РАССЛЕДОВАНИЕ ХИЩЕНИЙ, СОВЕРШАЕМЫХ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ДОСТУПА

Кандидат юрид. наук **В.Г. Баяхчев**

В.В. Улейчик

Хищения, совершаемые в кредитно-финансовой сфере с использованием электронных средств доступа, в зависимости от способа, можно разделить на две большие группы:

- хищения с использованием пластиковых карт;

- хищения, сопряженные с неправомерным доступом в компьютерные сети.

Количество зарегистрированных в России преступлений подобного рода еще невелико. По имеющимся данным, в 1997 г., в стране зарегистрировано не более 10 хищений, сопряженных с несанкционированным проникновением в компьютерные сети банков и иных кредитно-финансовых учреждений и 131 факт хищения с использованием пластиковых карт. Однако если сравнивать эти показатели с предшествующими годами, прослеживается явная тенденция их роста.

Кроме того, зарубежный опыт свидетельствует, что подобные преступления приносят наибольший ущерб. Например, по данным ФБР США "среднестатистический" ущерб от одного такого преступления составляет 650 тыс. долларов США, в то время как аналогичный показатель ущерба от ограбления банка - только 9 тыс. долларов.

Практика расследования данной категории преступлений идет по пути их квалификации как мошенничества, что не может вызывать сколько-нибудь серьезных возражений. Поскольку конкретные проблемы квалификации мошенничества нашли достаточно широкое и подробное освещение в литературе, в настоящих методических рекомендациях основное внимание будет уделено наиболее важным аспектам тактики и методики расследования данного

вида преступлений.

1. Хищения с использованием пластиковых карт.

1.1. Общая характеристика платежных систем карточных расчетов.

Незаконное завладение имуществом с помощью пластиковых карт является сравнительно новым для России способом хищения в силу того, что сами пластиковые карты и их инфраструктура появились у нас совсем недавно. В настоящее время на территории России функционируют несколько платежных систем карточных расчетов (VISA, MasterCard, AMERICAN EXPRESS и др.). Каждая из них представляет собой объединение:

- банков-эмитентов, выпускающих платежные карточки;

- торговых и сервисных предприятий, заключивших договор с банком-эмитентом о приеме карт к оплате и открывших в данном банке свой расчетный счет;

- расчетных (процессинговых) центров, обеспечивающих ведение счетов клиентов и осуществляющих связь между банком-эмитентом и пунктом приема платежей по карточкам. (Каждая платежная система может включать несколько расчетных центров равноправных или соподчиненных).

Клиент (владелец или держатель карточки) может пользоваться ею только в тех торговых и сервисных предприятиях, которые включены в данную конкретную платежную систему. Важной составляющей процедуры оплаты с помощью карточки является ее авторизация (проверка платежеспособности), которая, в зависимости от типа карты, производится в одном из двух режимов.

При авторизации магнитной карточки устанавливается связь платежного терминала, установленного в торговом или сервисном предприятии, с расчетным центром, где и проверяется наличие средств на карт-счете.

При авторизации смарт-карты (имеющей встроенный процессор) процедура авторизации происходит непосредственно в пункте платежа, путем считывания терминалом заложенной в карте информации.

Если карта не внесена в список карт, платежи по которым запрещены, платеж можно производить. Для этого карта прокатывается через импринтер, который выдает чек на покупку (слип) с отпечатанными реквизитами карты и

клише предприятия. Далее кассир указывает дату, сумму покупки и подписывает слип. После того как картодержатель (клиент) проверил правильность заполнения слипа (чека), он в соответствующей графе расписывается. Кассир должен проверить, чтобы подпись в слипе соответствовала подписи в кредитной карте, а в случае, если сумма покупки превышает лимитную сумму, то истребовать у клиента документ удостоверяющий личность. Лимитная сумма по карте составляет, как правило, 150 долларов США.

Далее одна часть слипа (верхняя) отдается клиенту, вторая - прилагается к кассовой отчетности (в бухгалтерию пункта платежа), третья - в кредитную компанию. При получении слипа, компания производит его оплату за счет собственных оборотных средств и перечисляет ее на счет предприятия, в котором клиент расплачивался кредитной картой.

Следует отметить, что карточки бывают дебетовые и кредитные. С помощью первой можно делать покупки лишь в пределах заранее внесенной суммы. Кредитные карточки позволяют осуществлять платежи на суммы, превышающие остаток на счете. Во втором случае картодержателю один раз в месяц выставляется счет по всем его платежам, который он должен оплатить в течение 20 дней.

1.2. Основные способы совершения хищений с использованием пластиковых карт.

В самом общем виде можно выделить два способа совершения хищений с использованием пластиковых карт:

- использование подлинных карт;

- использование поддельных карт.

В свою очередь, внутри данных способов имеются определенные разновидности в значительной степени влияющие на предмет доказывания по уголовному делу.

Подлинные карты могут быть использованы для хищения в следующих случаях:

- использование найденной или украденной карты для оплаты товаров или услуг, либо для получения наличных денег в банкоматах (использование смарт-карты затруднено, поскольку преступнику необходимо знать индиви-

дуальный PIN-код, известный только владельцу карты);

- получение в кредитном учреждении пластиковой карточки по подложным документам с последующим невозвращением перерасходованных средств.

Теоретически возможно совершение хищения с помощью кредитной карты, полученной преступником по своим настоящим документам с целью не возвращения предоставленного кредита. Однако данный способ на практике не встречается, поскольку платежная система гарантировано обеспечивает установление перерасхода, который в последующем будет взыскан с клиента.

Указанные способы удобны для преступников тем, что им не надо устанавливать идентификационные данные карты (номер, имя владельца). Вместе с тем, для получения кредитной карты в банке необходим первоначальный капитал. Кроме того, возникает необходимость изготовления подложных или поддельных документов, отработки подписи лиц, на чье имя она открыта. Поэтому данные обстоятельства включаются в предмет доказывания по уголовному делу.

Следует отметить, что хищение преступниками самой пластиковой карты и подделка документов (с целью последующего хищения денежных средств) в определенных случаях должны квалифицироваться как приготовление к совершению мошенничества.

Изготовление и использование поддельных кредитных либо расчетных карт также сопряжено с изготовлением поддельных или подложных документов. Кроме того, перед преступниками дополнительно возникают две проблемы:

- получение идентификационных данных подлинных держателей карт;

- обеспечение безопасности авторизации карт.

Наличие этих проблем, а также достаточная дороговизна процедуры качественного изготовления поддельной карты, обуславливает совершение таких преступлений организованными группами. Соответственно значительно расширяется и предмет доказывания по уголовному делу.

Идентификационные данные карт преступники получают, как правило, через своих сообщников в торговых и сервисных предприятиях, кредитных

учреждениях. Например, по одному из уголовных дел было установлено, что все настоящие владельцы карт (иностранцы), идентификационные данные которых использовались преступниками, посещали в Москве ресторан "Арагви".

Следующим способом получения идентификационных данных карты, который однако не нашел отражения ни в одном из изученных уголовных дел, может заключаться либо в простом подсматривании при производстве расчетов в пунктах платежа, либо в получении информации из выброшенных клиентами своих экземпляров чеков.

В последнее время, в связи с развитием в России глобальных компьютерных сетей, появилась возможность получения идентификационных данных карт при помощи несанкционированного внедрения в указанные сети (например, через Интернет). В этом случае действия виновного должны квалифицироваться по совокупности ст.159 УК РФ и 272 УК РФ.

Для исключения опасности быть разоблаченными при авторизации карты, преступники могут осуществлять платежи через своих знакомых в торговых и сервисных предприятиях.

Другой способ, более сложный, заключается в создании по подложным документам лжепредприятия и вступление на договорной основе в платежную систему. Процесс авторизации поддельных карт в этом случае значительно облегчается. Перечисленные на счет лжепредприятия с этих карт денежные средства в последующем по платежному поручению перечисляются на счета других предприятий, также созданных по подложным документам, а затем изымаются.

В данном случае в действиях виновных лиц содержатся признаки не только мошенничества, но и лжепредпринимательства (ст.173 УК РФ).

Основной целью проведения преступниками операций с расчетными картами является завладение денежными средствами. Однако напрямую достичь этой цели возможно только при снятии денег в банкоматах (что затруднительно по указанным выше причинам). Во всех других случаях преступники вначале незаконно приобретают дорогостоящие товары (как правило бытовую технику), а потом реализуют их.

Для скорейшего достижения поставленной цели иногда используется

способ обналичивания денежных средств, содержащихся на карте. Суть данного способа заключается в следующем. Через своих сообщников в торговых и сервисных предприятиях либо просто знакомых, работающих в этих предприятиях кассирами, часть наличной выручки изымается из кассы, а образовавшаяся недостача проплачивается по карте.

Если в деле имеются доказательства того, что названные лица знали о противозаконном использовании карты, они должны быть привлечены к ответственности за соучастие в преступлении.

С недавнего времени появился новый способ мошенничества, заключающийся в оплате товаров через компьютерную сеть с помощью сообщения продавцу идентификационных данных чужих кредитных карт.

Для преступников данный способ привлекателен тем, что авторизация карточки состоит лишь в проверке ее кредитоспособности и не требует идентификации личности клиента.

Вместе с тем у фирмы, оказывающей подобные услуги, остается информация о паспортных данных клиента и месте его жительства.

Кроме того, товар вручается клиенту нарочным, который в последующем может опознать преступника.

1.3. Возбуждение уголовного дела и первоначальные следственные действия.

Особенностью возбуждения и расследования данной категории дел является то, что преступники задерживаются, как правило, в момент осуществления платежа по пластиковой карте. Такое задержание может быть как случайным, так и результатом проведения оперативной разработки. В любом случае необходимо изъять:

- карту, по которой производился платеж;

- слипы с указанием оплаченной суммы и подписью лица осуществлявшего платеж;

- слипы, свидетельствующие об использовании карты ранее;

- находящиеся при задержанном документы, удостоверяющие личность.

После возбуждения уголовного дела задержанного следует допросить

по следующим вопросам:

- каковы его подлинные анкетные данные;

- каким образом, когда, где, у кого и с какой целью он приобрел данную карту;

- как часто он ее использовал, где именно, на какие суммы осуществлял платежи;

- если приобретал товары, то какие именно, как ими распорядился, где они в данный момент находятся;

- осуществлял ли обналичивание денежных средств с помощью карты, если да, то где, каким образом и кто ему в этом помогал;

- кто еще входит в состав группы, совершавшей хищения, кто был инициатором ее создания, каким образом распределялись роли, как делился доход;

- у кого, когда, где, при каких обстоятельствах приобрел подложные либо поддельные документы, удостоверяющие личность;

- с какой целью открыл текущий счет в банке и приобрел карту по подложным или поддельным документам;

- каким образом и где была изготовлена поддельная карта, где находится оборудование для ее изготовления;

- каким образом были получены идентификационные данные для изготовления поддельной карты.

После проведения допросов всех лиц подозреваемых в совершении преступления, необходимо немедленно произвести обыски по месту их проживания. В результате обыска могут быть изъяты:

- похищенное имущество;

- слипы, свидетельствующие о ранее совершенных хищениях;

- другие поддельные карты;

- поддельные и подложные документы;

- образцы подписей с подражанием подписи владельца карты;

- оборудование для изготовления поддельных карт;

- записные книжки, черновые записи, свидетельствующие о круге знакомств задержанного.

Для закрепления всех обстоятельств задержания лица с поличным не-

обходимо допросить:

- сотрудников торгового или сервисного предприятия (как правило, это кассир или продавец) обнаруживших неплатежеспособность карты. Данным лицам должны быть заданы вопросы: что послужило причиной не допуска карты для осуществления платежа (не прошла авторизацию, внешний вид карты вызвал подозрения, подпись предъявителя карты не соответствовала подписи на карте, у предъявителя карты не оказалось документов, удостоверяющих личность), какая сумма подлежала оплате, изымалась ли карта, где она в настоящее время находится;

- сотрудников милиции или службы безопасности предприятия, осуществивших непосредственное задержание лица: по конкретным обстоятельствам задержания. Кроме того, следует выяснить, не было ли у задержанного сообщников.

1.4. Задачи дальнейшего расследования.

Задачи и ход дальнейшего расследования определяются кругом обстоятельств, подлежащих доказыванию, в самом общем виде они определены в ст.68 УПК РСФСР. Применительно к рассматриваемым преступлениям, данные обстоятельства могут быть конкретизированы и дополнены.

Общие задачи дальнейшего расследования.

Одной из важнейших задач дальнейшего расследования, характерной для расследования всех уголовных дел данной категории, является установление всех эпизодов преступной деятельности обвиняемых.

Обладая информацией, какие именно кредитные карты ими использовались для совершения хищений, следует направить запрос в расчетный центр, обслуживающий данную платежную систему, где можно получить сведения о всех фактах использования данной кредитной карты с указанием пункта платежа.

После этого в указанных предприятиях необходимо изъять подлинники слипов, на которых указаны дата платежа, уплаченная сумма, реквизиты карты, подпись плательщика. Все слипы должны быть направлены на почерковедческую экспертизу для определения лица, подписавшегося за клиента.

Кроме того, с помощью указанных слипов можно установить кассира,

принявшего платеж, который должен быть допрошен для выяснения возможности опознания им преступника.

В последующем необходимо произвести опознания кассирами преступников.

Поскольку в слипах пробита стоимость каждой покупки, есть возможность определить, какие именно товары были приобретены, что поможет в их последующем поиске и расширении доказательственной базы.

В связи с тем, что большинство функционирующих в России платежных систем оперирует средствами в иностранной валюте, для установления размера причиненного ущерба необходимо направить запрос в Центральный Банк РФ с просьбой сообщить курс той или иной валюты по отношению к рублю на день проведения платежа.

Важным вопросом, требующим специального выяснения при расследовании рассматриваемых преступлений, является установление потерпевшего по делу.

В соответствии с Гражданским кодексом банк, получая денежные средства клиента, становится их собственником, а у вкладчика появляется на эти средства право требования. Следовательно, ущерб причиняется банку.

Получение в кредитном учреждении пластиковой карточки по подложным документам с последующим невозвращением перерасходованных средств.

В этих случаях преступники используют обычно утерянные или похищенные паспорта, в которых переклеивают фотографию.

В связи с этим необходимо назначить технико-криминалистическую экспертизу паспорта, использованного для открытия счета с целью установления внесенных в него изменений.

Изъять в кредитном учреждении, выдавшем карточку, заявление об открытии лицевого счета, текущего валютного вклада, документа о получении личной карточки.

Установить и допросить истинного владельца паспорта по вопросам:

- при каких обстоятельствах и когда был утрачен паспорт;

- обращался ли в милицию по этому поводу;

- знакомы ли ему лица, проходящие по делу;

- им ли выполнены подписи в заявлении об открытии лицевого счета, текущего валютного вклада, документе о получении личной карточки. Допросить сотрудников кредитного учреждения (операциониста), открывавших счет и выдававших личную карту об обстоятельствах происшедшего, могут ли они опознать и по каким признакам лицо, открывшее счет.

Провести опознание сотрудниками кредитного учреждения виновного лица.

Использование найденной или украденной карты для оплаты товаров или услуг, либо для получения наличных денег в банкоматах.

Этот способ является наиболее примитивным и его успех во многом зависит от того, насколько быстро виновное лицо осуществит задуманное, поскольку в случае своевременного обращения владельца карты в кредитную организацию на нее выставляется стоп-лист.

В данном случае необходимо:

- допросить истинного владельца карты по обстоятельствам ее утраты, заявлял ли он об этом в кредитное учреждение и как быстро;

- допросить сотрудников кредитного учреждения и расчетного центра по вопросам: обращался ли к ним с заявлением об утрате карты ее истинный владелец, выставлялся ли стоп-лист и если нет, то почему;

- изъять видеозаписи в случае хищения из банкомата (местонахождение банкомата в обязательном порядке контролируется видеоаппаратурой) и назначить по ним портретную экспертизу.

Хищение с использованием поддельных кредитных либо расчетных карт.

В случае изъятия поддельной карты необходимо назначить технико-криминалистическую экспертизу, на разрешение которой поставить вопросы: изготовлена ли представленная на исследование карта (указать ее идентификационные данные) предприятиями данной платежной системы (указать какой именно); если нет, то каким способом и с применением каких материалов она выполнена; изготовлена ли данная пластиковая карта на оборудовании,

изъятом у подозреваемого. Одновременно эксперту должны быть представлены образцы подлинных карт, которые можно изъять у предприятия-изготовителя.

Далее следует установить и допросить истинного владельца карты по вопросам:

- какой картой он пользуется и как давно;

- кто еще мог пользоваться данной картой;

- не замечал ли, что кто-то пользуется его счетом и сохраняла ли карта авторизацию, обращался ли он по этому вопросу в банк-эмитент;

- пользовался ли он услугами торговых и сервисных предприятий, через которые осуществлялись платежи по его карте;

- его ли подпись стоит в слипах, изъятых в данных предприятиях.

Поскольку преступники стараются использовать идентификационные данные карт иностранных владельцев, проведение данного следственного действия может быть затруднено. В этом случае имеет смыл воспользоваться каналами Интерпола, либо использовать возможности самих кредитных учреждений, куда следует направить запрос с просьбой установить истинных владельцев карт и получить ответы на интересующие вопросы. Приобщенный к материалам дела ответ кредитного учреждения будет отвечать признакам иного документа в смысле ст.88 УПК РСФСР и может использоваться в доказывании.

Важным обстоятельством, подлежащим доказыванию при использовании преступниками поддельных карт является способ завладения идентификационными данными карты. В этом случае работа должна вестись в двух направлениях. Во-первых, необходимо принять меры к установлению круга знакомых обвиняемого. Интересующие сведения могут содержаться в его записных книжках, черновых записях и т.п. По данному вопросу надо допросить его родственников (если они согласятся давать показания), соседей, знакомых, дать отдельное поручение органу дознания. Особое внимание следует обращать на связи в кредитных, торговых и сервисных предприятиях.

Во-вторых, следует принять меры для установления в каких именно предприятиях истинные владельцы карт использовали их. Это поможет выявить одно-два предприятия, услугами которых пользовались все картодер-

жатели и на отработке именно их сотрудников сосредоточить основное внимание.

Использование поддельных карт неразрывно связано с их изготовлением. Поэтому в процессе расследования должны быть приняты меры, направленные на обнаружение соответствующего оборудования. В случае обнаружения оборудования для изготовления пластиковых карт, оно должно быть изъято, осмотрено и приобщено к делу в качестве вещественного доказательства. В последующем имеет смысл провести следственный эксперимент для определения возможности изготовления на данном оборудовании поддельной пластиковой карты.

Создание по подложным документам лжепредприятия и заключение с банком договора на обслуживание пластиковых карт.

Данный способ является разновидностью совершения хищений с помощью поддельных карт.

В данном случае необходимо:

- изъять учредительные документы предприятия в регистрационной палате либо банке;

- изъять в банке: договор на открытие банковского счета, договор об обслуживании держателей пластиковых карт и соглашения к нему, карточки с образцами подписей руководителей предприятия, сводные чеки и слипы, представленные предприятием в банк;

- по всем указанным документам назначить почерковедческую экспертизу для установления, кем исполнены в них подписи (в графах "клиент", "кассир" и т.д.).

- допросить по обстоятельствам заключения договора на обслуживание пластиковых карт специалиста управления пластиковых карт банка;

- допросить сотрудников банка, отвечающих за анализ платежных систем, об обстоятельствах сотрудничества с интересующим лжепредприятием.

Поскольку в рассматриваемом случае поддельные кредитные карты могут быть и не обнаружены, необходимо изъять в расчетном центре все слипы по интересующим пластиковым картам. После этого необходимо назначить технико-криминалистическую экспертизу для определения соответствия от-

тисков с кредитных карт в этих слипах и оттисков с аналогичных карт в слипах, предоставленных в банк обвиняемым.

2. Расследование хищений в кредитно-финансовой сфере, совершенных с использованием компьютерной техники.

Деятельность органов внутренних дел по своевременному выявлению и раскрытию преступлений, совершаемых с использованием компьютерной техники, затрудняется высоким уровнем латентности данного вида преступлений (по оценкам специалистов до 90 %). Не являются исключением и хищения в кредитно-финансовой сфере.

Анализ отечественной и зарубежной специальной литературы, изучение уголовных дел, опросы работников оперативных служб, следователей и судей позволили выявить основные проблемы, возникающие при расследовании таких дел о хищениях.

1) сложности в установлении (в случае совершения преступления с использованием компьютерной техники) самого события преступления и правильная его квалификация;

2) значительные затруднения у следователя при проведении следственных действий по обнаружению, изъятию, фиксации и исследованию компьютерной информации;

3) отсутствие у следователей как практики расследования преступлений, совершаемых с использованием компьютерной техники, так и знаний самой техники.

Анализ выявленных преступлений, совершенных с использованием электронных средств доступа, показывает, что наиболее часто преступные посягательства направлены на локальные компьютерные сети и базы данных кредитно-финансовых учреждений.

Практика расследования хищений, совершаемых с использованием компьютерной техники, идет по пути их квалификации как мошенничества, что не может вызывать сколько-нибудь серьезных возражений. Вместе с тем, поскольку данные преступления совершаются путем неправомерного доступа к компьютерной информации, то необходима дополнительная квалификация по ст. 272 УК России, а также по ст. 327 УК, если использовались подложные документы.

Расследование хищений, совершаемых с использованием компьютерной техники, осуществляется по следующим основным направлениям:

- сбор фактов, свидетельствующих о совершении незаконных операций с использованием компьютерной техники;

- проведение мероприятий, направленных на установление причинной связи между действиями, образующими способ проведения незаконной операции, и наступившими последствиями путем детализации характера совершенных виновным действий;

- определение размера ущерба, причиненного противоправными действиями;

- сбор и фиксация фактов о причастности виновного лица к совершенным действиям и наступившим последствиям.

Каждое из этих направлений предполагает решение своих специфических задач. Однако основной спецификой расследования данной категории преступлений является необходимость уделять приоритетное внимание сбору и фиксации компьютерной информации. Именно компьютерная информация во многих случаях позволяет установить фактические обстоятельства дела, выявить круг лиц, причастных к совершению преступления, а также обнаружить следы преступления.

Учитывая особенности компьютерной информации, а именно: бездокументарная форма хранения, быстрота и легкость уничтожения, ее обезличенность (при вводе информации через компьютер), при расследовании перед следователем возникает ряд задач, без решения которых успешное раскрытие преступления будет невозможно.

Прежде всего, к работе по расследованию необходимо привлечь грамотного специалиста по компьютерным системам и многопользовательским сетям.

Особо выделяя необходимость участия специалиста в области вычислительной техники и программирования, отметим, что опрос следователей и указанных специалистов показал: только 14% следователей работают на ЭВМ на уровне пользователя и 56% не знают ничего о принципах работы ЭВМ. С другой стороны 92% из числа программистов считают, что на современном уровне развития вычислительной техники без участия профессионала найти в компьютере «спрятанную» информацию без опаски уничтожить искомые данные крайне сложно[1]. Участие соответствующего специалиста необходимо также и при производстве допросов, на которых выясняются технические аспекты совершенного преступления.

Отсутствие системного подхода к исследованию информационных следов пре-

[1] См.: Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: Автореф.дисс … канд. юрид. наук. Москва, 1997. С. 15-18.

ступления приводит к необоснованному прекращению уголовных дел или отказу в возбуждении уголовного дела, неполному возмещению материального ущерба и невозможности привлечения к ответственности всех лиц, причастных к преступлению.

Можно выделить три типичные ситуации, складывающиеся при совершении хищений с использованием компьютерной техники:

1. Владелец или пользователь компьютерной сети (базы данных) собственными силами выявил факт незаконного проникновения и иных противоправных действий, обнаружил виновное лицо и заявил об этом в правоохранительные органы.

2. Владелец или пользователь компьютерной сети (базы данных) информационной системы выявил факт незаконного проникновения и иных противоправных действий, но не смог установить виновное лицо и заявил об этом в правоохранительные органы.

3. Информация о незаконном проникновении в компьютерную сеть и иных совершенных противоправных действиях стали общеизвестны либо были установлены в ходе проведения оперативно-розыскных мероприятий.

Таким образом, первоначальной задачей следователя и оперативного работника является сбор и фиксация с помощью собственника системы факта незаконного проникновения в компьютерную сеть и совершения иных противоправных действий.

В компьютерных сетях, как правило, программное обеспечение настраивается таким образом, чтобы максимально полно протоколировать все события происходящие в системе. Протоколируется, с какого компьютера произошло соединение, а если на компьютере установлена программа идентификации, то и имя пользователя, который запросил соединение, и т.д.

Обеспечение сохранности электронных протоколов, указывающих на проникновение в сеть, является одной из задач следователя, поскольку такая информация, изъятая в ходе расследования уголовного дела с соблюдением уголовно-процессуальных требований, может служить доказательством по делу. По аналогичным соображениям необходимо обеспечить сохранность жесткого диска взломанного компьютера. Если уголовное дело возбуждено, то следователь может разрешить владельцу снять копию с жесткого диска, а сам диск направляется на экспертизу. Дальнейший анализ диска может позволить определить, что успел сделать злоумышленник, как он проник в систему и где находится компьютер, использовавшийся для проникновения в сеть.

Особое внимание необходимо обращать на способ, незаконного проникновения в локальную вычислительную сеть: подбор либо знание паролей, отключение средств защиты (в том числе извне), использование несовершенства средств защиты, использование специальных программных средств, а также на содержание и назначение информации, подвергшейся воздействию. В отдельных случаях указанная информация позволяет достаточно четко определить круг подозреваемых лиц.

В основном объектами посягательства являются денежные средства и ценные бумаги. Как правило, с целью совершения хищения указанных ценностей в систему электронных расчетов (записей) вносится подложная операция на перечисление (зачисление) денежных средств, ценных бумаг на определенный счет или счета. Затем из данного кредитно-финансового учреждения происходит перечисление денежных средств на счета в заранее подобранные банковские либо иные учреждения, позволяющие произвести обналичивание и получение денежных средств. Указанная схема является наиболее распространенной. Кроме того, известны случаи когда в расчетную программу одного из кредитно-финансовых учреждений были внесены такие изменения, что в результате проведения каждой расчетной операции, на определенный счет перечислялась незначительная сумма денег, но, учитывая объемы расчетных операций, была совершена попытка похищения значительной суммы денежных средств.

Наглядно иллюстрирует возможности хищения с использованием компьютерной техники следующий пример. Анализ базы данных одного из депозитариев, осуществлявших операции с ценными бумагами показал, что в результате воздействия на файлы баз данных сторонним программным обеспечением стало возможным создание ничем не обеспеченного количества акций, для последующего их сбыта. Примерная схема воздействия выглядит следующим образом:

1. Выбирался лицевой счет (чаще иногороднего клиента). На этот счет (назовем его накопительным) с помощью стороннего программного обеспечения производилось фиктивное списание акций с большой группы счетов для накопления их значительного количества .

2. Для обеспечения баланса системы расчетов сторонним программным обеспечением была создана фиктивная запись, никому не принадлежащая, с отрицательным количеством акций равным сумме акций всех накопительных счетов. В итоге на счете, реально содержащим иное количество акций, создавался значительный пакет акций, который с точки зрения системы расчетов имел легальный статус.

3. Владелец накопительного счета или его доверенное лицо (иногда с фиктивной доверенностью) оформляли в депозитарии "легальный" перевод со своего счета на счет другого регионального депозитария. Сотрудники депозитария оформляли перевод. Таким образом происходила легализация фиктивных акций.

4. На накопительном счете восстанавливалось истинное количество акций и уничтожались все следы воздействия сторонним программным обеспечением.

Вместе с тем, учитывая многообразие компьютерных баз данных и операционных и служебных программ, способы хищений могут быть самыми различными. Следователю прежде всего необходимо определить является ли электронная запись полностью фиктивной или в ее подтверждение имеется бумажный носитель, в последнем случае очевидно, что к хищению причастен кто-то из сотрудников кредитно-финансового учреждения.

Если хищение с использованием электронно-вычислительной техники совершаются путем проникновения в компьютерную сеть, то определенную помощь в получении первоначальных данных по вышеуказанным вопросам может оказать системный администратор указанной сети.

Далее с помощью системного администратора и службы безопасности (если она имеется) необходимо попытаться установить местонахождение компьютерной техники, которая использовалась при совершении преступления.

Учитывая конкретные обстоятельства, следователем могут быть выдвинуты следующие общие версии:

1. Хищение совершено сотрудником данного кредитно-финансового учреждения, либо лицом, входящим в круг родственников, друзей, знакомых сотрудников учреждения, иным лицом, имеющим доступ к компьютерной технике в данном учреждении.

2. Преступление совершено группой лиц с участием сотрудника данного учреждения.

3. Хищение совершено лицом или группой лиц, не связанных с деятельностью данного кредитно-финансового учреждения.

Следует отметить, что, по мнению отечественных и зарубежных специалистов на долю хищений, совершенных сотрудниками учреждения, имеющего локальную вычислительную сеть, или по сговору с ними приходится около 70 - 80 % всех хищений с незаконным использованием компьютерной информации. Как правило, подоб-

ные хищения совершаются группой, причем один из ее членов, является либо сотрудником данного учреждения, либо имеет свободный доступ к компьютерам (представитель службы технического обеспечения, постоянный контрагент и т.п.), умеет работать с вычислительной техникой, хорошо представляет, какая информация и где расположена в компьютере.

В этом случае преступника характеризуют два признака, которые существенно сужают круг подозреваемых: знание функций, паролей различных операций выполняемых тем или иным компьютером в организации и наличие доступа к компьютеру или их сети.

Особое внимание следует обратить на то, что часто хищения осуществляют не только квалифицированные специалисты, знания которых позволяют им взломать защиту большинства компьютерных систем, но и неквалифицированные служащие, имеющие возможность доступа к средствам компьютерной техники.

В этой связи большое значение приобретают допросы потерпевших и свидетелей, а также получение документов характеризующих работу как учреждения в целом, так и отдельных его сотрудников.

Исходя из этого, следователь устанавливает:

- существует ли в данном учреждении локальная сеть, какая компьютерная техника используется, каким образом организована ее работа и какие кредитно-денежные и иные финансовые операции через нее осуществляются;

- кто является системным администратором сети, как и в каком порядке им осуществляется администрирование;

- каким образом организована защита компьютерной сети от несанкционированного проникновения, сертифицированы ли программы системной защиты;

- имеются ли специальные технические средства защиты финансовой и иной конфиденциальной информации, какие протоколы используются при передаче данных и т.п.;

- имеются ли пароли защиты, как часто происходит их смена, кому и в каком объеме они известны;

- существуют ли идентификационные программы, имеются ли в рабочих программах специальные файлы протоколов, регистрирующие вхождение в систему пользователей и каково их содержание, как долго и в каком виде они хранятся;

- каков порядок доступа пользователей в компьютерную сеть;

- кто из пользователей и какими правами обладает на внесение изменений в финансовую либо иную компьютерную программу;

- каков распорядок рабочего дня пользователей компьютерной сети;

- имеют ли право и остаются ли служащие, допущенные к эксплуатации компьютерной сети после окончания рабочего дня, если да, то кто именно и с какой целью;

- существуют ли в кредитно-финансовом учреждении специальные службы по эксплуатации локальной компьютерной сети, ответственные за ее функционирование и служба безопасности, каковы их полномочия, каков состав их сотрудников, каковы их обязанности;

- как осуществляется эксплуатация, хранение, и уничтожение компьютерных распечаток (листингов) отчетного финансового дня, кто имеет к ним доступ;

- существуют ли внутриведомственные правила эксплуатации ЭВМ и их сети, каков порядок ознакомления с ними и контроля за их исполнением;

- какие сотрудники учреждения были в течение интересующего периода времени уволены и по каким мотивам;

- каков документооборот по операциям, дублирующим работу компьютерной программы на бумажных носителях, кто из сотрудников и на какой операции задействован;

- каков порядок квитовки операций, проводимых через компьютерную сеть, и операций, осуществляемых в обычном порядке (путем внесения записей в ведомости, реестры и т.п.), как часто она проводится.

Разумеется, вышеуказанный перечень не является исчерпывающим и круг вопросов, выясняемых следователем, значительно шире и определяется конкретными обстоятельствами дела. Одновременно с этим отрабатываются и вопросы, связанные с движением похищенных денежных средств, ценных бумаг и т.п., проводятся следственные и оперативно-розыскные мероприятия, направленные на установление лиц, совершивших указанные противоправные действия.

Поскольку особенности данных мероприятий неоднократно рассматривались в методической и научной литературе вкратце отметим, что изучаются счета, на которые были перечислены денежные средства, изымаются документы, послужившие основанием для их открытия, а также свидетельствующие о движении денежных средств и ценных бумаг по ним. Выявляются лица (если возможно) открывшие ука-

занные счета. Если счет в кредитно-финансовом учреждении открыт на юридическое лицо, то изымается юридическое дело, нотариально заверенная карточка с образцами подписей. При необходимости изымаются образцы подчерка, назначаются почерковедческие экспертизы, проводятся опознания и т.п.

В случае установления места, где находится компьютер, с которого было осуществлено проникновение в сеть, необходим тщательный сбор информации на предмет установления владельца компьютера или его пользователя и обеспечения возможности изъятия компьютерной информации.

Кроме сведений о лицах, имеющих доступ к данному компьютеру, по возможности надо установить, какая компьютерная техника используется, подключена ли она к источнику автономного или бесперебойного питания, где расположен щиток по отключению электроэнергии в данном помещении, имеются ли у пользователя сообщники, выставляется ли контрнаблюдение во время работы компьютера и т.д. Через узел связи, на котором зарегистрирован данный абонентский номер телефона, необходимо установить время, когда осуществляется модемная связь.

Указанная информация необходима для обеспечения успешного проведения одного из первоначальных следственных действий по уголовным делам данной категории - обыска.

С учетом собранной информации определяется тактика проведения указанного следственного действия.

1. Определяется время начала обыска и меры, обеспечивающие его внезапность и конфиденциальность. В случае наличия информации о нахождении на компьютере данных, свидетельствующих о причастности его владельца к совершению преступления, начинать обыск лучше в то время, когда возможность работы на нем сведена к минимуму.

2. Проконсультировавшись со специалистами, определить какая информация может находиться на компьютере и подготовить соответствующую технику для ее копирования. Определить возможные меры безопасности, предпринимаемые преступниками с целью уничтожения доказательств по делу.

3. Подобрать понятых, которые разбираются в компьютерной технике (основных операциях, названиях компьютерных программ и т.п.), с тем, чтобы исключить возможность оспаривания в суде правильности проведенного следственного действия и его результатов.

Специфичность и сложность манипуляций с компьютерной техникой для непосвященного человека могут нивелировать усилия следователя по закреплению обнаруженной доказательственной информации. Непонимание смысла происходящего понятым может убедить суд в признании недопустимыми собранные доказательства.

4. Исходя из квалификации и профессиональных навыков владельца компьютера, определить специалиста по компьютерной технике, который примет участие в следственном мероприятии.

По прибытии на место обыска или осмотра необходимо:

- быстро и неожиданно войти в помещение, чтобы свести к минимуму возможность уничтожения информации, находящейся на компьютере. В некоторых случаях, когда это возможно и целесообразно, непосредственно перед входом в обыскиваемое помещение следует обесточить его;

- не разрешать, кому бы то ни было из лиц, работающих на объекте обыска, или иным лицам, прикасаться к работающим компьютерам, магнитным носителям, включать и выключать компьютеры, при необходимости удалить персонал в другое помещение;

- не разрешать, кому бы то ни было из персонала выключать или включать электроснабжение объекта;

- если перед началом обыска электроснабжение было отключено, то до его подключения следует отключить от электросети все компьютеры и периферийные устройства;

- не производить никаких манипуляций с компьютерной техникой, если их результат заранее неизвестен.

После выполнения перечисленных мероприятий необходимо произвести предварительный осмотр компьютерной техники с целью определения, какие программы работают в данный момент. В случае обнаружения работающей программы по уничтожению информации, она останавливается, и осмотр[2] начинается именно с этого компьютера.

Если компьютеры, находящиеся в помещении, соединены в локальную сеть, их осмотр целесообразно начать с сервера, затем осматривают работающие компьютеры, а затем остальную компьютерную технику и источники питания.

---

[2] В данном случае и далее под осмотром подразумевается осмотр компьютерной техники и определение подлежащих изъятию устройств.

При осмотре работающего компьютера необходимо:

- определить, какая программа выполняется в данный момент. Для этого изучается изображение на экране дисплея и детально описывается в протоколе. При необходимости может осуществляться фотографирование или видеозапись изображения на экране дисплея;

- остановить исполнение программы и зафиксировать в протоколе результаты своих действий, отразить изменения, произошедшие на компьютере;

- определить наличие у компьютера внешних устройств-накопителей информации на жестких магнитных дисках (винчестере), на дискетах и устройствах типа ZIP, наличие виртуального диска (временный диск, который создается при запуске компьютера для ускорения его работы), отразив полученные данные в протоколе;

- определить наличие у компьютера внешних устройств удаленного доступа к системе и определить их состояние (подключение к локальной сети, наличие модема), после чего отключить компьютер из сети и выключить модем, отразив в протоколе результаты своих действий;

- скопировать программы и файлы данных, созданные на виртуальном диске (если он имеется), на магнитный носитель или на жесткий диск компьютера в отдельную директорию;

- выключить компьютер и далее действовать в соответствии с положениями раздела “осмотр неработающего компьютера”.

При осмотре неработающего компьютера необходимо:

- отразить в протоколе и на прилагаемой к нему схеме местонахождение компьютера и его периферийных устройств (принтера, модема, клавиатуры, монитора и т.п.);

-отразить в протоколе назначение каждого устройства, название (обычно указывается на лицевой стороне), серийный номер, комплектацию (наличие и тип дисководов, сетевых карт, разъемов и др.), наличие соединения с локальной вычислительной сетью и (или) сетями телекоммуникации, состояние устройств (целое или со следами вскрытия);

- точно описать порядок соединения между собой указанных устройств, промаркировав (при необходимости) соединительные кабели и порты их подключения,

после чего разъединить устройства компьютера[3];

- в ходе осмотра компьютера необходимо с помощью специалиста установить наличие внутри компьютера нештатной аппаратуры, изъятия микросхем, отключение внутреннего источника питания (аккумулятора);

- упаковать (с указанием в протоколе места их обнаружения) магнитные носители на дискетах и лентах. Для упаковки могут использоваться как специальные футляры для дискет, так и обычные бумажные и целлофановые пакеты, исключающие попадание грязи и т.п. на рабочую поверхность дискеты или магнитной ленты;

- упаковать каждое устройство компьютера и соединительные кабели. Предварительно, для исключения доступа посторонних лиц, необходимо опечатать системный блок - заклеить лентой кнопку включения компьютера и гнездо для подключения электрокабеля, а также места соединения боковых поверхностей с передней и задней панелями.

Если в ходе осмотра и изъятия компьютерной техники возникает необходимость включения компьютера, его запуск необходимо осуществлять с заранее подготовленной загрузочной дискеты, исключив тем самым запуск программ пользователя.

Другим важным следственным действием по делам данной категории является назначение экспертиз. Основной и наиболее значимой является программно-техническая (компьютерно-техническая). Поскольку в системе МВД России не имеется экспертов, проводящих подобные экспертизы, практика идет по пути назначения указанного вида экспертиз в подразделениях ФАПСИ, либо привлечения специалистов соответствующей квалификации из внеэкспертных учреждений.

На разрешение программно-технической экспертизы могут быть поставлены следующие вопросы:

- Какую информацию содержат предъявленные на экспертизу системные блоки и дискеты? Какая информация имеется на системных блоках и на магнитных носителях, ее назначение и возможность использования?

- Какие программы содержатся на предъявленных системных блоках и магнитных носителях? Каково их назначение и возможность использования?

- Содержатся ли на предъявленных системных блоках и магнитных носителях текстовые файлы? Если да, то каково их содержание и возможность использования?

---

[3] Разъединение устройств, подключенных к компьютеру, может производиться только после их отключения от сети.

- Имеется ли уничтоженная информация на представленных магнитных носителях? Возможно ли ее восстановление? Если да, каково ее содержание, возможности использования?

- Какие программные продукты содержатся на предъявленных магнитных носителях? Каково их содержание, назначение, возможность использования?

- Имеются ли на представленных магнитных носителях специализированные программы, используемые для подбора паролей либо иного незаконного проникновения в компьютерные сети? Если да, то каковы их названия, особенности работы, возможности использования для проникновения в конкретную компьютерную сеть? Имеются ли признаки, свидетельствующие о применении конкретной программы для незаконного проникновения в вышеуказанную сеть? Если да, то какие?

- Какова хронологическая последовательность необходимых действий для запуска конкретной программы, либо совершения определенной операции?

- Возможно ли, работая в данной компьютерной сети произвести в среде программных продуктов какие-либо изменения программных файлов? Если возможно, то какие, каким образом и с какого компьютера могут быть произведены подобные изменения?

- Возможно ли, получить доступ к финансовой и иной конфиденциальной информации, имеющейся в указанной сети? Каким образом осуществляется такой доступ?

- Каким образом осуществлено незаконное проникновение в указанную локальную компьютерную сеть? Каковы признаки, свидетельствующие о таком проникновении?

- Если незаконное проникновение произошло извне, то какие имеются возможности по идентификации компьютера, с которого произошло проникновение?

- Если отсутствуют признаки вхождения в сеть стороннего пользователя, указать с каких компьютеров можно произвести подобные операции?

Может ставиться вопрос о совместимости тех или иных программ, возможности использования программы на конкретном компьютере и т.п.

Кроме того, перед экспертами могут ставиться вопросы о назначении того или иного предмета, связанного с компьютерной техникой:

- Каково назначение данного предмета, возможность его использования? Какие конструктивные особенности он имеет? Из каких частей состоит? Промышленным

или кустарным способом изготовлен?

- Если предмет изготовлен кустарным способом, то познаниями в какой области науки, техники и ремесла обладает лицо, изготовившее указанный предмет, каков уровень профессионализма указанного лица?

- В совокупности с какими предметами и приборами может быть использован данный предмет?

- Каковы технические характеристики данного предмета?

Предложенные методические рекомендации далеко не исчерпывают всех вопросов, связанных с расследованием хищений в кредитно-финансовой сфере, совершаемых с использованием электронных средств доступа, а лишь отражают наиболее важные особенности расследования данного вида преступлений.

НИЛ-4 ВНИИ МВД России