уголовных дел.

Основные положения диссертационного исследования изложены в следующих научных изданиях:

Публикация в ведущем рецензируемом журнале или издании по перечню, определенному Высшей аттестационной комиссией Минобрнауки России:

1. Костомаров К. В. Типичные ситуации, формирующиеся к моменту получения первичной информации о преступлениях, связанных с незаконным доступом к компьютерной информации банков // Проблемы права. – 2010. – № 4. – С. 166-171.

2. Костомаров К. В. Проверка обоснованности подозрения в совершении преступления, связанного с незаконным доступом к компьютерной информации банков // Проблемы права. – 2012. – № 1. – С. 224-230.

Публикации в иных научных изданиях:

3. Костомаров К. В. Некоторые проблемы судебной компьютерно-технической экспертизы // Материалы Международной научно-практической конференции «Актуальные проблемы уголовного процесса и криминалистики России и стран СНГ», посвященной 80-летию со дня рождения профессора, доктора юридических наук, заслуженного деятеля высшей школы Ю. Д. Лившица. – Челябинск, 2009. – С. 310-313.

4. Костомаров К. В. Некоторые особенности выявления сетевых компьютерных преступлений // Инновации и право: материалы региональной межвузовской научно-практической конференции студентов и аспирантов. – М., 2010. – С. 31-35.

5. Костомаров К. В. Классификация субъектов преступлений, связанных с незаконным доступом к компьютерной информации // Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях: материалы Международной научно-практической конференции. – Тюмень, 2010. – С. 139-141.

6. Kostomarov K. V. Fixation of traces and organization of interaction

with an expert in investigation of illegal access to computer information of a bank // International Journal of Criminal Investigation, Volume 1, Issue 4. SAV & AIT Laboratories, 2011. – P. 187-194.