УДК 34. 340

Задорожная В.И., доцент кафедры ПДиНБ
Руководитель научно-исследовательской работы
«Южно-Уральский государственный университет»
Россия, г. Челябинск
Усольцева А.В.
Студент
5 курс, Кафедра Правоохранительной деятельности и национальной безопасности
«Южно-Уральский государственный университет»
Россия, Челябинск

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ХИЩЕНИЙ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

Аннотация: *Статья посвящена проблеме расследования хищений электронных денежных средств. Также рассматривается криминалистическая характеристика компьютерных преступлений.*

Ключевые слова: *хищение, кража, электронные денежные средства.*

Annotation: *The article is devoted to the problem of investigation of theft of electronic funds.The criminalistic characteristics of computer crimes are also considered.*

Key words: *of embezzlement, theft, electronic funds.*

В последние годы наблюдается интенсивное развитие информационных технологий, вычислительной техники и средств коммуникаций. Начавшаяся в середине века информационная революция наряду с удобствами оперативного доступа к всевозможным данным породила множество проблем - этических, психологических, социальных и правовых.

Исследователями еще с 80-х годов проводится анализ зарубежной судебной практики по отдельным видам рассматриваемой категории деяний, делаются выводы о невозможности обеспечения в рамках действующего законодательства уголовного преследования лиц, виновных в совершении противоправных деяний с использованием вычислительной техники, однако судебная практика по компьютерным преступлениям, совершаемым в стране, равно как и разработка соответствующих уголовно-правовых норм, ни разу не проводились.

"Использование компьютеров, одного из самых современных достижений научно-технического прогресса при преступных посягательствах значительно повышает степень их общественной опасности," - считает Н.Ф.Ахраменка. Специфическим является характер наносимого при этом вреда, и, кроме того, ущерб от компьютерных преступлений, как свидетельствует мировая практика, обычно весьма велик (в среднем, потери от одного компьютерного мошенничества в США составляют почти 500000$, что на в несколько десятков раз превышает ущерб, наносимый при традиционном ограблении). "В среднем одно компьютерное вторжение в банковскую информационную систему приносит сегодня ущерб в 650 тыс. долл., в то время как при обычном ограблении из банков в среднем за один раз уносится только 25 тыс." Один из характерных примеров отечественной практики - уголовное дело о хищении 125500$ и подготовке к хищению еще свыше 500000$ во Внешэкономбанке СССР в 1991г., рассмотренное московским судом. По материалам другого уголовного дела, в сентябре 1993г. было совершено покушение на хищение денежных средств в особо крупных размерах из Главного расчетно-кассового центра Центрального банка России по г.Москве на сумму 68 млрд. руб. Такие же факты имели место: в апреле 1994г. из расчетно-кассового центра г.Махачкалы на сумму 35 млрд. руб.; в московском филиале Инкомбанка; в филиалах Уникомбанка; в коммерческом банке Красноярского края, откуда было похищено 510 млн. руб.; в

акционерном коммерческом банке г.Волгограда - 450 млн. руб.; в Сбербанке г.Волгограда - 2 млрд. руб.

Председатель Госдумы Российской Федерации Геннадий Селезнев, выступая на открытии международного конгресса "Развитие телекоммуникаций и построение информационного общества в СНГ, заявил, что Россия теряет ежегодно до 5 млрд. долл. "только на несанкционированном изъятии из компьютерных сетей разного рода информации". По его словам, в 2000г. в Госдуме состоялось семь парламентских слушаний по этой проблеме, кроме того, руководящими органами СНГ утверждена концепция формирования единого информационного пространства Содружества.

Проблему представляет и расследование компьютерных преступлений: само противоправное действие в силу технических особенностей может длиться микросекунды, а подготовка к нему - месяцы или даже годы. Установление фактов, имеющих существенное значение для расследования подобного рода дел, может длиться достаточно долгое время или даже вообще быть невозможным для следствия в силу объективных (например, из-за простоты "заметания следов" для преступника) или субъективных (нежелание потерпевших возбуждать уголовное дело) причин. Легкий доступ к обучению навыкам работы с вычислительной техникой, быстрый рост компьютерных технологий, расширяющаяся сфера их применения - все это также свидетельствует об особой, повышенной общественной опасности компьютерных преступлений.

Официальной статистики о состоянии компьютерной преступности в республике пока что нет, однако, отсутствуя юридически, она наличествует фактически. Н.Ф.Ахраменка считает, что анализ отечественной следственной и судебной практики даже по тем немногим случаям совершения компьютерных преступлений, ставших известными, позволяет сделать вывод о неготовности правоохранительных органов к борьбе с ними: "Проблемы, возникающие с выявлением самого факта совершения, с обнаружением и

сохранением следов преступлений, совершённых с использованием ИВС либо в их отношении, с квалификацией анализируемой категории посягательств, определением размера наносимого при этом ущерба, уже на современном этапе ставят задачу научной разработки методов борьбы (в том числе и уголовно-правовых) с этим новым видом преступности."

Следует отметить, что ни законы сами по себе, ни только организационно-технические меры не способны защитить информационные системы от преступных посягательств, поэтому государству в законодательной и правоприменительной практике следует адекватно прореагировать на существование общественно опасных посягательств в сфере информатизации, как это уже сделано в сфере программно-аппаратных мер защиты.

Термин "компьютерное преступление" в основном существует в зарубежных источниках, в законодательстве РФ легального определения не существует. Следует отметить, что общепризнанного определения компьютерного преступления на сегодняшний день не имеется вообще, уголовное право иностранных государств охватывает этим понятием различные по своему характеру и степени общественной опасности виды противоправных деяний.

Так, в законодательстве ряда европейских стран (Австрии, Дании, Франции) предусматривается уголовная ответственность за неправомочное вмешательство в функционирование информационно-вычислительных систем. Из содержания норм уголовного права Великобритании следует, что его санкции применяются к "злоумышленникам, причинившим с помощью ЭВМ ущерб или использовавшим информацию в своих целях." В 80-е годы системой уголовной юстиции ФРГ был предложен целый ряд уголовно-правовых определений исследуемой категории противоправных деяний. Уголовная полиция этой страны к компьютерным преступлениям относит "все

противоправные действия, при которых электронная обработка информации является орудием их совершения и (или) их объектом."

Таким образом, общим в определении компьютерного преступления является то, что совершаются они либо в отношении, либо посредством вычислительной техники, то есть компьютерные преступления условно можно разделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, что наносит ущерб общественным или личным интересам, и преступления, использующие компьютеры как необходимые технические средства для достижения противоправных целей.

Отечественная наука в основном придерживается подобного определения. Так, А.В.Дулов к компьютерным преступлениям относит "различные преступления, совершаемые с помощью компьютеров, с нарушением их деятельности." Нам кажется, подобное определение является довольно широким и содержащим существенную неточность: результатом компьютерного преступления не обязательно должно быть нарушение деятельности самих компьютеров. Общественно-опасные последствия могут наступать и при нормальном функционировании программно-аппаратных средств компьютера при условии неверных исходных данных, при ошибках оператора или программиста, при кражах машинного времени, неправомерном доступе и т.д.

Н.А. Селиванов относит к компьютерным преступления, предметом которых является компьютерная информация, либо средством совершения которых выступает электронно-вычислительная техника, используемая с целью совершения противоправного посягательства на иной объект.

Ю.М. Батурин подразделяет объекты компьютерных атак на три категории: сами компьютеры, объекты, которые могут быть атакованы с помощью компьютера как инструмента, объекты, для которых компьютер является окружением. Представляется обоснованным не включать в состав объектов компьютерных преступлений первую категорию по данной

классификации в случаях, когда компьютеры являются не более чем имуществом, абсолютно равнозначным любым другим материальным вещам, и не подлежат выделению в отдельную правовую категорию единственно по признаку их наименования.

Классической точки зрения о том, что рамки компьютерных преступлений можно ограничить использованием ЭВМ в качестве инструмента (орудия) и предмета посягательства, придерживается и Н.Ф. Ахраменка. При этом указывается, что сам компьютер не может быть рассмотрен как предмет компьютерных преступлений, так как "предметом посягательств при их совершении является отнюдь не техника как таковая (ей ущерб, как правило, не наносится), а информация, хранимая, обрабатываемая или передаваемая этой техникой. Определяя объект компьютерных посягательств, мы исходим из того, что преступления такого рода с гораздо большим основанием следует отнести к информационным." На наш взгляд, предмет компьютерных преступлений следует еще больше расширить: помимо информации включить еще нормальное функционирование вычислительной техники и течение информационных процессов.

Обобщая вышесказанное, можно дать следующее определение компьютерного преступления: под компьютерным преступлением следует понимать виновное противоправное общественно опасное деяние, совершенное либо с помощью компьютерной техники, либо в отношении хранимой, передаваемой или обрабатываемой информации, предусмотренное нормой особенной части уголовного кодекса.

Аналогично понятию, в литературе нет единого мнения о том, каким образом и по каким критериям классифицировать преступления в этой сфере. Одной из первых попыток в отечественной науке было предложенное Ю.М. Батуриным разделение компьютерных преступлений по способу их совершения на:

1. методы перехвата;

2. методы несанкционированного доступа;

3. методы манипуляции.

В каждой из указанных групп Батурин выделяет группы способов, название и описание которых дано ниже, в разделе "Способы совершения компьютерных преступлений".

Марк Экенвайлер выделил три основных категории (с дальнейшей дифференциацией) в зависимости от способа использования компьютера при совершении преступлений:

1) Компьютер является объектом правонарушения, когда цель преступника - похитить информацию или нанести вред интересующей его системе:

a) изъятие средств компьютерной техники. К этой группе относятся традиционные способы совершения обычных видов преступлений, в которых действия преступника направлены на изъятие чужого имущества

b) хищение информации;

c) хищение услуг (получение несанкционированного доступа к какой-то системе с целью безвозмездного пользования предоставляемыми ею услугами);

d) повреждение системы. Данная группа объединяет преступления, совершаемых с целью разрушить или изменить данные, являющиеся важными для владельца или одного или многих пользователей системы - объекта несанкционированного доступа;

e) уивинг (запутывание следов, когда целью атаки является стремление скрыть свое имя и местонахождение).

Здесь следует отметить, что объектом правонарушения может быть устройство, не являющееся компьютером в общепринятом понимании этого слова - сотовый телефон, кассовый аппарат, PIC и т.п.

2) Компьютеры используются как средства, способствующие совершению преступления:

a) как средство совершения традиционных преступлений (как правило, мошенничество);

b) как средство атаки на другой компьютер, средство совершения иного компьютерного преступления.

3) Компьютер используется как запоминающее устройство (например, после взлома системы создается специальная директория для хранения файлов, содержащих программные средства преступника, пароли для других узлов, списки украденных номеров кредитных карточек и т.п.)

Способ совершения преступления представляет собой совокупность действий преступника, направленных на подготовку, совершение и сокрытие данного преступления. С криминалистической точки зрения способы совершения имеют достаточно важное значение и проявляются в следующих характеристиках: распространенность, приемы и условия его применения, необходимые для этого технические средства, источники их получения и т.д.

Конкретных, общепринятых названий способов и их классификации в науке в настоящее время не существует - эта проблема пока что находится в стадии теоретической разработки. В зарубежной литературе имеется ряд наработок в этой сфере, которые, с определенной долей условности, можно применять и у нас, с учетом международного характера компьютерных преступлений. Так, основными методами получения несанкционированного получения информации, по данным Американского Национального института компьютерной безопасности, являются:

- применение подслушивающих устройств (закладок);
- дистанционное фотографирование;
- перехват электронных излучений;
- мистификация (маскировка под запросы системы);
- перехват акустических излучений и восстановление текста принтера;
- хищение носителей информации и производственных отходов (сбор мусора);

- считывание данных из массивов других пользователей;

- копирование носителей информации с преодолением мер защиты;

- маскировка под зарегистрированного пользователя;

- использование программных ловушек;

- незаконное подключение к аппаратуре и линиям связи;

- вывод из строя механизмов защиты.

Ю.М. Батурин выделяет три основные группы способов совершения компьютерных преступлений:

1. Методы перехвата.

Непосредственный перехват - его особенностью является то, что подключение производится прямо к коммуникационным каналам либо узлам передачи данных. Объектами перехвата могут быть кабельные и проводные системы, системы радио- и спутниковой связи.

Электромагнитный перехват осуществляется по остаточным излучениям тех или иных устройств (дисплея, принтера, систем коммуникаций), причем на достаточном удалении от объекта излучения.

Представляется обоснованным выделить здесь подгруппу "удаленный перехват", поместив туда электромагнитный перехват, аудиоперехват (снятие информации по виброакустическому каналу) и видеоперехват (получение информации с помощью видеооптической техники).

Э.Мелик выделяет также в этой группе метод "Уборка мусора", то есть поиск "отходов" информационного процесса, как физического характера (бумаги, счета, иной мусор), так и электронного (поиск и восстановление удаленных данных).

2. Методы несанкционированного доступа.

Эти методы имеют свои специфические названия, достаточно распространенные как за рубежом, так и в отечественной практике.

Метод "Следование за дураком" (pigbacking). Заключается в несанкционированном проникновении в закрытые зоны следом за законным пользователем или вместе с ним.

Метод "Захвост" (between the lines entry). Это подключение к линии связи законного пользователя и, после прекращения им сеанса связи, продолжение осуществления доступа к системе от его имени.

Метод "Компьютерный абордаж" (hacking). Обычно используется для проникновения в чужие информационные сети путем перебора идентифицирующих признаков законных пользователей (как правило, имен и паролей).

Метод "Неспешный выбор" (browsing). Однажды обнаружив слабые места в системе защиты, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости.

Метод "Маскарад" (masquerading). Проникновение в компьютерную систему, имитируя законного пользователя.

Метод "Мистификация" (spoofing). Используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коды пользователя.

Особую опасность представляет несанкционированный доступ в компьютерные системы финансовых учреждений с целью хищения финансовых средств.

По оценкам отечественных специалистов, уже сейчас хищения с применением компьютерной техники и средств электронного платежа представляют серьезную угрозу. В ближайшем будущем прогнозируется значительный рост преступности в данной сфере и увеличение ее доли в общем количестве преступлений.

3. Методы манипуляции.

Подмена данных заключается во вводе неверной информации, на основании которой системы автоматизированной обработки информации имеют на выходе неверные результаты.

Подмена кода - это, по сути, изменение самого процесса ввода, хранения, обработки, вывода информации.

Моделирование используется как для анализа процессов, в которые преступники предполагают вмешаться, так и для планирования методов совершения преступления.

Троянский конь (Trojan horse) - способ, состоящий в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

Салями (salami attack) - присваивание округляемых остатков на счетах.

Логическая бомба (logic bomb) - тайное встраивание в программу набора команд, который должен сработать при определенных условиях.

Временная бомба (time bomb) - разновидность логической бомбы, условием в которой является определенный момент времени или временной интервал.

Асинхронная атака состоит в смешивании команд двух или нескольких пользователей, чьи команды компьютерная система выполняет одновременно.

Специфика рассматриваемой категории преступлений такова, что юрист-следователь, как правило, не обладает специальными познаниями в этой области. Предположения о том, что тот или иной компьютер или носитель является хранилищем важной для данного дела информации, являются обычно вероятностными, следователь не обладает доказательственной информацией, в лучшем случае лишь оперативной, необходимыми техническими навыками для ее безопасного извлечения он также не обладает. Поэтому специалисты крайне необходимы для участия в

обысках, осмотрах, выемках как в стадии предварительного расследования, так и в стадии возбуждения уголовного дела.

По мнению А.Н. Яковлева, специальные познания должны использоваться:

* при подготовке к производству отдельных следственных действий;

* при осмотре места происшествия, обыске и выемке;

* при допросе, очной ставке, следственном эксперименте.

В системе МВД Российской Федерации уже начато производство так называемых программно-технических экспертиз, с помощью которых решаются следующие задачи:

1. Распечатка всей или части информации, содержащейся на жестких дисках компьютеров и на внешних магнитных носителях, в том числе из нетекстовых документов;

2. Распечатка информации по определенным темам;

3. Восстановление стертых файлов и стертых записей в базах данных, уточнение времени стирания и внесения изменений;

4. Установление времени ввода в компьютер определенных файлов, записей в базы данных;

5. Расшифровка закодированных файлов и другой информации, преодоление рубежей защиты, подбор паролей;

6. Выяснение каналов утечки информации из локальных вычислительных сетей, глобальных сетей и распределенных баз данных;

7. Установление авторства, места подготовки и способа изготовления некоторых документов;

8. Выяснение технического состояния и исправности средств компьютерной техники.

В связи с тем, что при осмотре ЭВМ и носителей информации производится изъятие различных документов, в ходе расследования возникает

необходимость в назначении криминалистической экспертизы для исследования документов.

Кроме того, дактилоскопическая экспертиза может выявить на документах, частях ЭВМ и машинных носителях следы пальцев рук причастных к делу лиц.

Специалисты и эксперты могут оказать действенную помощь при решении следующих вопросов (примерный список):

1. Какова конфигурация и состав компьютерных средств и можно ли с помощью этих средств осуществить действия, инкриминируемые обвиняемому?

2. Какие информационные ресурсы находятся в данной ЭВМ?

3. Каким способом мог быть совершен несанкционированный доступ в данную компьютерную систему?

4. Не являются ли обнаруженные файлы копиями информации, находившейся на конкретной ЭВМ?

5. Подвергалась ли данная компьютерная информация уничтожению, копированию, модификации?

6. Не являются ли представленные тексты на бумажном носителе записями исходного кода программы, внесения изменений в существующую программу, и каково назначение этой программы либо каков результат внесенных изменений?

7. Не являются ли представленные файлы с программами, зараженными вирусом, и если да, то каким именно?

8. Является ли предоставленный код вирусным?

Одним из отрицательных последствий развития вычислительной техники и электронных средств коммуникаций является компьютерная преступность - совершение противоправных деяний в отношении или посредством ЭВМ. Эта проблема в последнее время приобретает особую актуальность в свете неразвитой законодательной базы, регулирующей

отношения в этой сфере, неготовности правоохранительных органов к расследованию, пресечению и предупреждению правонарушений и отсутствия судебной практики.

Эффективная защита прав и интересов граждан может быть обеспечена лишь применением всего комплекса мер как организационно-технического, так и правового характера. В республике в настоящее время объективно сложились основания криминилизации такого рода правонарушений - преступлений против информационной безопасности, что требует внесения соответствующих изменений и дополнений в действующее законодательство, развития методической системы расследования данных преступлений.

На симпозиуме по профилактике и пресечению компьютерной преступности (VIII конгресс ООН по профилактике преступлений и обращению с правонарушителями, Гавана, 1990 год) было констатировано, что "компьютерная преступность и ее последствия представляют собой новую форму антиобщественного поведения, которое лишь недавно получило признание как явление, представляющее собой всеобщую угрозу безопасности и нормальному функционированию нашего общества."

Компьютерная преступность имеет международный характер, поскольку в связи с созданием единого информационного пространства территориальных ограничений для нее не существует, что требует столь же широкого международного сотрудничества правоохранительных органов в этой сфере. Нам следует использовать уже накопленный позитивный опыт зарубежных стран в борьбе с компьютерной преступностью, а общее отставание в сфере информатизации ликвидировать хотя бы в части предупреждения компьютерной преступности и разработки научно-методологических основ правового регулирования отношений в этой сфере. Легальная дефиниция составов конкретных компьютерных преступлений в уголовном кодексе уже дана, следующими этапами являются создание криминалистических характеристик компьютерных преступлений, научное

изучение феномена информации как объекта поиска, обнаружения, фиксации и криминалистического исследования, проблемы обучения навыкам поиска, обнаружения, фиксации и исследования доказательств при расследовании информационных преступлений.

Исходя из вышеописанных задач, в данной работе была сделана попытка дать понятие компьютерного преступления в общем виде, провести анализ конкретных видов, дать уголовно-правовую и криминалистическую характеристику компьютерных преступлений, а также разработать прогноз возможных следственных ситуаций и методику их расследования.

Библиографический список:

1. Ахраменка Н.Ф. Криминализация общественно опасного поведения с использованием информационно-вычислительных систем.

2. Батурин Ю.М. "Компьютерное преступление" - что за термином? // Право и информатика. - М.: МГУ, 1990.

3. Белкин Р.С. Курс криминалистики. Т. 3: Криминалистические средства, приемы и рекомендации. - М.: Юристъ, 1997.

4. Борьба с компьютерной преступностью в рамках ООН. // Борьба с преступностью за рубежом. - М.: ВИНИТИ, 1992, №5.

5. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. - М.: Право и Закон, 1996.

6. Волков Д.В. "В Россию за идеями". // Computerworld Россия. -М., "Открытые Системы", 1996, №38.

7. Дулов А.В. Криминалистический анализ компьютерных преступлений. // Проблемы "компьютерной преступности": Выпуск 2. - Мн.: НИИ ПККСЭ МЮ РБ, 1992.

8. Мелик Э. Компьютерные преступления. Информационно-аналитический обзор. - Internet: http://www.melik.narod.ru

9. Селиванов Н.А. Расследование особо опасных преступлений. Пособие для следователей. - М., Бек, 1998.
10. Черкасов В.Н. Компьютерная преступность и ее предупреждение. - Мн.: НИИПККиСЭ, 1996.
11. Яковлев А.Н. Использование специальных познаний при расследовании "компьютерных" преступлений // Конфидент. - С-Петербург, 2000. №6.