

Вехов В. Б.

Компьютерные преступления. Способы совершения методики расследования.

Введение

Современный этап развития российского общества характеризуется стратегическим курсом на создание правового государства. В стране осуществляются радикальные социально-экономические реформы, идет процесс демократизации всех сторон общественной жизни, который невозможен без укрепления законности и правопорядка, обеспечения надежной охраны конституционных прав и свобод граждан.

Вместе с тем в последние годы произошло резкое ухудшение криминальной обстановки, которая в настоящее время оценивается как чрезвычайно острая и сложная. Отмечается резкое нарастание криминального профессионализма, множатся дерзкие по замыслу и квалифицированные по исполнению преступления. При общем сокращении краж, грабежей и разбоев возрастает число хищений крупных денежных сумм из банков и иных кредитно-финансовых учреждений, касс предприятий и организаций.

Дестабилизирующее влияние на обстановку в стране оказывает и набирающая силу организованная преступность, которая в последнее время наряду с совершением общеуголовных преступлений интенсивно интегрируется в экономическую сферу с целью получения сверхвысоких незаконных доходов, сливаясь при этом с конгломератом экономической преступности. В связи с этим происходит процесс расширения масштабов преступных проявлений, который характерен практически для всех отраслей экономики России [16].

Одновременно с вышеуказанным развертывание научно-технической революции обуславливает не только коренные прогрессивные изменения в составе факторов экономического развития России, но и негативные тенденции развития преступного мира, приводит к появлению новых форм и видов преступных посягательств. Это ярко проявляется в том, что преступные группы и сообщества начинают активно использовать в своей деятельности новейшие достижения науки и техники. Так, преступники для достижения корыстных целей все чаще применяют системный подход при планировании своих действий, разрабатывают оптимальные варианты проведения и обеспечения криминальных "операций", создают системы конспирации и скрытой связи, принимают дополнительные меры по оказанию эффективного противодействия сотрудникам правоохранительных органов, используют современные технологии и специальную технику, в том числе и всевозможные компьютерные устройства и новые информационно-обрабатывающие технологии.

Особую тревогу в этом плане вызывает факт появления и развития в России нового вида преступных посягательств, ранее неизвестных отечественной юридической науке и практике и связанных с использованием средств компьютерной техники и информационно-обрабатывающей технологии, — компьютерных преступлений. Последние потребовали от российского законодателя принятия срочных адекватных правовых мер противодействия этому новому виду преступности. Поэтому при подготовке работы автором были изучены и проанализированы: нормы действующего уголовного и уголовно-процессуального законодательства Российской Федерации; нормативные акты МВД России (приказы, указания, директивы); аналитические материалы, относящиеся к исследуемой проблематике; соответствующая отечественная и зарубежная литература; материалы следственной практики; материалы международных конференций по проблемам правового обеспечения процессов информатизации и формирования единого информационно-правового пространства, а также по проблемам борьбы с преступностью; законодательные акты Российской Федерации по вопросам ответственности за компьютерные правонарушения.

Проблемам компьютерной преступности в последние годы было уделено определенное внимание в монографиях, учебных пособиях, научных статьях. Однако большая часть из них посвящена исследованию уголовно-правовых и криминологических аспектов компьютерной преступности, нашедших свое отражение в работах А.Б. Агапова, А.Б. Атлас, Ю.М. Батурина, С. Гришаева, А. Днепрова, АМ Жодзишского, КА Зуева, ИЛ Исаченко, И.З. Карась, Г.Б. Кочеткова, А.В. Литвинова, ИМ Могилевского, АЛ. Полежаева, Е.А Суханова, ВН. Черкасова, А Черных, Э. Черных и др. Криминалистические же аспекты компьютерных преступлений освещены лишь частично в работах В.Н. Белова, П.Б. Гудкова, АН. Караханьяна, В.Д. Курушина, В.Д. Ларичева, Н.С. Полевого, Н.А. Селиванова, Ю.Н. Соловьева, В. Федорова, А.В. Шопина.

Несмотря на несомненную и бесспорную теоретическую и практическую значимость указанных исследований, в них не рассматривается в комплексе криминалистическая характеристика компьютерных преступлений, а также четко не выделены проблемы, касающиеся совершенствования практики их раскрытия и предупреждения. Это в конечном итоге оказывает негативное влияние на качественный уровень профессиональной подготовки сотрудников правоохранительных органов, приводит к снижению эффективности следственной и оперативной работы по преступлениям рассматриваемой категории.

Поэтому, критически оценивая современное состояние криминалистической теории и учитывая потребность оперативно-следственной практики, надо признать, что в целом проблемы криминалистической характеристики и совершенствования практики раскрытия, расследования и предупреждения компьютерных преступлений изучены явно недостаточно. Особенно много вопросов возникает по поводу содержания понятия и криминалистической классификации данных преступных посягательств, определения способа их совершения, необходимости планирования и своевременности проведения тех или иных следственных действий на первоначальном этапе расследования преступления. Необходимость всестороннего исследования обозначенных проблем диктуется как потребностью следственной практики, так и задачами дальнейшего совершенствования криминалистической теории и усиления ее влияния на результативность борьбы с компьютерной преступностью.

В качестве одного из возможных вариантов решения указанных выше проблем следует рассматривать предлагаемую работу.

Понятие компьютерных преступлений

В современных условиях социально-экономического развития Российской Федерации компьютерная преступность стала реальностью общественной жизни.

Понимание причин ее возникновения и развития требует анализа сложившихся кризисных ситуаций, влияющих на социальное, экономическое и правовое развитие российского общества. Проведенное исследование проблем борьбы с компьютерной преступностью позволяет нам сделать вывод, что ее появлению и последовательному росту способствует ряд факторов: политических, социальных, экономических и правовых. Так, 87% опрошенных нами респондентов считают, что на возникновение и развитие компьютерных преступлений существенное влияние оказывают экономические факторы, 35% — выделяют социальные факторы, 30% — правовые и лишь 13% — политические. В то же время 92% респондентов уверены в том, что по мере компьютеризации российского общества количество компьютерных преступлений будет увеличиваться (здесь и далее по тексту работы приводятся цифровые данные, отражающие материалы проведенного автором в течение 1992-1995 гг. научного исследования, в ходе которого были изучены материалы значительного числа уголовных дел и по специальным анкетам были опрошены 86 начальников городских/районных управлений/отделов органов внутренних дел, 44 руководителя следственных подразделений и 22 следователя УВД и МВД практически всех областей, регионов, республик и автономных образований, входящих в состав Российской Федерации). Среди секторов экономики страны, имеющих в настоящее время наиболее благоприятные условия для совершения компьютерных преступлений, были выделены следующие: смешанный (33% опрошенных), государственный (32% опрошенных), во всех в равной мере (31% опрошенных), а среди отраслей экономики — банковская (81%) и финансовая (53%).

Как показывает анализ дискуссионных материалов в литературе и периодической печати, данные проведенного нами исследования, негативные тенденции в значительной степени обусловлены бурным процессом развития научно-технической революции (НТР).

Эта революция, как и предшествующие ей в истории общества революции (аграрная и промышленная), повлекла за собой серьезные социальные изменения, наиболее важным из которых является появление нового вида общественных отношений и общественных ресурсов — информационных. Последние отличаются от известных ранее сырьевых, энергетических ресурсов целым рядом особенностей, а именно:

- 1) они непотребляемы и подвержены не физическому, а моральному износу;
- 2) они по своей сущности нематериальны и несводимы к физическому носителю, в котором воплощены;
- 3) их использование позволяет резко сократить потребление остальных видов ресурсов, что в конечном итоге приводит к колоссальной экономии средств;
- 4) процесс их создания и использования осуществляется особым способом — с помощью компьютерной техники [85, с. 9],

Информация стала первоосновой жизни современного общества, предметом и продуктом его деятельности, а процесс ее создания, накопления, хранения, передачи и обработки в свою очередь стимулировал прогресс в области орудий ее производства: электронно-вычислительной техники (ЭВТ), средств телекоммуникаций и систем связи. Все это в целом входит в емкое понятие определения новой информационной технологии (НИТ), которая является совокупностью методов и средств реализации информационных процессов в различных областях человеческой деятельности, т. е. способами реализации информационной деятельности человека, которого также можно рассматривать как информационную систему [1, с. 31]. Иными словами, информация становится продуктом общественных (информационных) отношений, начинает приобретать товарные черты и становится предметом купли-продажи [37, с. 3; 38, с. 40-41]. Следствием протекающих в обществе информационных процессов является возникновение и формирование новых социальных отношений и изменение уже существующих. Например, уже сейчас можно констатировать значительный объем договорных отношений, связанных с изготовлением, передачей, накоплением и использованием информации в различных ее формах: научно-технической документации, программного обеспечения ЭВТ, баз данных, систем управления базами данных (СУБД) и др. [85, с. 9—10].

Данные положения нашли свое официальное закрепление в Федеральном Законе “Об информации, информатизации и защите информации”, вступившем в действие с января 1995 г. В соответствии со ст. 2 которого:

- 1) под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- 2) документированной информацией (документом) признается зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- 3) информационным процессом считается процесс сбора, обработки, накопления, хранения, поиска и распространения информации;
- 4) информационным ресурсом являются отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- 5) под информационной системой понимается организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в т. ч. с использованием средств компьютерной техники и связи, реализующих информационные процессы. А в п. 6 ст. 6 данного законодательного акта информация и информационные ресурсы признаются товаром со всеми вытекающими из этой дефиниции последствиями [31].

В связи с этим новые информационные технологии дали толчок не только в плане прогресса общества, но и стимулировали возникновение и развитие неизвестных ранее негативных процессов. Одним из них является появление новых форм преступности. Так, например,

революция в области электроники предоставила преступникам, их группировкам и сообществам широкие возможности в плане доступа к новым техническим средствам, которые позволяют им незаконно присваивать миллиарды рублей, отмывать огромные доходы, полученные преступным путем, уходить от налогообложения и проводить комплексные мероприятия по подготовке, совершению и маскировке различных видов преступлений [25, п. 9].

Помимо негативных факторов исторического развития общества в период научно-технической революции, существует и ряд других, не менее важных, также оказывающих существенное влияние на развитие новых форм преступности в России. К ним, в частности, на наш взгляд, можно отнести:

- 1) частичную потерю государственным аппаратом функций полнокровного управления обществом и государством;
- 2) противоречивость и несовершенство законодательной базы;
- 3) неспособность государственных институтов удовлетворить жизненно необходимые потребности населения;
- 4) бесхозяйственность и разбалансированность экономики страны особенно в кредитно-финансовой, валютно-денежной и товарно-сырьевой сферах;
- 5) незаинтересованность в сохранности материальных ценностей со стороны должностных лиц государственных и финансово-коммерческих структур.

Процесс социальной, экономической и политической перестройки российского общества, в свою очередь, вызвал снижение общего уровня жизни значительного числа населения.

Постоянное увеличение числа граждан, оказавшихся за чертой бедности, процессы миграции населения страны из бывших республик СССР, растущий уровень безработицы и неполной занятости трудоспособных лиц из-за сокращения общей продолжительности рабочей недели и вынужденных отпусков по причине остановки предприятий, учреждений и организаций, падение нравственности на фоне образа жизни и двойной морали представителей властно-управленческих и коммерческих структур, инфляционные процессы в экономике, послужили надежным источником пополнения всех эшелонов преступности, явились катализатором ее новых форм и видов.

Среди этого отрицательного многообразия факторов нам представляется необходимым обратить особое внимание на растущую безработицу и неполную занятость трудоспособной части населения. Во-первых, рынок безработных в России с каждым днем пополняется за счет так называемого конверсионного сокращения высококвалифицированных специалистов, обслуживавших структуры военно-промышленного комплекса, различные научно-исследовательские центры, лаборатории и институты, а также реорганизованного в недавнем прошлом КГБ и Министерства безопасности России, уволенных в запас по разным причинам сотрудников силовых министерств и выпускников высших учебных заведений страны, не нашедших работу по специальности. Во-вторых, именно за счет таких лиц современная преступность не испытывает недостатка в кадрах, способных эффективно использовать новейшие электронные средства, технологические новшества, свои профессиональные знания и умения для подготовки, совершения, маскировки преступлений и активного противодействия работе правоохранительных органов. Например, зарубежной практике уже известны случаи, когда организованные преступные группы и сообщества, специализирующиеся на торговле наркотиками, использовали самые современные средства компьютерной техники, чтобы избежать прослушивания телефонных переговоров. Так, по мнению специалистов, с помощью указанных технических средств преступники могут определить момент начала наблюдения за ними, в связи с чем в настоящее время наблюдается рост числа случаев использования преступниками современных средств связи, основанных на использовании микропроцессорной техники, позволяющих преступнику без особого труда проникать в различные системы связи с целью перехвата телефонных разговоров, определения номера интересующего абонента и т. п., обеспечивая тем самым проведение собственных разведывательных и контрразведывательных мероприятий. Таким образом можно, например, определить, кто находится "на разработке" специальных служб и подразделений правоохранительных органов (46, с. 5].

По данным российских спецслужб, отмечены случаи обнаружения так называемых “жучков” на телефонных линиях связи в некоторых крупных коммерческих организациях и по месту жительства их сотрудников, что свидетельствует об использовании спецтехники криминальными структурами. Имеются оперативные данные о создании подпольных мастерских по изготовлению разведывательной и контрразведывательной техники бывшими сотрудниками органов внутренних дел и органов безопасности. Специальная техника свободно продается в коммерческих магазинах по доступной цене, что делает возможным криминальным элементам практически бесконтрольно проводить оперативно-технические мероприятия, в т. ч. для получения информации о деятельности спецслужб и правоохранительных органов [13, с. 23].

Тревожит тот факт, что этот процесс имеет тенденцию к дальнейшему расширению.

Рост безработицы сразу же повлиял на изменение криминогенной ситуации. Это в свою очередь коренным образом изменило расклад сил в криминальном мире, объективно расширило ресурсную базу преступности, повысило ее профессионализацию, а также “социальную значимость” лидеров преступных групп и сообществ, способных организовать жизнедеятельность определенной части потерявших работу граждан, дать им возможность к существованию в условиях кризиса экономики страны и паралича государственных структур [65, с. 30].

Именно эти факторы в своей совокупности и обусловили динамичный рост и поступательное развитие новых видов преступлений к числу которых относятся и компьютерные преступления.

Анализ состояния преступности в России показывает, что криминогенная обстановка в последние годы чрезвычайно обострилась. Преступность стала одним из основных дестабилизирующих факторов общественного развития. Ее масштабы представляют реальную угрозу процессу становления российской государственности, успешному осуществлению социально-экономических реформ. Вместе с этим в динамике преступности произошли существенные изменения. Устойчивый характер приобретают тенденции роста тяжких преступлений, вооруженности, профессионализма и организованности преступников, развитие межрегиональных и транснациональных связей преступных сообществ. Нарастает число дерзких по замыслу и квалифицированных по исполнению преступлений [16, п. I].

Основной особенностью современной криминогенной ситуации является интенсивное перерастание количественных характеристик преступности в негативные качественные. Набирают силу опасные процессы сращивания организованной преступности с так называемой респектабельной (“беловоротничковой”), к которой нами относятся экономическая и компьютерная преступность; лидеров преступных групп и сообществ с коррумпированными должностными лицами. По данным проведенного нами исследования, 75% опрошенных респондентов отнесли компьютерные преступления к разряду “беловоротничковых”, отметив при этом, что они, как правило, совершаются группой лиц и носят организованный характер. Идет активный процесс размывания граней между различными видами преступлений. Например, преступники, организованные в группы и сообщества, начинают применять методы, традиционно используемые в своей преступной деятельности преступниками экономической сферы, нередко используя при этом средства компьютерной техники, связи и телекоммуникаций и входя в сговор с должностными лицами. Данный процесс приводит к тому, что многие преступные сообщества начинают переориентировать свою преступную деятельность с получения и использования незаконных средств, добытых противоправными действиями (например, вымогательством), на совершение противоправных манипуляций с законными средствами в корыстных целях. Иными словами, переходят от оборота преступных средств к более выгодному преступному обороту законных средств. Международный опыт свидетельствует, что современная преступность проникает в область законного предпринимательства, подрывая репутацию тех, кто так или иначе соприкасается с ней, и коррумпирует должностных лиц, услуги которых ей необходимы для отмыкания незаконных доходов. На уровне ООН констатировано, что возможности преступности манипулировать значительным капиталом, проникать в область законного предпринимательства и разорять своих конкурентов с помощью контроля над ценами и курсом валют представляет собой серьезную угрозу самому существованию любого общества (65, с. 42]. Например, огромные незаконные средства, проникающие в экономику страны, денежную систему, банковское дело путем манипулирования валютой с целью “отмыкания” денег или для получения незаконных доходов, неизбежно приводят к нарушению естественного действия рыночных сил, оказывают пагубное влияние на обменные курсы валют и банковские системы одновременно во многих странах [25].

Анализ криминогенной ситуации в России показывает, что зачастую лидеры преступных группировок, собрав достаточные суммы, вступают в легальный бизнес, становятся генеральными и коммерческими директорами негосударственных структур, банков, вступают в непосредственный контакт с представителями законодательной, исполнительной и судебной власти, работниками правоохранительных органов.

Созданные лидерами преступных группировок предприятия негосударственного сектора экономики используются ими в роли легальной “крыши” для отмывания средств, добытых незаконным путем. В конечном итоге это дает им возможность реинвестировать доходы в новые поставки товаров и посредством инвестиций в законную экономику сливаться с легальным бизнесом. Последний при этом служит им удобным прикрытием для совершения крупномасштабных сделок, связанных с контрабандными перевозками сырья и полуфабрикатов, цветных и драгоценных металлов, энергоносителей, товаров народного потребления, продукции производственно-технического и военного назначения, с бестоварными экспортно-импортными операциями, а также для незаконного перевода денежных средств на счета зарубежных банков и т. д. В результате чего увеличивается количество преступлений транснационального характера на территории России.

Подобная тенденция скрывает высокую социальную опасность преступности для общества, поскольку значительно затрудняет возможности раскрытия, расследования подобных преступлений установления конкретной потерпевшей стороны. Например, крайне низка в настоящее время эффективность борьбы с преступными посягательствами в сфере денежного обращения. Практика показывает, что по этим видам преступлений в основном задерживаются и привлекаются к уголовной ответственности второстепенные участники организованных преступных групп и сообществ, тогда как их лидеры и организаторы остаются безнаказанными [16]. Между тем в России в настоящее время специалистами констатируется беспрецедентная криминальная экспансия в банковскую систему. По этому поводу бывший председатель Центрального банка России В.В. Герашенко, выступая на Всероссийском совещании по проблемам борьбы с организованной преступностью и коррупцией 12 февраля 1993 г. отметил, что преступные элементы умело воспользовались дезорганизацией платежной системы: в частности, было выявлено прохождение фиктивных банковских документов, в том числе и с грифом “Россия”, на сотни миллиардов рублей, что в свою очередь потребовало применения экстренных дорогостоящих мер по усилению защиты банковской информации, приведшее к еще большему замедлению расчетов и усугублению и без того критической ситуации неплатежей [65, с. 84].

Быстрый количественный рост преступности и ее качественные изменения, обусловленные обострением противоречий в различных областях общественной жизни, частой реорганизацией системы правоохранительных органов, несовершенство законодательства и частое его изменение, серьезные упущения в правоприменительной практике, на наш взгляд, способствуют ускорению процессов развития компьютерной преступности как социального явления.

Как отмечалось в докладе генерального секретаря ООН, мировой опыт свидетельствует о том, что по мере развития в мире техники и появления специалистов более высокой квалификации “... появляется все больше талантливых людей для изобретения новых уникальных способов совершения преступлений”, особенно в области информационно-обрабатывающих технологий [25, п. 20].

По нашему мнению, в этой области законодательство часто не поспевает за развитием техники, а подготовка сотрудников Правоохранительных органов является недостаточной для решения задач, связанных с обнаружением и контролем за этим Новым видом преступности. “Ножницы” между нарастающим профессионализмом, организованностью преступного мира и Уровнем подготовки, опытом противостоящих ему работников органов внутренних дел существенным образом влияют на результативность и качественные характеристики в борьбе с преступностью. Не способствует повышению эффективности борьбы с компьютерной преступностью и состояние кадрового состава следственно-оперативных работников, который характеризуется в первую очередь ослаблением профессионального ядра, сокращением числа высококвалифицированных и опытных специалистов.

Между тем, анализируя нынешнее развитие ситуации с точки зрения будущего, специалистами прогнозируется рост организованной преступности, связанной с использованием электронных средств, одним из которых является компьютер [25, п. 5]. Финансовые системы мира, несомненно, во все большей степени будут полагаться на обработку данных с помощью ЭВМ и новых информационных технологий и по мере развития техники все большее число стран будет

подключаться к существующим и вновь образуемым электронным компьютерным информационным сетям, на которые в настоящее время опирается вся мировая экономика, что неизбежно приведет к появлению еще большего желания обогащения со стороны преступных групп и сообществ [25, п.п. 9, 21]. Так, например, по данным ФБР США, российским специалистам-компьютерщикам, входящим в состав отечественных преступных групп и сообществ, осуществляющих свою преступную деятельность на территориях США и западноевропейских стран и обладающих достаточным финансовым и кадровым потенциалом, в настоящее время не составляет особого труда “взломать” почти любые коды и получить доступ к коммерческим секретам крупнейших многонациональных корпораций. В результате чего с использованием компьютерной технологии как в России, так и за рубежом совершаются банковские транс- и транзакции, при которых десятки миллионов долларов в считанные минуты незаконно снимаются со счетов корпораций и переводятся на оффшорные счета, используемые преступниками [69]. Только на Кипр в 1991 г. из России на оффшорные счета фирм поступило 2,6 млрд. долларов США [26, с. 81]. Согласно оценкам специалистов, ежемесячно совершается около тысячи подобных “операций”, проследить за которыми ни ФБР, ни другие спецслужбы пока не в состоянии [102;103].

Отсутствие четкого определения компьютерной преступности, единого понимания сущности этого явления значительно дудняют определение задач правоприменительных органов „ выработке единой стратегии борьбы с ней.

До недавнего времени считалось, что компьютерная преступность — явление, присущее только зарубежным капиталистическим странам, и по причине слабой компьютеризации нашего общества, т. е. недостаточного внедрения в производственные и общественные отношения информационных технологий, отсутствует вообще. На наш взгляд, именно это обстоятельство и привело к отсутствию сколько-нибудь серьезных научных исследований этой проблемы. Только в последние годы появились работы по проблемам борьбы с компьютерной преступностью, в которых рассматриваются в основном уголовно-правовые и криминологические аспекты этого явления. Как нередко случалось уже ранее, например — ситуация с наркоманией или с организованной преступностью, борьба с этим социально опасным явлением началась лишь после того, как материальные потери от этого нового вида преступлений достигли существенных размеров и стали резко выделяться на общем фоне потерь от обычных видов общеуголовной преступности. Само появление компьютерной преступности в нашей стране приводит к выводу о том, что это явление свойственно всем государствам, которые в силу своего научного прогресса вступают в период широкой компьютеризации своей деятельности. Так, анализ специальной литературы показывает, что практически во всех промышленно развитых государствах наблюдается увеличение числа уголовных дел, связанных с компьютерной преступностью.

Впервые о проблемах борьбы с компьютерной преступностью в России отечественная криминалистическая наука официально заявила лишь совсем недавно, с июля 1992 г. с момента создания постоянно действующего межведомственного семинара “Криминалистика и компьютерная преступность”, организованного в рамках координационного бюро по криминалистике при Научно-исследовательском институте проблем укрепления законности и правопорядка Генеральной прокуратуры Российской Федерации и Экспертно-криминалистического центра МВД России [86]. Этому факту предшествовал ряд объективных и субъективных обстоятельств, которые и будут рассмотрены нами далее.

Так, в течение последних 15-20 лет по мере компьютеризации хозяйственно-управленческой и финансово-коммерческой деятельности появились, как мы уже отмечали, новые, ранее не встречавшиеся в следственной практике виды преступлений, которые стали называться компьютерными, исходя из аналогов и терминологии зарубежной юридической практики.

Данные преступные деяния получили наибольшее распространение в различных отраслях хозяйства и управления, в том числе производстве, банковском деле и в сфере обслуживания населения. Так, проведенное исследование свидетельствует о том, что за последние годы в числе выявленных корыстных преступлений широкое распространение получили хищения денежных средств в крупных и особо крупных размерах на промышленных предприятиях, в учреждениях и организациях, применяющих автоматизированные системы, функционирующие на основе ЭВМ для обработки первичных бухгалтерских документов, отражающих кассовые операции, движение материальных ценностей и другие разделы учета. Первое преступление подобного рода в бывшем СССР было зарегистрировано в 1979 г. в г. Вильнюсе. Ущерб государству от хищения составил 78584 рубля. Данный факт был занесен в международный реестр правонарушений подобного рода

и явился своеобразной отправной точкой в развитии нового вида преступлений в нашей стране [2, с. 126].

В настоящее время в России особенно ярко подобная тенденция проявляется в финансовых учреждениях всех форм собственности вследствие все более возрастающего использования ими разнообразных средств компьютерной техники. Автоматизированные информационные системы начинают играть доминирующую роль (по сравнению с ручными) в обработке данных и осуществлении всех типов финансовых операций как внутри страны, так и в государственных контактах. В криминалистической литературе отмечается, что, как показывает практика борьбы с компьютерной преступностью в зарубежных странах, сегодня возможно с помощью манипуляций клавишами клавиатуры персонального компьютера в стране "А" получить необходимую информацию, хранящуюся в банке данных компьютерной системы страны "В", затем перевести ее в страну "С", достигнув при этом поставленной корыстной цели: путем осуществления незаконной транзакции похитить и присвоить денежные средства [64, с. 36]. Ярким примером этому может служить одно из уголовных дел, расследование которого осуществлялось отечественными правоохранительными органами в тесном контакте с правоохранительными органами США. Данное уголовное дело было возбуждено в отношении Л. и других граждан Российской Федерации, которые вступили в сговор на хищение денежных средств в крупных размерах, принадлежавших "City Bank of America", расположенного в г. Нью-Йорке (США). Образовав устойчивую преступную группу, они в период с июня по сентябрь 1994 г., используя электронную компьютерную систему телекоммуникационной связи InterNet и преодолев при этом несколько рубежей многоконтурной защиты от несанкционированного доступа (НСД), с помощью персонального компьютера стандартной конфигурации из офиса АО "С" находящегося в г. С.-П. (Россия), вводили в систему управления наличными фондами указанного банка ложные сведения. В результате чего преступниками было осуществлено не менее 40 переводов денежных средств на общую сумму 10 млн. 700 тыс. 952 долл. США со счетов клиентов названного банка на счета лиц, входящих в состав преступной группы, проживавших в шести странах: США, Великобритании, Израиля, Швейцарии, ФРГ, России. Так, например, в результате проведения первой транзакции было похищено 400 тыс. долл. США, которые поступили на счет К., контролировавшего деятельность двух коммерческих компаний в штате Калифорния (США) и являвшегося одновременно другом детства Л.

Из показаний свидетелей (сослуживцев и родственников) стало очевидно, что Л. является талантливым программистом и специалистом по компьютерной технике. Об этом наглядно свидетельствует тот факт, что при его непосредственном участии была разработана и внедрена на различных предприятиях С.-П. компьютерная система бухгалтерского учета, занявшая второе место по России на конкурсе аналогичных программных продуктов.

3 марта 1995 г. Л. вылетел к родственникам в Лондон, где по прибытии в аэропорт Хитроу был арестован правоохранительными органами Великобритании. В приведенном примере стоит, на наш взгляд, подчеркнуть следующую немаловажную деталь: состоявшийся в августе 1995 г. лондонский суд отложил принятие решения по делу Л. на неопределенный срок, поскольку в ходе судебного разбирательства было доказано (с помощью адвоката), что для получения доступа к счетам клиентов "Ситибанка" подсудимый использовал в качестве орудия совершения преступления компьютер, находящийся на территории России, а не на территории США, как требует того уголовное законодательство Великобритании. На основании вышеизложенного просьба американских и российских представителей о выдаче им Л. была судом отклонена (неудовлетворена). В итоге — правоохранительные органы США и России были лишены возможности завершить работу по раскрытию ряда преступлений, совершенных членами указанной преступной группы и арестованных в этих странах.

В настоящее время находит все более широкое применение межбанковская система электронных платежей и взаиморасчетов — компьютерная система электронной связи, которая, естественно, не может быть абсолютно надежной. Например, с 1993 г. только в Московском регионе функционирует автоматизированная система расчетов, объединяющая 500 банков г. Москвы и 120 банков Московской области. Этой системой, по оценкам специалистов, выполняется 40% всех банковских операций в России. Через всю эту финансовую сеть, имеющую развитую периферийную связь с различными финансовыми учреждениями и организациями (биржи, компании, коммерческие банки) других регионов, а также с Центральным банком России и его филиалами, в течение одних суток проходит около 2 тыс. документов, что приблизительно эквивалентно денежному потоку в 600 млрд. руб. [98, с. 16]. Складывающаяся ситуация привлекает преступников, которые, "взламывая" электронную защиту (а в некоторых звеньях этой системы она отсутствует вообще),

получают несанкционированный доступ к компьютерным банкам данных для совершения незаконных манипуляций в корыстных целях.

Приходится констатировать, что процесс компьютеризации общества приводит к увеличению количества компьютерных преступлений, возрастанию их удельного веса по размерам похищаемых сумм в общей доле материальных потерь от обычных видов преступлений. Этот факт подтверждается и данными проведенного нами исследования. Так, на вопрос анкеты о динамике роста количества компьютерных преступлений по мере компьютеризации российского общества, 92% опрошенных респондентов дали ответ: “будет увеличиваться”. Согласно же данным комиссии по предупреждению преступности и уголовному правосудию Организации Объединенных Наций, ежегодный экономический ущерб от компьютерных преступлений, по экспертным оценкам, исчисляется миллионами долларов США, причем многие потери не обнаруживают или о них не сообщают по причине высокой латентности (90%) преступлений данного вида. Ведь только объем операций при электронной передаче денежных средств указывает на то, что тенциальные потери выше, чем при тех же операциях с использованием бумажных документов [25, п. 22]. Потери же от „вно взятого государства в таких случаях за считанные минуты могут достигать колоссальных размеров. Один из характерных примеров — уголовное дело о хищении 125,5 тыс. долл. США и подготовке к хищению еще свыше 500 тыс. долл. во Внешэкономбанке СССР в 1991 г., рассмотренное московским судом. По материалам другого уголовного дела, в сентябре 1993 г. 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. 309 млн. 768 тыс. руб. Такие же факты имели место: в апреле 1994 г. из расчетно-кассового центра (РКЦ) г. Махачкалы на сумму 35 млрд. 1 млн. 557 тыс. 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. [21, с. 141; 44; 61].

Между тем в настоящее время в отечественной криминалистической науке все еще не существует четкого определения понятия компьютерного преступления, дискутируются различные точки зрения по их классификации. Сложность в формулировках этих понятий существует, на наш взгляд, как по причине невозможности выделения единого объекта преступного посягательства, так и множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны. Например, Ю.М. Батулин считает, что компьютерных преступлений как особой группы преступлений в юридическом смысле не существует, отмечая, однако, при этом тот факт, что многие традиционные виды преступлений модифицировались из-за вовлечения в них вычислительной техники и поэтому правильнее было бы говорить лишь о компьютерных аспектах преступлений, не выделяя их в обособленную группу преступлений [2, с. 129]. Другого, более определенного взгляда в этом вопросе, по нашему мнению, придерживается АЛ. Караханьян. Под компьютерными преступлениями он понимает противозаконные действия, объектом или орудием совершения которых являются электронно-вычислительные машины [71, с. 243]. Существуют и другие точки зрения по этому вопросу. Однако мы считаем, что ни одно из них в полной мере не отражает всех компонентов социального явления, которые имеются в действительности.

Исходя из анализа научных работ и публикаций отечественных и зарубежных исследователей по обозначенному кругу проблем, можно сделать обобщающий вывод о том, что в настоящее время существуют два основных течения научной мысли. Одна часть исследователей относит к компьютерным преступлениям действия, в которых компьютер является либо объектом, либо орудием посягательства. При этом, в частности, кража самих компьютеров рассматривается ими как один из способов совершения компьютерных преступлений. Исследователи же второй группы относят к компьютерным преступлениям только противозаконные действия в сфере автоматизированной обработки информации. Они выделяют в качестве главного классифицирующего признака, позволяющего отнести эти преступления в обособленную группу, общность способов, орудий, объектов посягательства [4]. Иными словами, объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства. Отметим, что законодательство многих стран, в том числе и в России, стало развиваться именно по этому пути.

Поскольку уголовное право исходит из материального, правового определения понятия преступления, то суть любого преступления состоит в том, что оно изменяет, разрывает конкретное общественное отношение, представляющее собой определенную связь людей по поводу материальных, социальных и идеологических ценностей, охраняемых уголовно-правовыми

нормами. При этом структура в системе любого общественного отношения всегда состоит из трех основных элементов:

- 1) участников (субъектов) общественного отношения;
- 2) предмета общественного отношения;
- 3) содержания отношения (связи между участниками отношения по поводу конкретного предмета общественного отношения), а уголовное законодательство всегда охраняет от причинения вреда только:

- 1) личность;
- 2) предметы, социальные, духовные ценности, блага;

3) социально полезную деятельность [53, с. 12]. Для установления объекта преступления из ряда общественных отношений выделяют то общественное отношение, которое охраняется уголовно-правовой нормой. Далее раскрывается содержание и значение каждого элемента его составляющего. Например, определяется круг субъектов отношений (субъективный состав), повод, предмет отношения и его содержание.

Для наиболее полного выявления качественных свойств объекта конкретных преступлений, роли и значения объекта, а также отражения объективно существующих в действительности различных общественных отношений выделяются три вида объектов преступления: общий объект, родового и непосредственный. Первый представляет собой совокупность общественных отношений, охраняемых нормами уголовного законодательства России, второй — совокупность охраняемых уголовно-правовыми нормами сходных (родственных), однородных по своему внутреннему содержанию, взаимосвязанных общественных отношений, которые в результате преступления подвергаются разрушению или общественно опасному вредному изменению, и третий — то конкретное общественное отношение (или их совокупность), на которое непосредственно посягает преступление [17].

Под предметом же преступления в уголовном праве понимаются все материальные предметы внешнего мира, на которые непосредственно направлены действия виновного при посягательстве на объект [53]. Иными словами, предмет преступного посягательства — это элемент объекта, воздействуя на который преступник нарушает или пытается нарушить само общественное отношение.

Следует заметить, что преступление часто изменяет предмет посягательства, и эти изменения можно установить.

Применительно к рассматриваемой нами проблеме, все вышеуказанное требует некоторого пояснения.

На наш взгляд представляется, что относительно объекта преступного посягательства двух мнений быть не может — им, естественно, является информация, а действия преступника следует рассматривать как покушение на информационные отношения общества. Далее необходимо учесть, что если информация является не объектом, а средством покушения на другой объект уголовно-правовой охраны, то здесь необходимо делать различия в том была ли это машинная информация, т. е. информация, являющаяся продуктом, произведенным с помощью или для компьютерной техники, либо она имела другой, “некомпьютерный” характер. Поэтому сразу оговоримся, что под машинной информацией нами понимается информация, циркулирующая в вычислительной среде, зафиксированная на физическом носителе в форме, доступной восприятию ЭВМ, или передающаяся по телекоммуникационным каналам: сформированная в вычислительной среде и пересылаемая посредством электромагнитных сигналов из одной ЭВМ в другую, из ЭВМ на периферийное устройство, либо на Управляющий датчик оборудования [38, с. 40]. В первом случае преступление должно относиться к категории компьютерных преступлений, во втором — к категории того вида преступных деяний, которые собственно и обозначены в уголовном законе. Здесь мы приходим к тому, что в криминологическом-криминалистическом плане понятие терминов “компьютерная преступность” и “компьютерное преступление” будет

значительно шире понятия компьютерного преступления, которое выделено в специальном разделе Уголовного кодекса Российской Федерации. Так, в главе 28 “Преступления в сфере компьютерной информации” определяются следующие общественно опасные деяния в отношении средств компьютерной техники.

1) Неправомерный доступ к охраняемой законом компьютерной информации, т. е. информации на машинном носителе, в электронновычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

2) Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

3) Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (машинной информации — автор)[92, с. 4].

Следует уточнить, что законодательством России охраняется три основных вида информации, которые одновременно подлежат защите, а именно:

1) сведения, отнесенные к государственной тайне соответствующим федеральным законом, под которыми на основании ст. 5 понимается информация в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которой может нанести ущерб безопасности России [29];

2) сведения, отнесенные к служебной и коммерческой тайне в соответствии со ст. 139 Гражданского кодекса России, под которыми понимается информация, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, если к ней нет законного доступа на законных (санкционированных) основаниях и обладатель такой информации принимает меры к охране ее конфиденциальности [20];

3) сведения, имеющие статус персональных данных, под которыми в соответствии со ст. 11 Федерального Закона “Об информации, информатизации и защите информации” понимается информация о гражданах, включаемая в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, органов местного самоуправления, а также получаемая и собираемая негосударственными организациями [31].

Итак, с точки зрения уголовно-правовой охраны под компьютерными преступлениями следует, по нашему мнению, понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть. При этом необходимо учитывать одну особенность, а именно” компьютер в преступлениях может выступать одновременно в качестве предмета и в качестве орудия совершения преступления. Указанное свойство компьютера определяется технологической спецификой его строения (архитектурой), под которой понимается концепция взаимосвязи элементов сложной структуры, включающей в себя компоненты логической, физической и программной структур [68, с. 27]. Это явление можно объяснить посредством следующего. Если в течение последних двадцати лет в практике широко использовались компьютеры 1-ГУ поколений (классификация вычислительных систем по степени развития аппаратных и программных средств, определяющееся элементной базой, архитектурой и вычислительными возможностями), предполагающие в архитектуре своего строения наличие “фон Неймановского” принципа “управления потоками команд” с помощью аппаратных средств, который позволял проводить разграничение между собственно аппаратными и программными ресурсами, то в последние годы начинают массово использоваться компьютеры V поколения, отличительной особенностью которых является уже наличие диаметрально противоположного принципа — искусственного интеллекта — “управления потоками данных” [68, с. 439-440]. Реализация этого принципа в строении компьютера уже не позволяет конкретно разграничить между собой

аппаратные и программные средства, так как последние технологически реализованы в аппаратных средствах посредством многократного усложнения на атомно-молекулярном уровне логических алгоритмов, представляющих собой топологию сверхбольших интегральных микросхем, т. е. зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы: микросхемного изделия окончательной или промежуточной формы, предназначенного для выполнения функций электронной схемы, элементы и связи которого нераздельно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие, и связей между ними (28, ст. 1;68,с. 201].

С криминалистической точки зрения, по нашему мнению, компьютерное преступление следует понимать в широком смысле этого слова. Так, в марте 1993 г. на заседании постоянно действующего межведомственного семинара “Криминалистика и компьютерная преступность”, организованного в рамках координационного бюро по криминалистике при Научно-исследовательском институте проблем укрепления законности и правопорядка Генеральной прокуратуры Российской Федерации и Экспертно-криминалистического центра МВД России была сделана попытка дать первое отечественное определение понятия “компьютерное преступление”. Согласно этому определению, под компьютерным преступлением следует понимать “... предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного посягательства [86, с. 37]. Это определение в большей степени соответствует действительному характеру рассматриваемого нами социального явления.

Подводя некоторые итоги, можно выделить следующие его характерные особенности:

- 1) неоднородность объекта посягательства;
- 2) выступление машинной информации как в качестве объекта, так и в качестве средства преступления;
- 3) многообразие предметов и средств преступного посягательства;
- 4) выступление компьютера либо в качестве предмета, либо в качестве средства совершения преступления.

Учитывая обозначенные особенности, представляется возможным сделать вывод, что под компьютерным преступлением следует понимать предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной (компьютерной) техники. (Не вдаваясь в полемику в настоящей работе по поводу юридической “чистоты” представленной нами дефиниции, отметим, что такой подход нами избирается исключительно с точки зрения криминалистических аспектов проблемы и, безусловно, в уголовно-правовом смысле неприемлем.) При этом в качестве основного классифицирующего признака принадлежности преступления к разряду компьютерных нами выделяется понятие “использование средств компьютерной техники”, независимо от того, на какой стадии преступления она использовалась: при его подготовке, в ходе совершения или для сокрытия. Границы применения этого термина достаточно широки и вместе с тем очень определены, что в конечном итоге приводит к универсальности самого определения компьютерного преступления. Для обоснования этого утверждения более детально рассмотрим его составляющие.

Первая часть определения, на наш взгляд, не требует особых пояснений и зависит лишь от того, как будут называться (квалифицироваться) те или иные общественно опасные действия согласно формулировкам уголовного закона. Например, шпионаж с использованием средств компьютерной техники будет называться компьютерным шпионажем и относится криминалистической наукой к компьютерным преступлениям (тогда как в уголовно-правовом плане это преступление будет отнесено к разряду государственных преступлений), аналогично: подлог — компьютерный подлог, мошенничество — компьютерное мошенничество, хищение — компьютерное хищение, злоупотребление — компьютерное злоупотребление и т. д. Считаем необходимым отметить, что подобные понятия очень часто употребляются в зарубежной юридической практике при квалификации тех или иных компьютерных правонарушений. Поэтому, по нашему мнению, возможно использование данной терминологии в отечественной практике для обозначения сходных по своему содержанию преступных деяний для выделения их криминалистической

специфики. Вторая же часть определения требует, на наш взгляд, серьезных объяснений и подробной детализации.

Средства компьютерной техники (ранее существовавшие, ныне существующие и будущие существовать по мере развития техники) по своему функциональному назначению представляется возможным подразделить на две основные группы:

1) аппаратные средства (HardWare);

2) программные средства (SoftWare).

Под аппаратными средствами компьютерной техники понимаются технические средства, используемые для обработки данных: механическое, электрическое и электронное оборудование, используемое в целях обработки информации. К ним относятся:

1) персональный компьютер (ПЭВМ или ПК) — комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач [68, с. 439, 440-442];

2) периферийное оборудование — оборудование, имеющее подчиненный кибернетический статус в информационной системе: любое устройство, обеспечивающее передачу данных и команд между процессором и пользователем относительно определенного центрального процессора; комплекс внешних устройств ЭВМ, не находящихся под непосредственным управлением центрального процессора [68, с. 225];

3) физические носители машинной информации. Под программными средствами компьютерной техники в соответствии со ст. 1 Закона Российской Федерации “О правовой охране программ для электронно-вычислительных машин и баз данных” понимаются объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения [27]. К ним относятся:

1) программное обеспечение; совокупность управляющих и обрабатывающих программ, предназначенных для планирования и организации вычислительного процесса, автоматизации программирования и отладки программ решения прикладных задач, состоящее из:

— системных программ (операционные системы, программы технического обслуживания; драйверы, программы-оболочки, вспомогательные программы — утилиты);

— прикладных программ (комплекса специализированных программ), предназначенных для решения определенного класса задач, например редакторы текстов, антивирусные программы и системы, программы защиты от несанкционированного доступа, табличные процессоры, СУБД, графические редакторы, системы деловой и научной графики, системы автоматизированного проектирования (САПР), интегрированные системы, бухгалтерские программы, программы управления технологическими процессами, автоматизированные рабочие места, (АРМ), библиотеки стандартных программ и т. п.;

— инструментальных программ (систем программирования), состоящих из языков программирования: Turbo C, Turbo C++, Turbo Pascal, Microsoft C, Microsoft Basic, Clipper и др., и трансляторов — комплекса программ, обеспечивающих автоматический перевод с алгоритмических и символических языков в машинные коды.

2) машинная информация владельца, пользователя, собственника в соответствии со ст. 2 Федерального Закона “Об информации...” [31].

Столь подробное структурирование средств компьютерной техники приводится нами в первую очередь для более четкого понимания в последующем сути рассматриваемых способов совершения компьютерных преступлений, предметов и орудий преступного посягательства, а также для устранения разногласий по поводу их терминологии, имеющих место в практической

деятельности органов внутренних дел при оформлении различных процессуальных документов. Например, когда предметом посягательства является компьютер, то необходимо рассматривать его как систему и проводить различие между ее частями. Ведь компьютер в узком смысле этого слова есть просто процессор, реализованный на базе интегральных микросхем например, но на практике он никогда в основном не используется самостоятельно, а только в сочетании с периферийными устройствами, нередко связанными в единую сеть, которая может включать в себя и другие компьютеры и компьютерные системы. Для любой ее части реальна угроза стать предметом или средством совершения преступления [2, с. 127, 128].

Программные средства можно рассматривать и как часть компьютерной системы, и как самостоятельный предмет, для которого компьютер является окружающей (периферийной) средой. Этот факт, по нашему мнению, должен устанавливаться программно-технической экспертизой, исходя из каждого конкретного случая (например, учитывая уровень архитектурного строения компьютера и отнесения его к тому или иному поколению ЭВМ, либо по другим основаниям).

После детального исследования основных компонентов, представляющих в совокупности содержание понятия компьютерного преступления и определение последнего в настоящей главе, мы можем перейти к рассмотрению вопросов, касающихся основных элементов криминалистической характеристики преступных посягательств рассматриваемого вида.

Глава 2

Криминалистическая характеристика компьютерных преступлений

В настоящее время в отечественной криминалистической науке не существует сколько-нибудь обобщенных данных для формирования понятий основных элементов криминалистической характеристики компьютерных преступлений. Как показывают проведенные нами исследования, 55% опрошенных респондентов не имеют об этих категориях ни малейшего понятия, а 39% — лишь частично знакомы с криминалистической характеристикой лиц, склонных к совершению компьютерных преступлений по ненаучным источникам, из которых 66% — средства массовой информации, 28% — кино- и видеофильмы (как правило зарубежного производства). И это при том, что в качестве респондентов выступали в основном начальники городских и районных отделов и управлений органов внутренних дел и их заместители (начальники следственных отделов), которые в первую очередь должны обладать именно научной информацией о том, с чем им приходится сталкиваться в своей непосредственной практической работе. Такое положение, естественно, нельзя признать положительным. Поэтому, на наш взгляд, весьма актуальной как с научной, так и с практической точек зрения, является разработка проблемы криминалистической характеристики рассматриваемых видов преступных деликтов.

Криминалистическая характеристика компьютерных преступлений отличается от уже известных криминалистической науке преступных посягательств определенной спецификой. По нашему мнению, в первую очередь в нее должны входить криминалистически значимые сведения о личности правонарушителя, мотивации и целеполагании его преступного поведения, типичных способах, предметах и местах посягательств, а также о потерпевшей стороне.

Как известно, личность преступника служит объектом криминологического исследования, и многие типологические данные о ней являются элементом криминологической характеристики преступлений. Однако рамки криминологического изучения личности преступника ограничиваются главным образом теми личностными особенностями, которые необходимы для использования в целях уголовной профилактики, предупреждения преступлений. Исследованию этих проблем уделено достаточно много внимания в криминологической литературе. Ряд личностных черт преступников остается за пределами криминологической характеристики. В первую очередь — это главным образом “профессиональные” навыки преступников, которые проявляются в основном в определенных способах и приемах совершения преступлений, оставляют на месте совершения преступления определенный “почерк” преступника: результаты каждой преступной деятельности содержат следы личности человека, ее осуществившей. Обнаруживаемые на месте совершения преступления вещественные улики проливают свет как на сведения о некоторых его личных социально-психологических свойствах и качествах, так и на сведения о его преступном опыте, профессии, социальных знаниях, поле, возрасте, особенностях взаимоотношений с потерпевшим и т. п. [67, с. 35].

Выявление всех возможных форм выражения личности, проявляющихся в первичной информации о событии преступления, в ходе его расследования, позволяет составить представление об общих, а затем и о частных особенностях преступника. Подобная информация, несомненно, имеет криминалистическое значение. Так, с научной точки зрения, существует четкая классификация криминалистически значимой информации, которая подразделяется по следующим основаниям: по источнику получения, по физической природе, по форме представления, по характеру структуры, по структурным элементам события преступления, по направлению движения и назначению, по процессуальному значению [70, с. 30]. Прослеживание связи этой информации с выявленными данными о способе, механизме и обстановке совершения преступления создает новую самостоятельную информацию, позволяющую правильнее определить направление и способы розыска, задержания и последующего изобличения преступника, т. е. избрать с учетом других сведений по делу оптимальные методы расследования. Поэтому данные о том, кто чаще всего совершает преступления исследуемого вида, хотя и носят выраженный криминологический характер, тем не менее используются и в криминалистической характеристике преступления.

Криминалистически значимые данные о личности преступника в настоящее время базируются на двух специфических группах информации. Первая из которых включает в себя данные о личности неизвестного преступника по оставленным им следам как на месте преступления, в памяти свидетелей, так и по другим источникам с целью установления направления и приемов его розыска и задержания. Чаще всего такая информация дает представление об общих свойствах какой-то группы лиц, среди которых может находиться преступник, и реже — о некоторых качествах конкретной личности. Такого рода сведения в целях быстрее выявления и розыска преступника должны сопоставляться с криминалистическими данными о том кто чаще всего совершает преступления расследуемого вида. Вторая же группа включает в себя информацию, полученную с помощью изучения личности задержанного подозреваемого или обвиняемого с целью исчерпывающей криминалистической оценки личности субъекта. В этих целях обычно собираются сведения не только о жизненной установке, ценностных ориентациях, дефектах правосознания, особенностях антиобщественных взглядов, но и о том, какая информация о личности субъекта преступления, его связях, особенностях поведения до, во время и после совершения преступления может помочь следователю или оперативному работнику найти с последним необходимый следственно-оперативный контакт, получить правдивые показания, помочь в его изобличении, а также выбрать наиболее действенные способы профилактического воздействия на него. Представляется, что эти данные с учетом информации о преступниках, учитываемой в других элементах криминалистической характеристики, могут быть положены в основу типизации преступников.

Выделение типовых моделей разных категорий преступников, знание основных черт этих людей позволяет оптимизировать процесс выявления круга лиц, среди которых целесообразно вести поиск преступника и точнее определить способы установления и изобличения конкретного правонарушителя. Например, в тех случаях, когда преступление совершается организованной преступной группой или сообществом, оно становится самостоятельным объектом криминалистического изучения и соответственно одним из элементов криминалистической характеристики данного преступления. При этом, как правило, изучаются особенности группы или сообщества с точки зрения степени их организованности, структуры, разветвленности, ролевых функций участников и др. Уяснение этих особенностей дает возможность лучше сориентироваться в направлениях розыска фактических данных, необходимых для раскрытия всех звеньев преступной деятельности членов этих формирований и всех основных эпизодов этой деятельности [106, с. 333].

Как уже отмечалось, сам факт появления компьютерной преступности в обществе многие исследователи отождествляют с появлением так называемых “хеккеров” (англ. “hacker”) — пользователей вычислительной системы (обычно сети ЭВМ), занимающихся поиском незаконных способов получения несанкционированного (самовольного) доступа к средствам компьютерной техники и данным в совокупности с их несанкционированным использованием в корыстных целях [10, с. 120; 66, с. 62]. Иногда в литературе и средствах массовой информации таких лиц называют “компьютерными”: “пиратами”, “мошенниками”, “ворами”, “электронными бандитами”, “одержимыми программистами”, “ворами с электронными отмычками” и т. д. и т. п. К хеккерам относятся увлеченные компьютерной техникой лица, преимущественно из числа молодежи — школьники и студенты, совершенствующиеся на взломах различных защитных систем СКТ. По последним оперативным данным, хеккеры в России объединены в региональные группы, издают свои электронные средства массовой информации (газеты, журналы, электронные доски со срочными объявлениями), проводят электронные конференции, имеют свой жаргонный словарь, который

постоянно пополняется и распространяется с помощью компьютерных бюллетеней, в которых также имеются все необходимые сведения для повышения мастерства начинающего — методики проникновения в конкретные системы и взлома систем защиты. Российские хеккеры тесно контактируют с зарубежными, обмениваясь с ними опытом по глобальным телекоммуникационным каналам [21, с. 142].

Все вышеуказанные названия в своей совокупности определяют понятие “компьютерного” преступника. Поэтому с криминалистической точки зрения характеристику его личности целесообразнее, на наш взгляд, считать понятием собирательным в широком смысле этого слова, хотя и с некоторым делением на самостоятельные обособленные группы по ряду оснований. Рассмотрим их более подробно.

К первой группе “компьютерных” преступников, на наш взгляд, можно отнести лиц, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности. По мнению некоторых авторов, эти субъекты воспринимают средства компьютерной техники как своеобразный вызов их творческим и профессиональным знаниям, умениям и навыкам [4]. Именно это и является в социально-психологическом плане побуждающим фактором для совершения различных деяний, большинство из которых имеют ярко выраженный преступными характер. По имеющимся у ФСБ, ФАПСИ и ФБР оперативным данным, российских хеккеров уже используют организованные преступные группы для проникновения в зарубежные и отечественные компьютерные системы [21, с. 143]. Под воздействием указанного выше фактора лицами рассматриваемой группы изобретаются различные способы несанкционированного проникновения в компьютерные системы, нередко сопровождающиеся преодолением постоянно усложняющихся средств защиты данных, что в свою очередь приводит к наращиванию алгоритма преступных действий и объективно способствует увеличению разнообразия способов совершения компьютерных преступлений. Следует подчеркнуть, что характерной особенностью преступников этой группы является отсутствие у них четко выраженных противоправных намерений. Практически все действия совершаются ими с целью проявления своих интеллектуальных и профессиональных способностей. Ситуация здесь условно сравнима с той, которая возникает при различного рода играх, стимулирующих умственную активность игроков, например при игре в шахматы. Когда в роли одного игрока выступает гипотетический преступник, а в роли его соперника — обобщенный образ компьютерной системы и интеллект разработчика средств защиты от несанкционированного доступа. Подробно данная ситуация исследуется в математической науке в теории игр — модели поведения двух противоборствующих сторон [22, с. 127, 128]. При этом различают антагонистические и неантагонистические игры, а также игры, в которых одной из сторон является человек, а другой — природа или ЭВМ. В последнем взаимодействии человека с компьютером осуществляется по определенному игровому алгоритму с целью обучения, тренировки, имитации обстановки и с развлекательными целями [68, с. 115]. Особый интерес в криминалистическом аспекте изучения личности преступника, на наш взгляд, представляют специалисты-профессионалы в области средств компьютерной техники. Обобщенные эмпирические данные позволяют нам обозначить следующую социально-психологическую характеристику этого круга лиц. Представители данной специальности обычно весьма любознательны и обладают незаурядным интеллектом и умственными способностями. При этом они не лишены некоторого своеобразного озорства и “спортивного” азарта. Наращиваемые меры по обеспечению безопасности компьютерных систем ими воспринимаются в психологическом плане как своеобразный вызов личности, поэтому они стремятся во что бы то ни стало найти эффективные способы доказательства своего превосходства. Как правило, это и приводит их к совершению преступления. Постепенно некоторые субъекты рассматриваемой категории не только приобретают необходимый опыт, но и находят интерес в этом виде деятельности. В конечном итоге происходит переориентация их целеполагания, которое из состояния “бескорыстной игры”, переходит в свое новое качество: увлечение заниматься подобной “игрой” лучше всего совмещать с получением некоторой материальной выгоды (в России, как это было отмечено нами выше, данная ситуация обостряется и стимулируется тяжелым материальным положением значительного числа граждан под воздействием определенных социально-экономических факторов). Это может проявляться у преступников как в открытой форме — в различных ситуациях при их общении с окружающими: знакомыми, друзьями, родственниками, сослуживцами, так и в закрытой — в форме внутренних мыслей и переживаний без каких-либо внешних проявлений. Последнее обычно присуще людям замкнутым по характеру, малообщительным. Другие же могут продемонстрировать перед знакомыми или сослуживцами, родственниками и другими свои умения найти незащищенные места в компьютерной системе, а иногда и то, как эти слабости можно

использовать в личных целях. Таким образом происходит развитие и перерождение “любителя-программиста” в профессионального преступника.

На наш взгляд, к числу особенностей, указывающих на совершение компьютерного преступления лицами рассматриваемой категории, можно отнести следующие:

- 1) отсутствие целеустремленной, продуманной подготовки к преступлению;
- 2) оригинальность способа совершения преступления;
- 3) использование в качестве орудий преступления бытовых технических средств и предметов;
- 4) непринятие мер к сокрытию преступления;

5) совершение озорных действий на месте происшествия. Ближе к рассматриваемой выше группе преступников можно отнести, как нам представляется, еще одну, включающую в себя лиц, страдающих новым видом психических заболеваний — информационными болезнями или компьютерными фобиями. Из-за новизны и специфичности этого явления, рассмотрим его более подробно. Исходя из данных научных исследований этой проблемы, можно выделить следующие ее составляющие, непосредственно связанные с рассматриваемой нами дефиницией. В специальной литературе отмечается, что указанная категория заболеваний вызывается систематическим нарушением информационного режима человека: информационным голодом, информационными перегрузками, сбоями темпоритма, неплановыми переключениями с одного информационного процесса на другой, дефицитами времени на настройку, информационным шумом. Изучением этих вопросов в настоящее время занимается новая, сравнительно молодая отрасль медицины — информационная медицина [97]. С позиции данной науки человек рассматривается как универсальная саморегулирующаяся информационная система с установленным балансом биологической информации. Нарушение последнего под воздействием внешних или внутренних дестабилизирующих факторов как врожденного, так и приобретенного в процессе жизни индивида характера (т. е. инстинктов и рефлексов), приводят к различного рода информационным болезням, среди которых наиболее распространены информационные неврозы. Иными словами, человек нуждается в равной степени как в физической, так и в информационной энергии (духовной или эмоциональной, как ее называли ранее). Когда ее мало — наступает информационный голод, когда ее много — человек страдает от информационных перегрузок (различного рода стрессов и эмоциональных срывов), приводящих при стечении определенных обстоятельств к аффективному состоянию. Помимо этого, человеку необходимо, чтобы информация поступала в определенном нормированном режиме, зависящем от индивидуальных особенностей и свойств личности. Информация должна быть также адаптирована к каждой конкретной личности. Сам человек при этом должен быть психологически готов к ее восприятию (априорная настройка), войти в процесс по ее обмену, обработке и фиксации (закрепления) — (апостериорная настройка) и постоянно выдерживать темпоритм. Нарушение одной из этих компонент информационного процесса приводит к потерям информации субъектом (нарушение памяти человека), преждевременной физической и умственной усталости и, в конечном итоге, перерастает в информационную болезнь [95, с. 43].

В настоящее время в связи с оснащением рабочих мест персональными компьютерами в целях повышения скорости протекания информационных процессов и эффективности использования рабочего времени, многие служащие попадают в различные стрессовые ситуации, некоторые из которых заканчиваются формированием компьютерных фобий. По существу, это есть не что иное, как профессиональное заболевание. Основные симптомы его проявления следующие: быстрая утомляемость, резкие скачкообразные изменения артериального давления при аудиовизуальном или физическом контакте со средствами компьютерной техники, повышенное потовыделение, глазные стрессы, головокружение и головные боли, дрожь в конечностях, затрудненность дыхания, обмороки и т. д. Как видно, в основе компьютерной фобии лежит страх перед потерей контроля над своими действиями. Ситуация здесь осложняется тем, что страдающие фобией обычно знают об иррациональности их страха, однако это делает его еще более сильным по принципу резонанса [2, с. 216].

По данным специальной комиссии Всемирной организации здравоохранения (ВОЗ), обобщившей все имеющиеся в ее распоряжении материалы о влиянии компьютерных терминалов на здоровье

пользователей, негативные последствия для здоровья человека при его частой и продолжительной работе с персональным компьютером очевидны и являются объективной реальностью [15;23].

Применительно к рассматриваемому нами вопросу необходимо выделить следующее: компьютерные преступления могут совершаться лицами, страдающими указанным видом психических заболеваний. По нашему мнению, при наличии подобных фактов в процессе раскрытия и расследования компьютерного преступления, необходимо обязательное назначение специальной судебно-психиатрической экспертизы лицом, производящим дознание или ведущим расследование по данному уголовному делу на предмет установления вменяемости преступника в момент совершения им преступных деяний. Это в свою очередь должно повлиять на квалификацию деяний преступника в случае судебного разбирательства (преступление, совершенное в состоянии аффекта или лицом, страдающим психическим заболеванием и т. д.).

На основании всестороннего анализа эмпирических данных [см.: 71, с. 251, п. 14] нами делается вывод о том, что компьютерные преступления, совершаемые преступниками рассматриваемой группы, в основном связаны с преступными действиями, направленными на физическое уничтожение либо повреждение средств компьютерной техники без наличия преступного умысла, с частичной или полной потерей контроля над своими действиями.

Третью и последнюю группу, выделяемую нами, составляют профессиональные “компьютерные” преступники с ярко выраженными корыстными целями, так называемые “профи”. В отличие от первой переходной группы “любителей” и второй специфической группы “больных”, преступники третьей группы характеризуются многократностью совершения компьютерных преступлений с обязательным использованием действий, направленных на их сокрытие, и обладающие в связи с этим устойчивыми преступными навыками. Преступники этой группы обычно являются членами хорошо организованных, мобильных и технически оснащенных высококлассным оборудованием и специальной техникой (нередко оперативно-технического характера) преступных групп и сообществ. Лиц, входящих в их состав, в большинстве своем можно охарактеризовать как высококвалифицированных специалистов, имеющих высшее техническое, юридическое, либо экономическое (финансовое) образование. Именно эта группа преступников и представляет собой основную угрозу для общества, является кадровым ядром компьютерной преступности как в качественном, так и в количественном плане. На долю именно этих преступников приходится максимальное число совершенных особо опасных посягательств, например до 79% хищений денежных средств в крупных и особо крупных размерах и различного рода должностных преступлений, совершаемых с использованием средств компьютерной техники [71, с. 253].

На основании вышеизложенного, а также с учетом анализа специальной литературы, обобщенную характеристику личности “компьютерного” преступника, данные которой в равной степени можно отнести к любой из трех рассмотренных нами групп, представляется возможным изложить следующим образом.

Возраст правонарушителей колеблется в широких (15-45 лет) границах: на момент совершения преступления возраст 33% преступников не превышал 20 лет, 13% — были старше 40 лет и 54% — имели возраст 20-40 лет. Большинство лиц данной категории составляют мужчины (83%), но доля женщин быстро увеличивается из-за профессиональной ориентации некоторых специальностей и профессий (секретарь, делопроизводитель, бухгалтер, контролер, кассир и т. д.). При этом размер ущерба от преступлений, совершенных мужчинами, в четыре раза больше, чем от преступлений, совершенных женщинами. По уровню специального образования диапазон также весьма широк — от высококвалифицированных специалистов до лиц, обладающих минимально необходимыми познаниями для работы в качестве пользователя. 52% преступников имели специальную подготовку в области автоматизированной обработки информации, а 97% — являлись служащими государственных учреждений и организаций, использующих компьютерную технологию в своих производственных процессах, а 30% из них имели непосредственное отношение к эксплуатации средств компьютерной техники. Зарегистрировано также несколько случаев, когда преступник вообще не имел никакого технического опыта и специальных познаний в этой области (в основном при хищении средств компьютерной техники, либо при фальсификации данных традиционными методами и способами). Большинство преступников (77%) при совершении преступления имели средний уровень интеллектуального развития, 21% — выше среднего и только 2% — ниже среднего, при этом, 40% преступников имели среднее специальное образование, 40% — высшее и 20% — среднее. С исследовательской точки зрения интересен и тот факт, что из каждой тысячи компьютерных преступлений только семь совершаются профессиональными программистами [51, с. 3].

В последнее время, как свидетельствует статистика, резко увеличивается количество преступлений, совершенных в составе организованных групп и сообществ за счет активного участия в них преступников третьей группы. Так, 38% преступников действовали без соучастников, тогда как 62% — в составе преступных групп [80]. В поведении преступников рассматриваемой группы, как правило, внешне не обнаруживается отклонений от принятых общественных норм и правил. По своему общественному положению большинство из них являются служащими, нередко занимающими ответственные руководящие посты и соответственно обладающие доступом либо к средствам компьютерной техники, либо к учету и распределению материальных ценностей и благ, либо и то и другое вместе. В этом случае необходимо отметить высокий удельный вес руководящих работников всех рангов (более 25%), обусловленный тем, что управляющим обычно является специалист более высокого класса, обладающий профессиональными знаниями, имеющий право отдавать распоряжения исполнителям и непосредственно не отвечающий за работу средств компьютерной техники (49, с. 19; 63, с. 13). Вместе с этим более высокий удельный вес руководящих работников среди совершивших хищения (23%) и более высокий процент преступлений, совершенных в составе организованной преступной группы (35%), характеризует компьютерные хищения как организованные и групповые преступления [71, с. 253]. К косвенным признакам представителя рассматриваемого нами социального типа можно отнести внимательность, бдительность, осторожность, оригинальность (нестандартность) мышления и поведения, активную жизненную позицию.

В профессионально-классификационном плане круг “компьютерных” преступников чрезвычайно широк. Обычно это различные категории специалистов и руководителей: бухгалтеры, кассиры, контролеры, табельщики, нормировщики, операторы бензозаправочных станций, программисты, инженеры, финансисты, банковские служащие, адвокаты, менеджеры, юристы, коммерческие директора, управляющие, начальники смен, отделов и служб и т. д. Всех их можно разделить на две основные группы, исходя из классифицирующего признака категории доступа к средствам компьютерной техники:

1) внутренние пользователи;

2) внешние пользователи, где пользователь (потребитель) — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею [31, ст. 2].

Пользователи бывают двух видов: зарегистрированные (санкционированные) и незарегистрированные (несанкционированные, незаконные).

По оценкам многих специалистов, основная опасность в плане совершения компьютерного преступления исходит именно от внутренних пользователей: ими совершается 94% преступлений, тогда как внешними пользователями — только 6%, при этом 70% — это клиенты-пользователи компьютерной системы, а 24% — обслуживающий персонал [Рассчитано по кн.: 71, с. 253; 14, с. 9; 82, с. 9; 99, с. 19]. Таких преступников нам представляется возможным условно разделить на три группы по основанию функциональной категории доступа к средствам компьютерной техники.

К первой группе мы считаем возможным отнести преступников, совершивших компьютерные преступления, основанные на использовании программных средств. В частности, к ним можно отнести: операторов ЭВМ, бухгалтеров, кассиров, расчетчиков, табельщиков, продавцов, операторов бензозаправочных и наливных станций, операторов периферийных устройств, администраторов баз и банков данных, библиотек программных средств, операторов-программистов (системных и прикладных), инженеров-программистов и др.

Ко второй группе, соответственно, нами относятся лица, совершившие компьютерные преступления, основанные на использовании аппаратных средств компьютерной техники. Среди них можно выделить: операторов средств связи, инженеров по терминальному оборудованию, специалистов по компьютерному аудиту, инженеров по электронному оборудованию, инженеров-связистов.

К третьей группе относятся лица, совершившие компьютерные преступления, основанные на косвенном доступе к средствам компьютерной техники, т. е. те, кто занимается организационно-управленческими вопросами: управлением компьютерной сетью или системой; руководством операторами; управлением базами и банками данных; руководством работ по программному

обеспечению; старшие (главные) инженеры, программисты, связисты и т. д.; руководители и начальники различных служб и отделов (информационно-аналитический и др.); сотрудники служб безопасности; менеджеры и т. д.

Преступниками из числа внешних пользователей, как свидетельствует практика, обычно бывают лица, хорошо осведомленные о деятельности потерпевшей стороны. Их круг настолько широк, что уже не поддается какой-либо систематизации и классификации: им может быть любой, даже случайный человек. Например, представитель организации, занимающейся сервисным обслуживанием, ремонтом, разработкой программных средств компьютерной техники на договорной основе, представители различных контролирующих и властных органов или организаций, клиенты и просто хакеры.

Рассмотрим теперь мотивы и цели совершения компьютерных преступлений, играющие, по нашему мнению, немаловажную роль в определении криминалистической характеристики преступлений рассматриваемой категории. Мотивы и цели совершения преступления напрямую связаны с социально-психологической и криминалистической характеристиками личности преступника. Обобщенные сведения о наиболее распространенных мотивах и целях совершения компьютерных преступлений являются одним из важнейших компонентов криминалистической характеристики преступления. Так, мотив и цель преступления, входящие в группу субъективных факторов, решающим образом влияют на выбор средств и приемов достижения цели, определяют характер основных действий преступника, а следовательно, и содержание способа совершения преступления, представляющего собой определенный комплекс волевых действий человека и являющегося стержневым основанием криминалистической характеристики любого преступного посягательства [35].

Мотив и цель в некоторых случаях являются необходимыми признаками субъективной стороны умышленных преступлений (например, корыстный мотив при злоупотреблении властью или служебным положением, цель похищения денежных средств при несанкционированном доступе к данным и т. д.). Встречаются составы, в которых мотив и цель включены в качестве квалифицирующих признаков (например, хулиганские побуждения при введении в компьютерную систему вируса и цель сокрытия другого преступления при квалифицированном хищении). Некоторые мотивы указаны в уголовном законе в качестве отягчающих и смягчающих обстоятельств (совершение преступления из корыстных или иных низменных побуждений, совершение преступления вследствие стечения тяжелых личных или иных семейных обстоятельств, под влиянием угрозы или принуждения, либо материальной, служебной или иной зависимости, совершение преступления в состоянии аффекта или невменяемости и т. д.). Во всех этих случаях к элементам уголовно-правовой характеристики преступлений относятся мотив и цель. Однако для большинства умышленных преступлений мотив и цель не являются необходимыми элементами субъективной стороны и, следовательно, не входят в уголовно-правовую характеристику. Между тем во всех случаях при расследовании конкретного преступления мотив и цель должны быть выяснены. Это имеет важное значение не только для определения судом справедливого наказания за содеянное, но и способствует полному раскрытию преступления. Сведения о наиболее распространенных мотивах и целях совершения любых, в том числе и компьютерных, преступлений используются при выдвижении версий относительно субъекта и субъективной стороны преступления, а также при организации целенаправленного поиска преступника. Например, следственная практика свидетельствует, что целью уничтожения или повреждения физических носителей машинной информации в ряде случаев является сокрытие хищений материальных ценностей или денежных средств. Поэтому при расследовании таких преступлений, совершенных, например, в банке, на бензоколонке, в учреждении или организации, деятельность которых связана с учетом, хранением или распределением материальных ценностей или денежных средств (как непосредственно, так и косвенно), где хранились уничтоженные или поврежденные физические носители машинной информации, проверка версии об их полном или частичном уничтожении с целью скрыть совершенное хищение, может навести на след преступников, способствовать полному раскрытию их преступной деятельности.

Исходя из результатов изучения зарубежных и отечественных исследователей по этому вопросу, в настоящее время можно выделить пять наиболее распространенных мотивов совершения компьютерных преступлений, расположенных нами в рейтинговом порядке:

1) корыстные соображения — 66% (совершаются в основном преступниками третьей группы, выделенной нами выше);

2) политические цели — 17% (шпионаж, преступления, направленные на подрыв финансовой и денежно-кредитной политики правительства, на дезорганизацию валютной системы страны, на подрыв рыночных отношений — совершаются исключительно преступниками третьей группы);

3) исследовательский интерес — 7% (студенты и профессиональные программисты из числа преступников первой группы);

4) хулиганские побуждения и озорство — 5% (хеккеры, преступники первой группы);

5) месть — 5% (преступники первой и второй групп) [48, с. 9; 57, с. 3-5].

На основании эмпирического исследования материалов конкретных уголовных дел, анализа литературных источников по данной проблеме нам представляется возможным выделить следующие наиболее типичные преступные цели, для достижения которых преступниками использовались средства компьютерной техники: подделка счетов и платежных ведомостей; приписка сверхурочных часов работы; фальсификация платежных документов; хищение наличных и безналичных денежных средств; вторичное получение уже произведенных выплат; перечисление денежных средств на фиктивные счета; отмыwanie денег; легализация преступных доходов (например, путем их дробления и перевода на заранее открытые законные счета с последующим их снятием и многократной конвертацией); совершение покупок с фиктивной оплатой (например, фальсифицированной или похищенной электронной кредитной карточкой); незаконные операции с сырьевыми и топливно-энергетическими ресурсами; незаконные валютные операции; незаконное получение кредитов; незаконные манипуляции с недвижимостью; получение незаконных льгот и услуг; продажа конфиденциальной информации; хищение материальных ценностей, товаров и услуг, топливно-сырьевых и энергетических ресурсов и т. п. и т. д. При этом, как правило, 52% преступлений связано с хищением денежных средств; 16% — с разрушением и уничтожением средств компьютерной техники; 12% — с подменой исходных данных; 10% — с хищением информации и программ и 10% — связано с хищением услуг (78, с. 91).

В заключение исследования этого вопроса отметим, что все действия компьютерного преступника обычно отличаются изощренностью и сопровождаются квалифицированной маскировкой. Однако заботятся о ней больше те преступники, чьи устремления направлены на обогащение или носят политический характер. Остальные же рассматривают средства компьютерной техники как “игрушку”, как предмет исследования и поэтому не ставят на первоначальном этапе своих действий преступных целей. Их больше всего заботит познавательная сторона дела — поиск эффективного способа нападения на средства компьютерной техники как на условного интеллектуального противника. Именно эти люди изобретают в большинстве своем новые способы совершения компьютерных преступлений, которыми затем на практике пользуются преступники третьей группы. Ближе к этим “разработчикам” примыкают преступники второй группы, характеризующиеся эмоциональной неустойчивостью и нарушением психики, вызываемыми работой с использованием средств вычислительной техники, и страдающие информационными болезнями. Их основной целью становится физическое полное или частичное уничтожение средств компьютерной техники, которая является для них объектом психического раздражения (условным раздражителем). Именно на его устранение и направлены действия преступника, нередко находящегося при этом в состоянии аффекта или невменяемости.

Существенную роль в структуре криминалистической характеристики компьютерных преступлений играют также обобщенные сведения о потерпевшей стороне. Криминалистически значимая информация подобного рода позволяет полнее охарактеризовать личность преступника, мотивы совершения преступления, рассмотренные нами выше, и соответственно помогает точнее очертить круг лиц, среди которых следует искать преступника, и планировать поисковые мероприятия по розыску важнейших доказательств по делу. В частности, выявление и изучение криминалистически значимых особенностей потерпевшей стороны и ее поведения (до, в момент и после совершения преступления) дают возможность глубже разобраться во многих обстоятельствах преступления, особенно указывающих на своеобразие, направленность и мотивы поведения преступника, его общие (типовые) и индивидуальные свойства. Это объясняется тем, что между преступником и потерпевшей стороной чаще всего прослеживается определенная взаимосвязь, в силу чего преступники обычно не случайно избирают их объектами своего преступного посягательства. Поэтому и неудивительно, что в преступлениях выявление преступника в значительной мере идет по цепи потерпевший — подозреваемый — обвиняемый. Особенно важно выявление и изучение этой связи в начале расследования.

Согласно данным международного комитета по компьютерной преступности, занимающегося исследованиями масштабов и видов компьютерных преступлений, а также правовыми аспектами борьбы с этим видом преступности, компьютерные преступления представляют собой серьезную угрозу для любой, располагающей компьютерной техникой организации, при этом наряду с высокой степенью риска ей наносится и значительный материальный ущерб. По существующим подсчетам, вывод из строя электронно-вычислительной системы в результате возникновения нештатной технической ситуации или преступления может привести даже самый крупный банк к полному разорению за четверо суток, а более мелкое учреждение — за сутки [64, с. 37].

Как показывает практика, в качестве потерпевшей стороны от компьютерных преступлений обычно выступает юридическое лицо. Это объясняется тем, что в настоящее время в России процесс компьютеризации охватил пока лишь различные учреждения, организации и предприятия всех форм собственности (т. е. юридических лиц), оставив при этом вне сферы своего влияния большинство населения страны (физических лиц) по причине достаточно высокой продажной цены средств персональной техники на внутреннем рынке. Для подавляющего большинства российских граждан персональный компьютер в настоящее время является недоступным. Поэтому компьютерная техника еще не получила своего широкого распространения в быту россиян. В то время как, например, почти треть американских домовладельцев имеют персональные компьютеры и у 11 млн. из них они оборудованы модемами (функциональными устройствами, обеспечивающими модуляцию и демодуляцию электромагнитных сигналов, т. е. преобразующими цифровые сигналы в аналоговую форму и обратно для передачи их по линиям связи — см.: 68, с. 206) для получения различных информационных услуг: электронной почты, связи с коллегами по работе, осуществления коммерческих сделок, проведения досуга и т. д. (90, с. 10]. Тем не менее мы считаем, что расширяющийся и набирающий силу процесс компьютеризации населения страны приведет в скором времени к появлению в качестве потерпевшей стороны от компьютерного преступления и физическое лицо, как это хорошо видно на примере зарубежных стран. На данном этапе мы лишь констатируем, опираясь на материалы конкретных уголовных дел отечественной практики, что потерпевшей стороной от компьютерных преступлений являются различного рода учреждения, предприятия и организации, имеющие статус юридического лица, поэтому нами используется термин “потерпевшая сторона”, а не “потерпевший”, под которым понимается лицо, которому преступлением причинен моральный, физический или имущественный вред [91, ст. 53].

В настоящее время исследователями выделяется три основные группы потерпевших сторон от компьютерных преступлений, исходя из прав собственности на компьютерную систему.

По данным Ю.М. Батурина, эти группы выглядят следующим образом:

- 1) собственники компьютерной системы составляют 79%;
- 2) клиенты, пользующиеся их услугами, — 13%;
- 3) третьи лица — 8% [2, с. 136).

Примечателен тот факт, что потерпевшая сторона первой группы, являющаяся собственником системы, неохотно сообщает (если сообщает вообще) в правоохранительные органы о фактах совершения компьютерного преступления. А поскольку они составляют большинство, а следовательно большинство и самих фактов совершения таких преступлений, то, по нашему мнению, именно этим и можно объяснить высокий уровень латентности компьютерных преступлений. Так, по оценкам ведущих зарубежных и отечественных специалистов, 90% компьютерных преступлений остаются необнаруженными или о них не сообщается в правоохранительные органы по различным причинам, а из оставшихся 10% обнаруженных и зарегистрированных преступлений раскрывается только каждое десятое (1%) [рассчитано по материалам: 71, с. 247; 45, с. 14; 47, с. 13; 51, с. 3; 105, с. 5; 99, с. 19]. При этом зарегистрированные компьютерные преступления обнаруживают следующим образом:

- 1) выявляются в результате регулярных проверок доступа к данным службами коммерческой безопасности — 31%;
- 2) устанавливаются с помощью агентурной работы, а также при проведении оперативных мероприятий по проверкам заявлений граждан (жалобам клиентов) — 28%;

- 3) случайно — 19%;
- 4) в ходе проведения бухгалтерских ревизий — 13%;
- 5) в ходе расследования других видов преступлений — 10%

[11, с. 6].

Специалистами выделяются следующие факторы, влияющие на решение потерпевшей стороны вопроса об обращении в правоохранительные органы по факту совершения компьютерного преступления [см.: 79, с. 5-6; 94; 2; 25, п. 22]:

- 1) некомпетентность сотрудников правоохранительных органов в вопросе установления самого факта совершения компьютерного преступления, не говоря уже о процессе его раскрытия и расследования. Это утверждение в равной мере относится к сотрудникам как российских, так и зарубежных правоохранительных органов;
- 2) учитывая, что в случае уголовного расследования убытки от расследования могут оказаться выше суммы причиненного ущерба, возмещаемого в судебном порядке, многие организации предпочитают ограничиваться разрешением конфликта своими силами, которые нередко завершаются принятием мер, не исключающих рецидив компьютерных преступлений. Обычно к лицам, допустившим совершение компьютерного преступления (а иногда ими являются и сами преступники) применяются меры дисциплинарного воздействия: их увольняют, переводят на нижеоплачиваемую работу, отказывают в предоставлении различных льгот и очередности на них, переводят в другие структурные подразделения, не связанные с доступом к средствам компьютерной техники, иногда это сопровождается взысканием причиненного материального ущерба с должностных лиц. Отказ от уголовного преследования в данном случае, по нашему мнению, свидетельствует о непонимании социальной опасности данных преступных деяний, что позволяет действительным преступникам уходить от уголовной ответственности, а другим, потенциальным, преступникам переходить от действий теоретического характера к их практическому осуществлению. Это приводит, в конечном итоге, к размыванию граней между законными и незаконными действиями;
- 3) боязнь подрыва собственного авторитета в деловых кругах и как результат этого — потеря значительного числа клиентов. Это обстоятельство особенно характерно для банков и крупных финансово-промышленных организаций, занимающихся широкой автоматизацией своих производственных процессов;
- 4) неминуемое раскрытие в ходе судебного разбирательства системы безопасности организации — нежелательно для нее;
- 5) боязнь возможности выявления в ходе расследования преступления собственного незаконного механизма осуществления отдельных видов деятельности и проведения финансово-экономических операций;
- 6) выявление в ходе расследования компьютерного преступления причин, способствующих его совершению, может поставить под сомнение профессиональную пригодность (компетентность) отдельных должностных лиц, что в конечном итоге приведет к негативным для них последствиям;
- 7) правовая и законодательная неграмотность подавляющего большинства должностных лиц в вопросах рассматриваемой нами категории понятий;
- 8) часто организации имеют весьма далекое представление о реальной ценности информации, содержащейся в их компьютерных системах. Обычно ценность определяется стоимостью ее создания или ее конкурентоспособностью, причем все чаще предпочтение отдается последнему. Диапазон содержащихся в ней данных простирается от производственных секретов и планов до конфиденциальной информации и списков клиентов, которые преступник может использовать с целью шантажа или в других преступных целях. Эта информация имеет различную ценность для собственника и того лица, которое пытается ее получить. (Непосредственная стоимость информации оценивается и с учетом затрат на ее сбор, обработку и хранение, а также рыночной

ценой,! В то же время на нее влияют и некоторые обстоятельства, связанные с совершением компьютерных преступлений. Если данные похищены или уничтожены (частично или полностью), убытки будут включать в себя неполученные доходы и услуги, стоимость восстановления информации, потери от взаимных ошибок при этом и т. д. [104, с. 29]. В дальнейшем похищенная информация может использоваться для различных целей, в том числе и против собственника, например с целью понижения его конкурентоспособности (что приводит к еще большему возрастанию общих убытков) либо с целью совершения вымогательства. Средства компьютерной техники, в частности компьютерная система, иногда используются преступником и как инструмент посягательства на другие объекты, например как средство воздействия на администрацию с целью повышения по службе. Так, в августе 1983 г. на Волжском автомобильном заводе в г. Тольятти следственной бригадой Прокуратуры РСФСР был избощлен программист, который из мести к руководству предприятия умышленно внес изменения в программу электронно-вычислительной машины, обеспечивающей заданное технологическое функционирование автоматической системы подачи механических узлов на главный сборочный конвейер завода. В результате произошел сбой в работе данного конвейера и заводу был причинен существенный материальный ущерб: 200 легковых автомобилей марки "ВАЗ" не сошло с конвейера, пока программисты не выявили и не устранили источник сбоев, что эквивалентно 1 млн. руб. в ценах 1983 г. Программист был привлечен к уголовной ответственности. В ходе судебного разбирательства судья и народные заседатели испытывали немалые затруднения. Подсудимый обвинялся по ст. 98 ч. 2 Уголовного кодекса РСФСР "Умышленное уничтожение или повреждение государственного или общественного имущества... причинившее крупный ущерб". При этом обвиняемый и его адвокат утверждали, что ничто натурально повреждено не было — поврежденным оказался лишь порядок работы, т. е. действия, не подпадающие ни под одну статью действующего уголовного законодательства. С исследовательской точки зрения интересен приговор суда: "три года лишения свободы условно; взыскание суммы, выплаченной рабочим за время вынужденного простоя главного конвейера; перевод на должность сборщика главного конвейера [94, с. 44].

Наконец, там, где средства компьютерной техники используются для осуществления финансовых и экономических операций, перед правонарушителями открываются широкие возможности для совершения различных преступных посягательств, которые будут рассмотрены нами далее. Считаем необходимым подчеркнуть, что нами со всей определенностью осознается тот факт, что все рассмотренные выше элементы криминалистической характеристики компьютерных преступлений не в полной мере раскрывают содержание последней, а приводимый перечень элементов криминалистической характеристики не является исчерпывающим. Вместе с тем, учитывая специфику рассматриваемого вида преступных деликтов, мы считаем возможным акцентировать внимание именно на отмеченных элементах. Более того, поскольку такой элемент криминалистической характеристики как способ совершения преступления, на наш взгляд, является ее стержневой основой, мы уделяем его исследованию более пристальное внимание и выделяем в самостоятельную главу в настоящей работе.

Глава 3

Способы совершения компьютерных преступлений

Важнейшим и определяющим элементом криминалистической характеристики любого, в том числе и компьютерного, преступления является совокупность данных, характеризующих способ его совершения.

Изучением этой проблемы в отечественной криминалистической науке занимались многие исследователи, например Н.П. Яблоков, И.Ф. Герасимов, Г.Г. Зуйков, И.Ф. Пантелеев, А.Ф. Савкин и др. Среди научных работ нами особо выделяется диссертационное исследование на соискание ученой степени доктора юридических наук профессора Г.Г. Зуйкова по теме: "Криминалистическое учение о способе совершения преступления" [35]. Лежащие в основе этого учения утверждения автора о детерминированности (совпадении детерминирующих факторов) и повторяемости способов совершения преступления, выраженные в высказывании о том, что "повторяемость способов как объективное явление действительности представляет собой проявление закономерной связи и взаимозависимости явлений", а также ряд других утверждений послужили прочным научным базисом для нашего исследования в вопросе изучения способов совершения компьютерных преступлений.

Под способом совершения преступления в криминалистическом смысле обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после

совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и соответственно определить наиболее оптимальные методы решения задач раскрытия преступления [106, с. 327]. Иными словами, способ совершения преступления складывается из комплекса специфических действий правонарушителя по подготовке, совершению и маскировке преступления. Во многих случаях эти действия представляют собой целую систему со многими ее элементами и оставляют во внешней обстановке соответствующие отражения, представляющие в информационном плане своеобразную модель преступления.

Как всякий акт человеческого поведения, преступление в целом и способы его осуществления определяются взаимодействием многих причин и условий, оказывающих влияние как прямо, так и опосредованно. Поэтому способ совершения преступления всегда является результатом совокупного действия значительного числа факторов. И чем больше будут они проявляться в действиях, тем больше следов будет оставлять преступник, тем большей информацией будет располагать следователь для выдвижения следственных и розыскных версий. Применительно к рассматриваемой нами проблеме наибольшую ценность будут представлять следы, указывающие на то, каким образом преступник осуществил следующее: попал на место преступления, ушел с него, преодолел различного рода преграды, использовал свое служебное положение, выполнил намеченную преступную цель, какие навыки, знания и физические усилия применил, пытался (или не пытался) скрыть следы совершенного деяния. Не менее существенны следы, свидетельствующие о характере связи преступника с предметом преступного посягательства, и др.

Именно такого рода признаки, проявляющиеся вовне, и позволяют создать основу для наиболее быстрого распознавания в процессе первоначальных следственных действий по делу того или иного характерного способа совершения расследуемого преступления даже по его отдельным признакам. Это соответственно дает возможность точнее определить направление и методы выявления остальных недостающих данных о предполагаемом способе совершения преступления и преступнике в целях быстрого раскрытия расследуемого преступления. При этом, с криминалистической точки зрения, важно не только выявить все внешние проявления, но и установить, что в нем было заранее заготовлено правонарушителем, а что явилось результатом приспособления к сложившейся на момент преступления внутренней и внешней обстановке (7, с. 243]. Это связано с тем, что сам факт и характер вносимых в заранее продуманный способ совершения преступления корректив также содержит существенную информацию о степени осведомленности преступника в той обстановке, которая сложилась к моменту преступного деяния, о привычках, навыках, наличии преступного опыта, некоторых физических, интеллектуальных, профессиональных и иных особенностях субъекта этого деяния.

Как известно, способ совершения преступления является в ряде составов необходимым элементом объективной стороны преступления и входит в его уголовно-правовую характеристику, а иногда служит и квалифицирующим обстоятельством. Некоторые способы совершения преступления, хотя и не предусмотренные в качестве квалифицирующих обстоятельств, всегда играют роль обстоятельств, отягчающих или смягчающих ответственность виновного. Во многих случаях способ совершения преступления, не указанный в тексте той или иной статьи Уголовного кодекса Российской Федерации, учитывается судом при избрании конкретной меры наказания и, следовательно, имеет уже уголовно-правовое значение и является элементом уголовно-правовой характеристики преступления. Отсюда видно, что характеристика способа совершения преступления не исчерпывается его уголовно-правовым значением, так как в уголовно-правовой характеристике способ совершения преступления представлен в общем виде, например способ открытого или тайного похищения, проникновение в помещение и т. д., и для нее безразличны приемы тайного похищения, конкретные способы проникновения в помещение, используемые при этом технические средства, источник их получения и т. д. В этом случае мы имеем дело уже с криминалистической характеристикой способа совершения преступления.

Структура способа совершения преступления как в криминалистическом, так и в уголовно-правовом смысле — категория непостоянная. В зависимости от своеобразия поведения преступника, ситуаций, возникающих до и после совершения преступления, и иных обстоятельств, она может быть трех видов:

- 1) трехзвенной (включающей поведение субъекта до, во время и после совершения преступления);
- 2) двухзвенной (в различных комбинациях);

3) однозвенной (характеризовать поведение субъекта лишь во время самого преступного акта) [106, с. 328].

Помимо этого, с криминалистической точки зрения, способ совершения преступления всегда конкретен и у него имеется немало таких граней, которые имеют важное следственно-оперативное значение. Среди них можно выделить следующие: распространенность данного способа, конкретные приемы его применения, используемые при этом технические и иные средства, их конструктивные особенности, методы использования при подготовке и исполнении преступления, а также сведения о том, как подготавливается преступление, каким образом проводятся тренировки, как и где изготавливаются или приспособляются необходимые орудия и другие технические средства совершения преступления, каковы источники их получения, какие недостатки в их учете и хранении облегчили доступ к ним преступных элементов, какие технологические процессы, оборудование, материалы использовались для их изготовления, каким образом они применялись при совершении преступления, и т. д. — все это входит в понятие криминалистической характеристики способов совершения преступления [67, с. 33].

В настоящее время в отечественной и зарубежной криминалистической науке не существует сколько-нибудь определенных понятий в вопросах характеристики способов совершения компьютерных преступлений, их конкретных названий и классификации. Эта проблема настолько нова для науки, что находится пока лишь в стадии осмысления и теоретических разработок. Особенно это касается отечественной криминалистической науки, которая всерьез стала заниматься этими вопросами лишь с начала 90-х гг., тогда как зарубежные исследователи — с конца 70-х гг. [86 и 32, с. 36]. У наших зарубежных коллег в этом плане уже имеется ряд ценных, с научной и практической точек зрения, разработок, которые, по нашему мнению, необходимо использовать при изучении и решении аналогичных вопросов в отечественной криминалистической науке с учетом определенных объективных и субъективных поправок и приближений, диктуемых реальностью функционирования и развития нашего общества, его политическими, правовыми, социальными и экономическими составляющими.

Такое почти двадцатилетнее отставание отечественной криминалистической науки от зарубежной в вопросах исследования компьютерных преступлений обусловлено, на наш взгляд, рядом объективных причин, одной из которых является сам факт появления компьютерных преступлений, целиком и полностью зависящий от уровня информатизации общества. Например, первое компьютерное преступление было зарегистрировано в США уже в 1966 г., тогда как у нас — только в 1979 г. [2, с. 126]. Здесь отмечается тот же 20-летний временной интервал отечественного “отставания”, который совпадает в этом плане и с временными рубежами начала процесса бурной компьютеризации.

В настоящее время, как это отмечалось нами выше, в юридической литературе существуют различные точки зрения в вопросах выделения, классификации и названия способов совершения компьютерных преступлений. Например, в июне 1983 г. Министерством здравоохранения США для Комитета по науке и технике конгресса был подготовлен доклад на тему: “Компьютерные преступления и правонарушения в правительственных учреждениях”, в котором исследователями было выделено 17 основных способов совершения компьютерных правонарушений [71, с. 251].

В основу доклада был положен опрос респондентов о всех случаях компьютерных мошенничеств и злоупотреблений, совершенных в период времени с 1 января 1978 г. по 31 марта 1982 г. Под компьютерным мошенничеством авторами доклада понималось любое незаконное умышленное действие (или ряд действий) с целью искажения данных для получения выгоды, если оно совершалось посредством манипулирования процессами ввода и передачи данных, коммуникациями, операционной системой и оборудованием. Компьютерным злоупотреблением авторы доклада считали правонарушение, включающее в себя неправомерное использование, уничтожение, изменение обрабатываемых информационных ресурсов. Респондентами опроса являлись 12 федеральных учреждений США, среди которых, в частности, были министерства обороны, энергетики, финансов, юстиции. Из 215 актов опроса 43 были исключены, т. к. они не содержали в себе компьютерных правонарушений, а остальные 172 составляли 69 мошенничеств и 103 злоупотребления, исходя из их определений, приведенных нами выше [71, с. 250].

Как видно из вышеизложенного, подавляющее большинство хищений совершается путем манипулирования входными и выходными данными, а также созданием несанкционированных файлов. В 70% случаев хищений установлено использование нескольких способов одновременно.

При злоупотреблениях наиболее часто правонарушителями использовались следующие способы: введение несанкционированных данных, создание несанкционированных файлов, программирование для личных целей. Наиболее распространенной формой является кража машинного времени. Как и при хищениях, в большинстве случаев злоупотреблений (в 78% случаев) применялось сочетание различных способов [71, с. 250].

В связи с отсутствием аналогичных отечественных статистических данных по рассматриваемому кругу вопросов мы считаем возможным с определенной степенью условности оперировать приведенными выше данными зарубежных исследований применительно к отечественной практике. Тем более, что материалы конкретных уголовных дел подтверждают правоту зарубежных коллег.

На основе анализа конкретных уголовных дел по преступлениям, совершенным с использованием средств компьютерной техники, а также всестороннего изучения специальной литературы нами выделяется свыше 20 основных способов совершения компьютерных преступлений и около 40 их разновидностей, число которых постоянно увеличивается по причине использования преступниками различных их комбинаций и логической модификации алгоритмов. Данное явление обусловлено как сложностью самих средств компьютерной техники, так и разнообразием и постоянным наращиванием выполняемых информационных операций, многие из которых отражают движение материальных ценностей, финансовых и денежных средств, научно-технических разработок и т. д., предопределяющих объект, предмет и орудие преступления. Немаловажным здесь является и факт специфичности самих средств вычислительной техники, участвующих в информационных процессах, выраженный в их двойственности: и как предмет, и как средства совершения преступного посягательства.

В то же время следует подчеркнуть, что практически все способы совершения компьютерных преступлений имеют свои индивидуальные, присущие только им признаки, по которым их 1 можно распознать и классифицировать в отдельные общие группы. Как правило, их основой являются действия преступника, направленные на получение различной степени доступа к средствам компьютерной техники. В большинстве своем, все эти действия сопровождаются весьма квалифицированными и хитроумными способами маскировки, что само по себе затрудняет процесс выявления, раскрытия и расследования преступления. Исследование показало, что в большинстве случаев преступниками используются различные количественные и качественные комбинации нескольких основных способов, имеющих достаточно простой алгоритм исполнения и хорошо известных отечественной юридической практике по традиционным видам преступлений. По мере их модификации и постоянного усложнения логических связей появляются все новые и новые способы, отличительной особенностью которых является уже наличие сложных алгоритмов действий преступника, которые из преступления в преступление все более совершенствуются и модернизируются. Происходит как бы их “естественный отбор”. Именно по этому принципу и будет построено наше дальнейшее исследование.

Все способы совершения компьютерных преступлений нами классифицируются в пять основных групп. При этом в качестве основного классифицирующего признака выступает метод использования преступником тех или иных действий, направленных на получение доступа к средствам компьютерной техники с различными намерениями. Руководствуясь этим признаком, мы выделили следующие общие группы (здесь и далее по тексту нами используется методологический подход Ю.М. Батурина в части, во-первых, некоторых терминологических выражений и, во-вторых, ряда предложенных им классификаций — см.: 2, с. 138—159):

- 1) изъятие средств компьютерной техники (СКТ);
- 2) перехват информации;
- 3) несанкционированный доступ к СКТ;
- 4) манипуляция данными и управляющими командами;
- 5) комплексные методы.

Рассмотрим их более подробно. ” К первой группе нами относятся традиционные способы совершения обычных видов (“некомпьютерных”) преступлений, в которых действия преступника

направлены на изъятие чужого имущества. Под чужим имуществом в данном случае понимаются средства компьютерной техники, подробно классифицированные нами в первой главе работы. С уголовно-правовой точки зрения подобные преступные деяния будут квалифицироваться соответствующими статьями Уголовного законодательства, например шпионаж, хищение, разбой, вымогательство, присвоение найденного или случайно оказавшегося у виновного чужого имущества, мошенничество и т. п. Характерной отличительной чертой данной группы способов совершения компьютерных преступлений будет тот факт, что в них средства компьютерной техники будут всегда выступать только в качестве предмета преступного посягательства, а в качестве орудия совершения преступления будут использоваться иные инструменты, технические устройства и приспособления (или без их использования), не являющиеся средствами компьютерной техники. Например, по материалам уголовного дела, расследованного следственным отделом ГУВД г. В. Волгоградской области, возбужденного по факту кражи чужого имущества, было установлено, что 3 мая 1994 г. в 3.00 неизвестные лица, перепилив с помощью ножовки по металлу прутья оконных металлических решеток, проникли в необорудованный охранной сигнализацией операционный зал государственного Сбербанка, откуда похитили два системных блока персональных компьютеров стандартной модификации типа IBM PC/AT-386 и PC/AT-286, содержащих в своей постоянной памяти банк данных на всех вкладчиков Сбербанка, физических и юридических лиц, кредиторов с полными установочными данными, зафиксированными электромагнитным способом на жестком магнитном диске (винчестере). Как видно из приведенного примера, способ совершения компьютерного преступления достаточно прост и традиционен. Именно подобные ему способы совершения компьютерных преступлений и относятся нами к рассматриваемой группе. К ней, в частности, мы относим и различные способы совершения преступлений, связанных с противоправным изъятием различных физических носителей ценной информации: магнитных лент и дисков, оптических и магнитооптических дисков, электронных кредитных карточек, электронных акций, услуг и т. п. Например, 5 декабря 1994 г. в г. Красноярске из НИИ "Биофизика" преступниками был похищен магнитный диск (дискета), на котором находилась медицинская программа по иммунологии, оцениваемая специалистами в 720 тыс. долл. США [60, с. 1].

Данные способы совершения преступлений достаточно полно изучены отечественной криминалистической наукой и мы считаем нецелесообразным их подробное рассмотрение в работе, т. к. это будет выходить за рамки выделенной нами темы.

Рассмотрим более подробно остальные группы способов совершения компьютерных преступлений, являющие собой неисследованную область отечественной криминалистической науки. В связи с этим считаем необходимым подчеркнуть, что особую научную ценность, на наш взгляд, при исследовании данного вопроса представляют положения о структуре и содержании способов совершения компьютерных преступлений, предложенные Батуриным Ю.М. [см.: 2, с. 138-159; 4, с. 11-22]. Поэтому, мы считаем возможным далее по тексту настоящей работы использовать его лексический перевод оригиналов названий способов с английского языка, которые наиболее часто применяются в международной юридической практике, а также подвергнуть некоторой детализации и конкретизации содержание предложенных автором дефиниций, дополнив их по некоторым позициям с целью придания им криминалистического значения.

" Ко второй группе нами относятся способы совершения компьютерных преступлений, основанные на действиях преступника, направленных на получение данных и машинной информации посредством использования методов аудиовизуального и электромагнитного перехвата, широко практикуемых в оперативно-розыскной деятельности правоохранительных органов. Отметим, что в этой и последующих рассматриваемых нами группах средства компьютерной техники будут выступать как в качестве предмета, так и в качестве орудия совершения преступного посягательства.

1. Непосредственный (активный) перехват. Осуществляется с помощью непосредственного подключения к телекоммуникационному оборудованию компьютера, компьютерной системы или сети, например линии принтера или телефонному проводу канала связи, используемого для передачи данных и управляющих сигналов компьютерной техники, либо непосредственно через соответствующий порт персонального компьютера. В связи с этим различают:

1) форсированный перехват (wilful intercept), представляющий собой перехват сообщений, направляемых рабочим станциям (ЭВМ), имеющим неполадки в оборудовании или каналах связи;

2) перехват символов (character seize) — выделение из текста, набираемого пользователем на клавиатуре терминала, знаков, не предусмотренных стандартным кодом данной ЭВМ;

3) перехват сообщений (message wiretapping) — несанкционированное подключение специального терминала к линии связи, прием и использование сообщений, циркулирующих между абонентскими пунктами и ЭВМ [68, с. 267].

Подключение осуществляется с помощью использования бытовых средств и оборудования: телефона, отрезка провода, составляющих телефонного кабеля, компьютерного полипроводного шлейфа, зажимов типа “крокодил”, специальных щупов-игл от контрольно-измерительной аппаратуры (в т. ч. и для прокалывания изоляционного слоя), набора радиомонтажных инструментов, кассетного портативного магнитофона, принтера, модема, либо персонального компьютера типа “Laptop” в блокнотном и субблокнотном исполнении.

После подключения к каналу связи, вся информация записывается на физический носитель или переводится в человеко-читаемую форму посредством бытовой или специальной радиоэлектронной аппаратуры [89, с. 13].

В качестве специальной аппаратуры преступниками могут использоваться:

а) компьютеризированные анализаторы проводных линий связи типа РК-1155, обеспечивающие программируемую последовательность записи перехватываемой информации, совместимые с любой проводной телефонной системой и позволяющие одновременно прослушивать до 256 линий связи [40, с. 52];

б) многофункциональный цифровой регистратор сигналов типа MSR (Multi Signal Regustrator), представляющий собой современную систему сбора и обработки телефонных и радиопереговоров, построенную на основе новейших информационных технологий — обычный персональный компьютер, реализованный на базе платформы Intel с использованием платы обработки сигналов на основе процессора ADSP с 16-канальным автоматическим цифровым преобразователем и выполненный в мультимедийном конструктиве LV-8000 со встроенными колонками Sound Blaster. Интересны следующие тактико-технические данные спецкомпьютера:

— программное обеспечение работает в режиме реального времени под управлением стандартной операционной системы MS-DOS;

— обеспечивается длительный непрерывный перехват речевой, факсимильной и цифровой информации по 4-8-16-32 каналам проводной и радиосвязи (“на выбор”) с последующей ее автоматической фильтрацией (удалением шумов и фона), распознаванием (идентификацией голоса), обработкой и архивированием [87, с. 771].

2. Электромагнитный (пассивный) перехват. Не все перехватывающие устройства требуют непосредственного подключения к системе. Данные и информация могут быть перехвачены не только в канале связи, но и в помещениях, в которых находятся средства коммуникации, а также на значительном удалении от них. Так, без прямого контакта можно зафиксировать и закрепить на физический носитель электромагнитное излучение, возникающее при функционировании многих средств компьютерной техники, включая и средства коммуникации [50, с. 4]. Это физическое явление привлекает особо пристальное внимание специалистов различных профессий из-за все более широкого применения компьютерных систем обработки данных. Ведь работа всех без исключения электронных устройств сопровождается электромагнитным излучением, в результате чего в различных электронных приемных устройствах возникают нежелательные помехи.

Электронно-лучевая трубка, являющаяся центральным элементом компьютерного устройства для видеоотображения информации на экране (дисплее) излучает в окружающее пространство электромагнитные волны, несущие в себе определенную информацию, данные (“электронный смог”) [23, с. 5]. Волны, излучаемые этим прибором, примерно так же, как при телевизионном вещании, проникают сквозь различные физические преграды с некоторым коэффициентом ослабления, например через стекло оконных проемов и стены строений, а принимать их можно, как показывают данные многочисленных экспериментов, на расстоянии до 1000 м. Как только эти сигналы приняты соответствующей аппаратурой и переданы на другой компьютер (преступника), можно получить изображение, идентичное изображению, возникающему на мониторе

“передающего” компьютера, для чего достаточно настроиться на его конкретную индивидуальную частоту. Каждый компьютер возможно идентифицировать по конкретным параметрам: рабочей частоте, интенсивности электромагнитного излучения и т. д. Так, благодаря излучению дисплейных терминалов, можно считывать с них данные при помощи различных технических средств, приобретаемых преступником как легальным путем, так и с использованием различных способов совершения преступлений, в том числе и выделенных нами в первой группе. Например, для осуществления преступных целей иногда достаточно смонтировать приемную антенну по типу волнового канала и имеющую более острую, чем у обычной дипольной антенны, несимметричную диаграмму направленности. После чего разработать (или использовать готовую) программу расшифровки “снятых” данных. Изготовление и подбор указанных орудий подготовки преступления могут быть осуществлены любыми лицами, имеющими средний профессиональный уровень подготовки по соответствующим специальностям.

Впервые дистанционный перехват информации с дисплея компьютера открыто был продемонстрирован в марте 1985 г. в Каннах на Международном конгрессе по вопросам безопасности ЭВМ. Сотрудник голландской телекоммуникационной компании РТТ Вим-Ван-Эк шокировал специалистов тем, что с помощью разработанного им устройства из своего автомобиля, находящегося на улице, “снял” данные с экрана дисплея персонального компьютера, установленного на восьмом этаже здания, расположенного в ста метрах от автомобиля [88, с. 37].

При совершении компьютерного преступления указанным способом преступниками в ходе осуществления криминальной “операции” используются приемы и методы оперативно-розыскной деятельности, в том числе и специальная техника. Например, различные сканирующие устройства, функционирующие на базе приемников электромагнитных сигналов типа AR-3000A, ICOM 7100/9000 и STABO XR-100 зарубежного производства, позволяющие принимать и демодулировать радиосигнал в широком диапазоне частот (стоимостью около 400 долл. США) [40, с. 54].

С исследовательской точки зрения интересен тот факт, что специалистам во время практических экспериментов удавалось принимать информацию одновременно с 25 дисплейных терминалов, расположенных в непосредственной близости друг от друга и разделять (сортировать) данные, выведенные на каждый экран из общего “электронного шума”. По мнению экспертов, теоретически возможно извлекать данные одновременно даже с 50 терминалов [3, с. 35]. Иногда преступники подключают к своему телевизионному приемнику видеомагнитофон (в обычном бытовом или портативном варианте исполнения), который позволяет им зафиксировать и накопить необходимую информацию на физическом носителе с целью ее дальнейшего анализа в стационарных условиях.

3. Аудиоперехват или снятие информации по виброакустическому каналу. Данный способ совершения преступления является наиболее опасным и достаточно распространенным. Защита от утечки информации по этому каналу очень сложна. Поэтому рассмотрим его более детально.

Этот способ съема информации имеет две разновидности: заходовую (заносную) и беззаходовую. Первая заключается в установке инфинитивного телефона (подслушивающего устройства — “таблетки”, “клопа”, “жучка” и т. п.) в аппаратуру средств обработки информации, в различные технические устройства, на проводные коммуникационные линии (радио, телефон, телевизионный кабель, охранно-пожарной сигнализации, электросеть и т. п.), а также в различные конструкции инженерно-технических сооружений и бытовых предметов, находящихся на объекте с целью перехвата разговоров работающего персонала и звуковых сигналов технических устройств (определение номера вызываемого абонента АТС и т. п.). Установка “клопа” или иной разведывательной аппаратуры на объект возможна тремя способами. В первом — необходимо скрытное или легендированное проникновение в помещение; во втором случае — радиопередающая и звукозаписывающая аппаратура устанавливается во время постройки или ремонта помещения; в третьем — приобретается или заносится самой потерпевшей стороной (монтируется в приобретаемую аппаратуру или предметы). Например, только в 1993 г. по данным отечественной фирмы “Анкор”, специализирующейся в области защиты информации, на территории России было продано свыше 70000 специальных устройств перехвата информации зарубежного производства стоимостью от 500 до 2000 долл. США. Наиболее часто закупалась следующая специальная техника:

— спецмикрофоны с рабочим диапазоном свыше 400 МГц (заносные и закладные, с прикрытием сигнала и без, с возможным дистанционным управлением);

— диктофоны с длительной записью различных модификаций;

— цифровые адаптивные фильтры типа АФ-512, DAC-256 и DAC-1024, позволяющие проводить обработку зашумленных речевых сигналов в реальном масштабе времени с эффективным подавлением помех [40, с. 55].

Обнаружить аппаратуру съема информации крайне трудно и технически сложно выполнимо, так как она, обычно, очень хорошо камуфлируется преступником (под микросхему, зажигалку, булавочную головку и т. д.) и может устанавливаться как внутри зоны контролируемого помещения, так и за ее пределами, а в ряде случаев — на значительном расстоянии.

Вторая — беззаходная разновидность — наиболее опасна. Заключается она в следующем. Акустические и вибрационные датчики съема информации устанавливаются на инженерно-технические конструкции, находящиеся за пределами охраняемого помещения, из которого необходимо принимать речевые сигналы. Выделяют следующие типовые конструкции инженерно-технических сооружений, по которым передаются речевые сигналы: несущие стены зданий, перегородки, перекрытия, окна, оконные рамы, двери и дверные коробки, вентиляционные воздуховоды, короба коммуникационных систем, трубопроводы. При этом необязательно проникать внутрь помещения — достаточно приблизиться к нему снаружи. Датчик устанавливается либо непосредственно, либо дистанционно. В последнем, используются различные выстреливающие устройства и специальное автоматическое крепление (захват) для удержания датчика на конструкции.

Иногда на более высокопрофессиональном уровне преступником могут использоваться направленные спецмикрофоны и дорогостоящие лазерные устройства, предназначенные для дистанционного снятия речевой информации через открытые сквозные проемы (двери, окна, форточки, мусоро- и воздухопроводы и т. п.) и оконные (автомобильные) стекла. Естественно, что при использовании подобной аппаратуры, которая помещается в маленьком дипломате, чемодане, коробке, установка датчика на объект не требуется [84, с. 316-317].

4. Видеоперехват. Данный способ совершения преступления заключается в действиях преступника, направленных на получение

С исследовательской точки зрения интересен тот факт, что специалистам во время практических экспериментов удавалось принимать информацию одновременно с 25 дисплейных терминалов, расположенных в непосредственной близости друг от друга и разделять (сортировать) данные, выведенные на каждый экран из общего “электронного шума”. По мнению экспертов, теоретически возможно извлекать данные одновременно даже с 50 терминалов [3, с. 35]. Иногда преступники подключают к своему телевизионному приемнику видеомангофон (в обычном бытовом или портативном варианте исполнения), который позволяет им зафиксировать и накопить необходимую информацию на физическом носителе с целью ее дальнейшего анализа в стационарных условиях.

3. Аудиоперехват или снятие информации по виброакустическому каналу. Данный способ совершения преступления является наиболее опасным и достаточно распространенным. Защита от утечки информации по этому каналу очень сложна. Поэтому рассмотрим его более детально.

Этот способ съема информации имеет две разновидности: заходную (заносную) и беззаходную. Первая заключается в установке инфинитивного телефона (подслушивающего устройства — “таблетки”, “клопа”, “жучка” и т. п.) в аппаратуру средств обработки информации, в различные технические устройства, на проводные коммуникационные линии (радио, телефон, телевизионный кабель, охранно-пожарной сигнализации, электросеть и т. п.), а также в различные конструкции инженерно-технических сооружений и бытовых предметов, находящихся на объекте с целью перехвата разговоров работающего персонала и звуковых сигналов технических устройств (определение номера вызываемого абонента АТС и т. п.). Установка “клопа” или иной разведывательной аппаратуры на объект возможна тремя способами. В первом — необходимо скрытное или легендированное проникновение в помещение; во втором случае — радиопередающая и звукозаписывающая аппаратура устанавливается во время постройки или ремонта помещения; в третьем — приобретается или заносится самой потерпевшей стороной (монтируется в приобретаемую аппаратуру или предметы). Например, только в 1993 г. по данным отечественной фирмы “Анкорт”, специализирующейся в области защиты информации, на территории России было продано свыше 70000 специальных устройств перехвата информации

зарубежного производства стоимостью от 500 до 2000 долл. США. Наиболее часто закупалась следующая специальная техника:

— спецмикрофоны с рабочим диапазоном свыше 400 МГц (заносные и закладные, с прикрытием сигнала и без, с возможным дистанционным управлением);

— диктофоны с длительной записью различных модификаций;

— цифровые адаптивные фильтры типа АФ-512, DAC-256 и DAC-1024, позволяющие проводить обработку зашумленных речевых сигналов в реальном масштабе времени с эффективным подавлением помех [40, с. 55].

Обнаружить аппаратуру съема информации крайне трудно и технически сложновыполнимо, так как она, обычно, очень хорошо камуфлируется преступником (под микросхему, зажигалку, булавоочную головку и т. д.) и может устанавливаться как внутри зоны контролируемого помещения, так и за ее пределами, а в ряде случаев — на значительном расстоянии.

Вторая — беззаходовая разновидность — наиболее опасна. Заключается она в следующем. Акустические и вибрационные датчики съема информации устанавливаются на инженерно-технические конструкции, находящиеся за пределами охраняемого помещения, из которого необходимо принимать речевые сигналы. Выделяют следующие типовые конструкции инженерно-технических сооружений, по которым передаются речевые сигналы: несущие стены зданий, перегородки, перекрытия, окна, оконные рамы, двери и дверные коробки, вентиляционные воздуховоды, короба коммуникационных систем, трубопроводы. При этом необязательно проникать внутрь помещения — достаточно приблизиться к нему снаружи. Датчик устанавливается либо непосредственно, либо дистанционно. В последнем, используются различные выстреливающие устройства и специальное автоматическое крепление (захват) для удержания датчика на конструкции.

Иногда на более высокопрофессиональном уровне преступником могут использоваться направленные спецмикрофоны и дорогостоящие лазерные устройства, предназначенные для дистанционного снятия речевой информации через открытые сквозные проемы (двери, окна, форточки, мусоро- и воздухопроводы и т. п.) и оконные (автомобильные) стекла. Естественно, что при использовании подобной аппаратуры, которая помещается в маленьком дипломате, чемодане, коробке, установка датчика на объект не требуется [84, с. 316-317].

4. Видеоперехват. Данный способ совершения преступления заключается в действиях преступника, направленных на получение требуемых данных и информации путем использования различной видеооптической техники (в том числе и специальной). С ее помощью преступник получает, а в некоторых случаях и фиксирует требуемую информацию и данные, которые “снимаются” дистанционно с устройств видеосъема, бумажных носителей информации (листинги, распечатки и т. д.), с нажимаемых клавиатурных клавиш при работе оператора (пользователя), а также с окружающих предметов и строительных конструкций.

Этот способ имеет две разновидности: физическую и электронную. В первом случае перехват информации производится с помощью применения преступником различной бытовой видеооптической аппаратуры, например подзорной трубы, бинокля, охотничьего прибора ночного видения, оптического прицела, видеофотоаппаратуры с соответствующими оптическими насадками (объективами) и т. п. Преступником проводится наблюдение за объектом-жертвой с некоторого расстояния с целью получения необходимой информации, которая в отдельных случаях фиксируется на физический носитель. При этом орудие преступления находится непосредственно в руках преступника.

Во-втором случае процесс получения информации преступником осуществляется с использованием специальной техники, предполагающей наличие различных каналов связи как постоянных, так и временно устанавливаемых. В данном случае передающее устройство находится непосредственно на объекте наблюдения, а приемное — в руках преступника. Может использоваться следующая спецтехника: спецвидеомагнитофоны, в т. ч. с длительной записью; оборудование для скрытой видеосъемки, включая цифровые электронные видеокамеры зарубежного производства, имеющие полную адаптацию с компьютерными системами и

различными линиями связи; телекоммуникационное оборудование с радиопередающей аппаратурой; приборы ночного видения [40, с. 60].

Как и предыдущий, этот способ также носит вспомогательный характер и служит для сбора информации, требующейся для получения основных данных. Часто при этом исследуется не сама информация, а схемы, по которым происходит ее движение [32, с. 44].

5. “Уборка мусора”. Этот способ совершения преступления заключается в неправомерном использовании преступником технологических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой (48, с. 8). Он осуществляется в двух формах: физической и электронной.

В первом случае поиск отходов сводится к внимательному осмотру содержимого мусорных корзин, баков, емкостей для технологических отходов и сбору оставленных или выброшенных физических носителей информации.

Электронный вариант требует просмотра, а иногда и последующего исследования данных, находящихся в памяти компьютера [32, с. 45]. Он основан на некоторых технологических особенностях функционирования СКТ. Например, последние записанные данные не всегда стираются в оперативной памяти компьютерной системы после завершения работы или же преступник записывает только небольшую часть своей информации при законном доступе, а затем считывает предыдущие записи, выбирая нужные ему сведения. Последнее возможно только в тех системах, в которых не обеспечивается необходимый в таких случаях иерархический принцип защиты доступа к данным. Примечателен здесь случай из зарубежной практики, когда сотрудник службы безопасности коммерческого вычислительного центра, обслуживающего несколько крупных нефтяных компаний, находясь на своем посту в зале работы клиентов, обратил внимание на то, что у одного из клиентов, работавших 1 на компьютере, перед тем, как загорится световой индикатор записи его информации на магнитный диск, всегда сравнительно продолжительное время горит индикатор считывания информации. Проведенной по данному факту доследственной проверкой было установлено, что клиент занимался промышленным шпионажем [2, с. 141].

В некоторых случаях преступником могут осуществляться действия, направленные на восстановление и последующий анализ данных, содержащихся в стертых файлах. Достижение этих целей предполагает обязательное использование в качестве орудия преступления различных программных средств специального назначения, относящихся к инструментальным программным средствам. Одним из них является программный комплекс PC Tools Deluxe, содержащий универсальную программу pct.exe, позволяющую восстанавливать ранее стертые (“уничтоженные” с точки зрения пользователя) программы и файлы, и имеющий широкое распространение в пользовательской среде. Экспериментально было установлено, что на эту операцию преступником обычно затрачивается всего несколько минут (94, с. 45).

Отметим, что чтение информации посредством данного способа возможно в том случае, когда пользователь выключает компьютер без соответствующих действий, направленных на полное уничтожение остаточных данных.

* К третьей группе способов совершения компьютерных преступлений нами относятся действия преступника, направленные на получение несанкционированного доступа к средствам компьютерной техники. К ним относятся нижеследующие.

1. “За дураком”. Этот способ часто используется преступниками для проникновения в запретные зоны — как производственные помещения, так и электронные системы.

Типичный прием физического проникновения хорошо известен специалистам, занимающимся вопросами совершенствования оперативно-розыскной деятельности. Он заключается в следующем: держа в руках предметы, связанные с работой на компьютерной технике (элементы маскировки), нужно ожидать кого-либо, имеющего санкционированный доступ, возле запертой двери, за которой находится предмет посягательства. Когда появляется законный пользователь, остается только войти вместе с ним или попросить его помочь донести якобы необходимые для работы на компьютере предметы. Этот вариант способа рассчитан на низкую бдительность сотрудников организации и лиц, ее охраняющих. При этом преступниками может быть использован прием легендирования [75, с. 16].

На таком же принципе основан и электронный вариант несанкционированного доступа. В этом случае он используется преступником из числа внутренних пользователей путем подключения компьютерного терминала к каналу связи через коммуникационную аппаратуру (обычно используются так называемые “шнурки” — шлейф, изготовленные кустарным способом, либо внутренняя телефонная проводка) в тот момент времени, когда сотрудник, отвечающий за работу средства компьютерной техники, выбранной в качестве предмета посягательства, кратковременно покидает свое рабочее место, оставляя терминал или персональный компьютер в активном режиме.

2. “За хвост”. Этот способ съема информации заключается в следующем. Преступник подключается к линии связи законного пользователя (с использованием средств компьютерной связи) и терпеливо дожидается сигнала, обозначающего конец работы, перехватывает его “на себя”, а потом, когда законный пользователь заканчивает активный режим, осуществляет доступ к системе. Этот способ технологически можно сравнить с работой двух и более неблокированных телефонных аппаратов, соединенных параллельно и работающих на одном абонентном номере: когда телефон “А” находится в активном режиме, на другом телефоне “Б” поднимается трубка, когда разговор по телефону “А” закончен и трубка положена — продолжается разговор с телефона “Б” [55, с. 4]. Подобными свойствами обладают телефонные аппараты с функцией удержания номера вызываемого абонента. Поэтому нет особого различия в том, что подключается к линии связи — телефон или персональный компьютер.

3. “Компьютерный абордаж”. Данный способ совершения компьютерного преступления осуществляется преступником путем случайного подбора (или заранее добытого) абонентного номера компьютерной системы потерпевшей стороны с использованием, например, обычного телефонного аппарата. После успешного соединения с вызываемым абонентом и появления в головном телефоне преступника специфического позывного сигнала, свидетельствующего о наличии модемного входа/выхода на вызываемом абонентном номере, преступником осуществляется механическое подключение собственного модема и персонального компьютера, используемых в качестве орудия совершения преступления, к каналу телефонной связи. После чего преступником производится подбор кода доступа к компьютерной системе жертвы (если таковой вообще имеется) или используется заранее добытый код. Иногда для этих целей преступником используется специально созданная самодельная, либо заводская (в основном, зарубежного производства) программа автоматического поиска пароля, добываемая преступником различными путями. Алгоритм ее работы заключался в том, чтобы, используя быстродействие современных компьютерных устройств, перебирать все возможные варианты комбинаций букв, цифр и специальных символов, имеющихся на стандартной клавиатуре персонального компьютера, и в случае совпадения комбинации символов с оригиналом производить автоматическое соединение указанных абонентов. Самодельная программа автоматического поиска пароля достаточно проста в плане ее математической и программной реализации. Иногда преступниками специально похищается носитель машинной информации с уже имеющимся паролем доступа, как это видно из примера, приведенного нами при рассмотрении первой группы способов совершения преступления. После удачной идентификации парольного слова преступник получает доступ к интересующей его компьютерной системе.

Стоит обратить внимание на то, что существует множество программ-“взломщиков”, называемых на профессиональном языке HACKTOOLS (инструмент взлома). Эти программы работают 3-127 65 по принципу простого перебора символов, которые возможно ввести через клавиатуру персонального компьютера. Но они становятся малоэффективными! в компьютерных системах, обладающих программой-“сторожем” компьютерных портов (данные средства будут подробно рассмотрены нами в четвертой главе работы), ведущей автоматический протокол обращений к компьютерной системе и отключающей абонентов в случае многократного некорректного доступа (абордаж ложного пароля). Поэтому в последнее время преступниками стал активно использоваться метод “интеллектуального перебора”, основанный на подборе предполагаемого пароля, исходя из заранее определенных тематических групп его принадлежности. В этом случае программе-“взломщику” передаются некоторые исходные данные о личности автора пароля добытые преступником с помощью других способов совершения компьютерного преступления. По оценкам специалистов, это позволяет более чем на десять порядков сократить количество возможных вариантов перебора символов и на столько же Ж(— время на подбор пароля. Как показывают многочисленны! эксперименты, вручную с использованием метода “интеллектуального перебора” вскрывается 42% от общего числа паролей, состоящих из 8 символов (стандартная величина названия файла)

В ходе проникновения в информационные сети преступники иногда оставляют различные следы, заметив которые подвергшиеся нападению субъекты нападения меняют систему защиты информации. В ответ на это некоторые преступники намеренно сохраняют следы в первом персональном компьютере информационной сети, вводя таким способом в заблуждение сотрудников служб компьютерной безопасности, которые начинают считать, что имеют дело с неопытным любителем-дилетантом. Тем самым теряется бдительность при контроле за другими системами, к которым преступники получают последующий доступ с помощью применения другого способа.

По существу, “компьютерный абордаж” является подготовительной стадией компьютерного преступления.

4. Неспешный выбор. Отличительной особенностью данного способа совершения преступления является то, что преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите. Однажды обнаружив их, он может не спеша исследовать содержащуюся в системе информацию, скопировать ее на свой физический носитель и, возвращаясь к ней много раз, выбрать наиболее оптимальный предмет посягательства. Обычно такой способ используется преступником в отношении тех, кто не уделяют должного внимания регламенту проверки своей системы, предусмотренному методикой защиты компьютерной системы.

5. “Брешь”. В отличие от “неспешного выбора”, когда производится поиск уязвимых мест в защите компьютерной системы, при данном способе преступником осуществляется их конкретизация: определяются участки, имеющие ошибку (ошибки) или неудачную логику программного строения. Выявленные таким образом “бреши” могут использоваться преступником многократно, пока не будут обнаружены. Последнее возможно лишь высококвалифицированным программистом или лицом, непосредственно разработавшим данную программу.

Появление этого способа обусловлено тем, что программисты иногда допускают ошибки при разработке программных средств, которые не всегда удается обнаружить в процессе отладки программного продукта. Например, методика качественного программирования предполагает: когда программа X требует использования программы Y — должна выдаваться только информация, необходимая для вызова Y, а не она сама. Для этих целей применяются программы группировки данных. Составление последних является делом довольно скучным и утомительным, поэтому программисты иногда сознательно нарушают методику программирования и делают различные упрощения, указывая, например, индекс места нахождения нужных данных, в рамках более общего списка команд программы. Именно это и создает возможности для последующего нахождения подобных “брешей” [2, с. 143].

Уязвимые места иногда могут быть обнаружены преступником не только в программно-логических, но и в электронных цепях. Например, не все комбинации букв используются для команд, указанных в руководстве по эксплуатации компьютера [2, с. 144]. Некоторые такие сочетания могут приводить и к появлению электронных “брешей” по аналогии с “нулевым” абонентом телефонной сети: случайный незарегистрированный абонентный номер, созданный посредством нарушения логики связи в электрических цепях коммутирующих устройств автоматической телефонной станции (АТС).

Все эти небрежности, ошибки, слабости в логике приводят к появлению “брешей”. Иногда программисты намеренно делают их для последующего использования в различных целях, в том числе и с целью подготовки совершения преступления.

5.1 “Люк”. Данный способ является логическим продолжением предыдущего. В этом случае в найденной “бреши” программа “разрывается” и туда дополнительно преступник вводит одну или несколько команд. Такой “люк” “открывается” по мере необходимости, а включенные команды автоматически выполняются. Данный прием очень часто используется проектантами программных средств и работниками организаций, занимающихся профилактикой и ремонтом компьютерных систем с целью автоматизации рутинной работы. Реже — лицами, самостоятельно обнаружившими “бреши”.

При совершении компьютерного преступления данным способом, следует обратить внимание на то, что при этом всегда преступником осуществляется преднамеренная модификация (изменение) определенных средств компьютерной техники.

6. “Маскарад”. Данный способ состоит в том, что преступник проникает в компьютерную систему, выдавая себя за законного пользователя. Системы защиты средств компьютерной техники, которые не обладают функциями аутентичной идентификации пользователя (например, по биометрическим параметрам: отпечаткам пальцев, рисунку сетчатки глаза, голосу и т. п.), оказываются незащищенными от этого способа. Самый простейший путь к проникновению в такие системы — получить коды и другие идентифицирующие шифры законных пользователей. Это можно сделать посредством приобретения списка пользователей со всей необходимой информацией путем подкупа, коррумпирования, вымогательства или иных противоправных деяний в отношении лиц, имеющих доступ к указанному документу; обнаружения такого документа в организациях, где не налажен должный контроль за их хранением; отбора информации из канала связи и т. д. Так, например, задержанный в декабре 1995 г. сотрудниками московского РУОПа преступник похищал наличные денежные средства из банкоматов банка “Столичный” с использованием обычной электронной кредитной карточки путем подбора цифровой комбинации кода доступа в компьютерную систему управления счетами клиентов банка. Общая сумма хищения составила 400 млн. руб. [83, с. 2].

Интересен пример и из зарубежной практики: преступник, являющийся законным пользователем компьютерной сети с рабочей станции передал сообщение всем пользователям сервера о том, что его телефонный номер якобы изменен. В качестве нового номера был назван номер собственного персонального компьютера преступника, запрограммированный таким образом, чтобы отвечать аналогично серверу. Пользователи, посылавшие вызов, набирали при этом свой личный код, что предусмотрено правилами электронного обмена информацией. Это обстоятельство и было использовано преступником в корыстных целях. Им был получен исчерпывающий список личных кодов пользователей. Затем, с целью сокрытия своих действий, им было послано сообщение о том, что прежний номер сервера восстановлен [2, с. 145].

В компьютерных преступлениях способ “маскарад”, так же как и способ “за дураком”, может выступать не только в электронной, но и в самой обычной физической форме. Чаще всего в этом случае преступники представляются корреспондентами, сотрудниками различных обслуживающих и вышестоящих организаций и получают необходимый им доступ к средствам компьютерной техники (используют метод легендирования).

7. Мистификация. Иногда по аналогии с ошибочными телефонными звонками случается так, что пользователь с терминала или персонального компьютера подключается к чьей-либо системе, будучи абсолютно уверенным в том, что он работает с нужным ему абонентом. Этим фактом и пользуется преступник, формируя правдоподобные ответы на запросы владельца информационной системы, к которой произошло фактическое подключение, и поддерживая это заблуждение в течение некоторого периода времени, получая при этом требуемую информацию, например коды доступа или отклик на пароль.

8. “Аварийный”. В этом способе преступником используется тот факт, что в любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ (аварийный или контрольный отладчик). Принцип работы данной программы заключается в том, что она позволяет достаточно быстро обойти все имеющиеся средства защиты информации и компьютерной системы с целью получения аварийного доступа к наиболее ценным данным. Такие программы являются универсальным “ключом” в руках преступника.

9. “Склад без стен”. Несанкционированный доступ к компьютерной системе в этом случае осуществляется преступником путем использования системной поломки, в результате которой возникает частичное или полное нарушение нормального режима функционирования систем защиты данных. Например, если нарушается система иерархического либо категорийного доступа к информации, у преступника появляется возможность получить доступ к той категории информации, в получении которой ему ранее было отказано.

К четвертой группе способов совершения компьютерных преступлений нами относятся действия преступников, связанные с использованием методов манипуляции данными и управляющими

командами средств компьютерной техники. Эти методы наиболее часто используются преступниками для совершения различного рода противоправных деяний и достаточно хорошо известны сотрудникам подразделений правоохранительных органов, специализирующихся по борьбе с экономическими преступлениями. Примечателен здесь факт, что одно из первых отечественных компьютерных преступлений было совершено именно посредством использования метода манипуляции ценными данными при совершении хищения денежных средств в 1979 г. в г. Вильнюсе [2, с. 126]. А второе подобное преступление было совершено уже в 1982 г. в г. Горьком (нынешний Н. Новгород). Совершению серии подобных преступлений с использованием ' одинаковых методик, по мнению специалистов, способствовало то обстоятельство, что в этот период времени все отделения связи бывшего СССР переводились на новую централизованную автоматическую систему обработки (получения и отправки) денежных переводов клиентов, функционирующую на базе компьютерного комплекса "Онега". Вместе с этой системой на переходном этапе компьютеризации отделений связи применялся и обычный ручной способ приема и отправления платежей. Совпадение этих двух обстоятельств (наличие автоматизированных и неавтоматизированных операций с денежными средствами) и позволило преступным группам лиц из числа работников связи совершать хищения денежных средств с использованием методов манипуляции данными [2, с. 126].

Далее, отечественная история развития этих методов такова, что уже к 1988 г. они приобрели социально опасный многочисленный характер. В настоящее время мы уже имеем более высокий их качественный и технологический уровень.

Как показывает проведенное нами исследование в отечественной практике наиболее часто преступниками стали использоваться методы манипуляции входными и выходными данными, с помощью которых совершаются хищения денежных средств в крупных и особо крупных размерах в учреждениях, организациях, на промышленных и торговых предприятиях, использующих автоматизированные компьютерные системы для обработки первичных бухгалтерских документов, отражающих кассовые операции, движение материальных ценностей и другие разделы учета. Здесь нами особо выделяется тот факт, что перевод на машинные носители учетно-экономической и финансовой информации крайне затрудняет проведение бухгалтерского и ревизионного контроля, до сих пор ориентированных преимущественно на визуальную проверку, которая в условиях применения новых компьютерных технологий становится все менее эффективной.

Недооценка важности надлежащего контроля за деятельностью должностных лиц, а в некоторых местах и полное его отсутствие, а также несовершенство законодательных и организационно-технических мер защиты информационных ресурсов позволяют преступникам с помощью указанных выше методов вносить изменения в отчетность и результаты финансово-бухгалтерских операций.

“ Рассмотрим наиболее широко используемые преступниками способы совершения компьютерных преступлений, относящиеся к группе методов манипуляции данными и управляющими командами средств компьютерной техники.

1. Подмена данных — наиболее простой и поэтому очень часто применяемый способ совершения преступления. Действия преступников в этом случае направлены на изменение или введение новых данных, которое осуществляется, как правило, при вводе-выводе информации. В частности, данный способ совершения преступления применяется для приписывания счету “чужой” истории, т. е. модификации данных в автоматизированной системе банковских операций, приводящей к появлению в системе сумм, которые реально на данный счет не зачислялись. Например, таким способом экономистом Брестского областного производственного объединения К. были совершены хищения денежных средств. Как свидетельствуют материалы уголовного дела, будучи экономистом по учету заработной платы и отвечая за достоверность документов и сдачу их в ОАСУ, К. на протяжении ряда лет (начиная с 1981 г.) вносила в документы на начисление заработной платы подложные документы. В результате чего заработная плата начислялась на счета вымышленных лиц и переводилась в сберкассы г. Бреста на специально открытые ею счета: на имя матери К. (7115 руб. 63 коп.), сестры (4954 руб. 30 коп.), знакомого (5379 руб.). Всего таким образом К. похитила 22960 руб. и в 1988 г. была осуждена Брестским областным судом по ч. 1 ст. 91 УК БССР [99, с. 19].

Этот способ применялся преступниками и при хищении материальных ценностей и чужого имущества. Например, при хищениях бензина на автозаправочных станциях, применяющих автоматизированные компьютерные системы отпуски горюче-смазочных материалов (ГСМ). В этом

случае преступниками производилось изменение (фальсификация) учетных данных, в частности путем частичного повреждения физических носителей машинной информации, в результате чего практически было невозможно определить количество отпущенного потребителям бензина [2, с. 126]. Этим же способом могут совершаться и преступления, связанные с оформлением фиктивных операций купли-продажи, например покупки железнодорожных и авиационных билетов, предполагающих собой использование компьютерных автоматизированных систем заказов и оформлений билетов и других проездных документов (например, система “Экспресс-2”). Так, по данным зарубежной печати, одно туристическое агентство в Великобритании было разорено конкурентами. Преступники, используя несанкционированный доступ в автоматизированную компьютерную систему продажи авиабилетов, совершили финансовую сделку — путем подмены данных они произвели закупку билетов на самолеты на всю сумму денежных средств, находившихся на счетах туристического агентства [45, с. 14]. С научной точки зрения интересен еще один пример из зарубежной практики. Он заключается в том, что преступнику путем изменения данных в компьютерной системе управления движением грузов по нью-йоркской железной дороге “Пенн-сентрал” удалось похитить 352 железнодорожных вагона с грузами на общую сумму более 1 млн. долл. США. Следствием было установлено, что неизвестным лицом тайно были подменены данные о пунктах назначения грузов, в результате чего они были отправлены по другим адресам и похищены [2, с. 146]. По данным российских спецслужб, имеются сведения о фактах несанкционированного доступа к ЭВМ вычислительного центра железных дорог России (раздел “движение грузов и грузоперевозки”), а также к электронной информации систем учета жилых и нежилых помещений местных органов управления во многих городах [21, с. 143]. Рассмотрим данную ситуацию подробнее на смоделированном отечественном примере.

На Новокуйбышевском нефтеперерабатывающем заводе Самарской области на базе персональных компьютеров действует автоматизированная система “Сбыт”. В соответствии с работой программы, обеспечивающей функционирование этой системы, в нее закладывается вся информация о договорах и контрагентах по поставкам нефтепродуктов. При запросе оператора ЭВМ выдает данные о наличии договора поставки, а в случае необходимости — соответствующие бухгалтерские документы (товарно-транспортные накладные, пропуска, путевые листы и т. д.). Использование подобной программы позволяет оптимизировать процесс оформления договора поставки нефтепродуктов. Однако здесь возможен вариант, когда оператор может ввести в ЭВМ ложные сведения о несуществующем получателе продукции и когда на складе запросят в банке данных подтверждающую информацию об этом, то ЭВМ выдаст ее вместе с набором соответствующей необходимой документации. Впоследствии, после получения продукции фиктивным получателем, оператор удаляет из памяти ЭВМ все сведения о получателе и таким образом ликвидирует следы ввода ложных данных и сам факт осуществления операции. Все эти операции, как показывает эксперимент, производятся оператором в считанные минуты [94, с. 45-46].

1.1 Подмена кода. Это частный вариант способа подмены данных. Он заключается в изменении кода данных, например бухгалтерского учета. Рассмотрим его более подробно на одном примере.

Анализ материалов уголовного дела, возбужденного по факту хищения денежных средств в особо крупных размерах в Волгоградском промторге, свидетельствует о том, что начальником финансово-расчетного отдела централизованной бухгалтерии указанной организации К. в период с января 1982 по декабрь 1984 г. было совершено хищение выручки от реализации талонов ГСМ в размере 17033 руб. 97 коп. путем злоупотребления служебным положением. При этом К. с целью сокрытия недостачи похищенной выручки от реализации талонов ГСМ при расчете с объединением “В.”, была создана искусственная кредиторская задолженность в том же размере (17033-97) путем заведомо неправильной кодировки переноса различных сумм в исправительных справках, платежных требованиях, поручениях и других документах. Следствием было установлено, что при кодировании таких документов К. карандашом ставила шифр “286”, предусмотренный для расчетов с “В.”. В результате чего поступающие промторгу от различных организаций суммы по машинограммам переносились на указанный шифр. При возвращении документов после их обработки в информационно-вычислительном центре (ИВЦ) К. стирала карандашную запись кода “286”, а впоследствии уничтожала часть документов с неправильной кодировкой. Так, например, в исправительной справке пачки документов № 67 (услуги) К. сделала кодировку 0-249-0-286-0-1856=25-764-764, где шифр “286” записала карандашом. В результате этого 1856 руб. 25 коп. по машинограмме были перенесены на расчеты с “В.”. При возвращении этого документа с ИВЦ К. стерла карандашную запись и вписала шифр “290”, за которым не числится никакой организации или предприятия. Иногда преступницей вписывался шифр других организаций и предприятий, шифр “262” — ошибка Госбанка — либо не вписывался вообще в зависимости от сложившейся

ситуации. Таким образом покрывалась недостача похищенных денежных сумм. В январе 1987 г. К. была осуждена Волгоградским областным судом.

Аналогичным способом преступниками осуществляется и прямое хищение денежных средств, товаров и услуг.

2. “Троянский конь”. Данный способ заключается в тайном введении в чужое программное обеспечение специально созданных программ, которые, попадая в информационно-вычислительные системы (обычно выдавая себя за известные сервисные программы), начинают выполнять новые, не планировавшиеся законным владельцем принимающей “тroyанского коня” программы, с одновременным сохранением прежней ее работоспособности [79, с. 8]. В соответствии со ст. 273 Уголовного кодекса Российской Федерации под такой программой понимается “программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети” [92, ст. 273]. По существу, “тroyанский конь” — это модернизация уже рассмотренного нами способа “люк” с той лишь разницей, что он “открывается” не при помощи непосредственных действий самого преступника (“вручную”), а автоматически — с использованием специально подготовленной для этих целей программы без дальнейшего непосредственного участия самого преступника.

С помощью данного способа преступники обычно отчисляют на заранее открытый счет определенную сумму с каждой операции. Возможен здесь и вариант увеличения преступниками избыточных сумм на счетах при автоматическом пересчете рублевых остатков, связанных с переходом к коммерческому курсу соответствующей валюты.

Данный способ основан на том, что компьютерные программы представляют собой сложную комбинацию алгоритмов, состоящих из набора порядка от нескольких сотен до миллионов команд, которые в свою очередь состоят еще из порядка 6-8 математических знаков кода (“0” и “1”), чтобы процессор мог оперировать с ними (так называемый “машинный язык”). Поэтому программа “тroyанского коня”, состоящая из нескольких десятков команд, обнаруживается с большими сложностями только квалифицированными экспертами-программистами. На ее поиск необходимо потратить значительное время, иногда до одного года. Проще заново воссоздать оригинал исследуемой программы, чем искать в ней “тroyанского коня”, что категорически недопустимо в процессе расследования преступления.

Из зарубежной следственной практики интересен факт использования “тroyанского коня” одним американским программистом. Он вставил в программное обеспечение персонального компьютера по месту своей работы команды, которые не выводили на печать для отчета определенные поступления денежных средств. Эти суммы особым образом шифровались и циркулировали только в информационной среде компьютера. Похитив бланки выдачи денег, преступник заполнял их с указанием своего шифра, а затем проставлял в них определенные суммы денег. Соответствующие операции по их выдаче также не выводились на печать и, следовательно, не могли подвергнуться документальной ревизии [2, с. 148].

2.1 “Тroyанская матрешка”. Является разновидностью “тroyанского коня”. Особенность этого способа заключается в том, что во фрагмент программы потерпевшей стороны вставляются не команды, собственно выполняющие незаконные операции, а команды, формирующие эти команды и после выполнения своей функции, т. е. когда уже будет автоматически на программном уровне создан “тroyанский конь”, самоуничтожающиеся. Иначе говоря, это программные модули-фрагменты, которые создают “тroyанского коня” и самоликвидируются на программном уровне по окончании исполнения своей задачи.

В данном случае эксперту-программисту, производящему технико-технологическую экспертизу на предмет обнаружения в алгоритме законного программного продукта фрагментарного вкрапления в алгоритма программы “тroyанского коня”, необходимо искать не его самого, а команды-модули, его создающие. Сделать это практически невозможно, т. к. коэффициент репродукций модулей может быть любого численного порядка по принципу функционирования обычной игрушки “Матрешка”.

2.2 “Тroyанский червь”. Еще одна разновидность способа “тroyанский конь”. Данный способ совершения преступления характеризуется тем, что в алгоритм работы программы, используемой

в качестве орудия совершения преступления, наряду с ее основными функциями, уже рассмотренными нами выше, закладывается алгоритм действий, осуществляющих саморазмножение, программное автоматическое воспроизводство “тroyанского коня”. “Программы-черви” автоматически копируют себя в памяти одного или нескольких компьютеров (при наличии компьютерной сети) независимо от других программ. При этом используется тактика компьютерных вирусов, которые будут рассмотрены нами далее по тексту настоящей работы.

2.3 “Салями”. Такой способ совершения преступления стал возможным лишь благодаря использованию компьютерной технологии в бухгалтерских операциях. Раньше он не использовался преступниками по причине его “невыгодности”. Данный способ основан на методике проведения операций перебрасывания на подставной счет мелочи — результата округления, которая на профессиональном бухгалтерском языке называется “салями”. Мелочной преступный расчет в этом случае построен на том, что ЭВМ в секунду совершает миллионы операций, в то время как высококвалифицированный бухгалтер за целый рабочий день может выполнить лишь до двух тысяч таких операций [8, с. 181-182]. На этом строится и тактика использования “тroyанского коня”, основанная на том, что отчисляемые суммы столь малы, что их потери практически незаметны (например, 1 руб. или 1 цент с бухгалтерской операции), а незаконное накопление суммы осуществляется за счет совершения большого количества операций. С точки зрения преступников; это один из простейших и безопасных способов совершения преступления. Он используется, как правило, при хищении денежных средств в тех бухгалтерских операциях, в которых отчисляются дробные (меньше чем одна минимальная денежная единица) суммы денег с каждой операции, т. к. в этих случаях всегда делается округление сумм до установленных целых значений. Ставка преступников делается на том, что при каждой ревизионной проверке потерпевший теряет так мало, что это практически не фиксируется документально. Между тем, учитывая скорость компьютерной обработки данных и количество осуществляемых в секунду операций, можно сделать вывод о размерах преступно накапливаемых и никем не регистрируемых сумм. Когда “салями” начинают понимать не в абсолютном, а в процентном смысле, вероятность раскрытия преступления значительно увеличивается.

2.4 “Логическая бомба”. Иногда из тактических соображений хищения удобнее всего совершать при стечении каких-либо обстоятельств, которые обязательно должны наступить. В этих случаях преступниками используется рассматриваемый способ совершения преступления, основанный на тайном внесении изменений в программу потерпевшей стороны набора команд, которые должны сработать (или срабатывать каждый раз) при наступлении определенных обстоятельств через какое-либо время [79, с. 8; 94, с. 45]. Далее включается алгоритм программы “тroyанского коня”. На практике заготовками данных программ пользуются системные программисты для законного тестирования компьютерных систем на их нормальную работоспособность, а также для исследовательских целей.

2.4.1 “Временная бомба”. Является разновидностью “логической бомбы”, которая срабатывает по достижении определенного момента времени. Например, в США получили широкое распространение преступления, в которых преступником используется способ “временной бомбы” для хищения денежных средств. Механизм применения этого способа заключается в следующем. Преступником, находящимся в стране “А”, посредством заранее введенной в банк данных автоматизированной системы межбанковских электронных операций программы “временной бомбы” в стране “Б”, похищаются деньги в определенный заданный момент времени при стечении благоприятных обстоятельств. Все манипуляции с ценными данными, а также начало осуществления бухгалтерских операций с ними производятся и контролируются программой. Преступнику лишь остается в определенный момент времени снять деньги, поступившие на заранее открытый счет. Аналогично происходят и преступления, направленные на разрушение определенных данных и информации в компьютерной системе для различных преступных целей [79, с. 7].

2.5 “Тroyанский конь” в электронных цепях. В отличие от “тroyанских коней” программных, которые представляют собой совокупность команд, внедряемых в программные средства, этот способ предполагает создание определенных логических связей в электронных цепях аппаратных средств компьютерной техники для автоматического выполнения незаконных манипуляций по аналогии с программным способом. “Тroyанский конь” в электронных цепях компьютеров — очень редкий способ совершения компьютерного преступления, который был впервые зарегистрирован в 1981 г. в Швеции [2, с. 148]. Особенность его заключается в том, что если в компьютерных системах I-IV поколений электронный “тroyанский конь” создавался преступником кустарным способом посредством нарушения логики токнесущих проводников печатных плат и внесения

конструкционных элементных изменений в электронную схему архитектуры строения компьютерной техники, то при эксплуатации компьютерных систем соответственно V и VI поколений, подобные преступные действия возможны лишь путем внесения конструкционных изменений в топологию интегральных микросхем при их заводском изготовлении [79, с. 3].

2.6 Компьютерные вирусы. С программно-технической точки зрения под компьютерным вирусом понимается специальная программа, способная самопроизвольно присоединяться к другим программам (“заражать” их) и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов (при файловой организации программной среды), искажение и стирание (уничтожение) данных и информации, переполнение машинной памяти и создание помех в работе ЭВМ. Такие программы обычно составляются (исполняются, пишутся) преступниками на языке программирования “ассемблер” и не выдают при своей работе никаких аудиовизуальных отображений в компьютерной системе. Переносятся при копировании информации и ценных данных с одного материального носителя на другой, либо по компьютерной сети с использованием средств телекоммуникации [68, с. 52-53]. С уголовно-правовой точки зрения, согласно ст. 273 Уголовного кодекса Российской Федерации, под компьютерным вирусом следует понимать вредоносную программу для ЭВМ, определение которой было приведено нами выше.

В самом общем виде этот способ совершения компьютерных преступлений является ничем иным, как логической модернизацией способа “троянский конь”, выполняющего алгоритм, например типа “сотри все данные этой программы, перейди в следующую и сделай то же самое”. Этот способ широко распространен по своему применению. Например, как свидетельствуют материалы одного уголовного дела, сотрудник Игналин-ской АЭС из корыстных побуждений разработал и использовал в информационно-вычислительных системах первого и второго блоков атомной электростанции несанкционированные программные модули, что привело к искажению информации, поступающей на средства отображения рабочего места управления атомным реактором, повлекшему за собой возникновение аварийной (нештатной) ситуации, последствия которой не нуждаются в пояснении. Рассмотрим данный способ более подробно.

В настоящее время в мире существует уже более 2000 вирусов, и это только для одной, наиболее популярной и широко используемой на практике операционной системы MS-DOS. Количество вирусов постоянно увеличивается. Однако для понимания способа совершения преступления все вирусы можно подробно классифицировать по определенным основаниям и разбить на несколько обобщенных групп. Нами выделяются:

- 1) загрузочные (системные) вирусы (поражающие загрузочные секторы машинной памяти);
- 2) файловые вирусы (поражающие исполняемые файлы, в том числе COM, EXE, SYS, BAT-файлы и некоторые другие);
- 3) комбинированные вирусы.

Заражение загрузочными вирусами происходит при загрузке компьютера с носителя машинной информации, содержащего вирус. Заражение может произойти как случайно, например, если потерпевший сам, не подозревая о наличии вируса на носителе, запустил с него компьютерную систему, так и преднамеренно, если преступник знал о его существовании и последствиях, которые наступят после запуска системы с вирусом-носителя. Причем носитель машинной информации может и не быть системным, т. е. не содержать файлов операционной системы. Заразить носитель достаточно просто. На него вирус может попасть, если пользователь просто вставил его в приемное устройство (дисковод) зараженного компьютера и, например, прочитал его оглавление. При этом вирус автоматически внедряется в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot Record — MBR), т. е. первый сектор логического диска (на флоппи-дисках он совпадает с первым физическим сектором), который содержит программу-загрузчик, отвечающую за запуск операционной системы, необходимой для поддержания дружественного интерфейса пользователя с ЭВМ [39, с. 7, 162]. Сектором магнитного диска (минимальной единицей его разбиения) называется участок дорожки, образующийся при форматировании диска и являющийся минимальной физически адресуемой единицей памяти [68, с. 345].

Файловые вирусы заражают компьютер, если пользователь запустил на своей ЭВМ программу, уже содержащую вирус. В этом случае возможно заражение других исполняемых файлов. Рассмотрим этот процесс более детально.

Многие вирусы обладают свойством переходить через коммуникационные сети из одной системы в другую, с одного компьютера на другой, распространяясь, как вирусное заболевание (сетевые вирусы) [24, с. 237]. Выявляется вирус не сразу: первое время компьютер “вынашивает инфекцию”, поскольку для маскировки этот способ нередко используется преступником в комбинации с приемами “логической” или “временной бомбы”, рассмотренных нами выше. “Вирус” как бы наблюдает за всей обрабатываемой в системе потерпевшего информацией и может перемещаться вместе с ней, благодаря ее постоянному движению. Начиная действовать (перехватывая управление средствами компьютерной техники “на себя”), вирус дает команду компьютеру, чтобы тот записал зараженную версию программы. После этого он возвращает программе управление. Потерпевший ничего не заметит, т. к. его компьютерная система находится в состоянии “здорового носителя вируса”. Обнаружить последнее может только специалист, обладающий чрезвычайной развитой программистской интуицией, поскольку никакие нарушения в работе средств компьютерной техники в данный момент активно не проявляют себя [2, с. 148-149]. Далее, через некоторое время происходит нарушение нормального режима функционирования СКТ: компьютер отказывается нормально загружаться или не загружается совсем, по неизвестным причинам исчезают из памяти файлы, некоторые программные средства самопроизвольно стираются, на экране дисплея, например, начинают опадать или геометрически перемешиваться буквы и символы (вирус “листопад”, “змейка”, “червячок”, “мозаика”), исчезают системные файлы или файлы с каким-либо определенным расширением (например, .com, .bat, .exe, .dbf, .txt и т. д.), либо резко на 180 градусов переворачивается изображение, периферийные устройства отказывают в работе, неожиданно на экране дисплея появляется реклама чего-либо или светящаяся точка (“итальянский попрыгунчик”) и т. д. и т. п.

Вопросами научного изучения компьютерных вирусов в настоящее время занимается специально созданная новая наука — компьютерная вирусология [5]. С точки зрения этой науки все программы-вирусы подразделяются на две группы, имеющие подгрупповое деление, а именно:

- 1) по способу заражения средств компьютерной техники вирусы подразделяются на резидентные и нерезидентные;
- 2) по алгоритму их строения и обнаружения на “вульгарный вирус” и “раздробленный вирус”.

Все запускаемые на выполнение программные средства делятся на резидентные — TSR (Terminate and Stay Resident) и на нерезидентные — NTSR (Not Terminate and Stay Resident). Резидентной называется программа, которая по окончании работы оставляет свой код или часть кода в оперативной памяти: программно адресуемая память, быстродействие которой соизмеримо с быстродействием центрального процессора и предназначенная для хранения исполняемых в данный момент программ и оперативно необходимых для этого данных [68, с. 256]. Одновременно с этим операционная система резервирует необходимый для работы этой программы участок памяти. После этого резидентная программа работает параллельно другим программам. Доступ к резидентной программе осуществляется либо через подмену прерываний, либо непосредственной адресацией. Нерезидентной называется программа, которая при завершении работы не оставляет своего кода или его части в оперативной памяти. При этом, занимаемая ею память освобождается [39, с. 161]. Так как вирус представляет собой программное средство, то он обладает этими свойствами.

Резидентный вирус при “инфицировании” программных средств оставляет в оперативной памяти компьютерной системы потерпевшей стороны свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентный вирус находится в памяти и является активным вплоть до выключения или перезагрузки компьютерной системы. В свою очередь, нерезидентный вирус не заражает оперативную память и является активным ограниченное время, а затем “погибает”, в то время как резидентный активизируется после каждого включения компьютерной системы. Заметим, что некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не имеют алгоритма распространения вируса. Такие вирусы являются нерезидентными.

Программа “вульгарного вируса” написана единым блоком и достаточно легко обнаруживается специалистами в самом начале ее активных проявлений с помощью набора стандартных антивирусных программных средств, которые будут подробно рассмотрены нами в четвертой главе настоящей работы. В случае же проведения программно-технической экспертизы эта операция требует, в частности, очень тщательного анализа всей компьютерной системы на предмет обнаружения в ней посторонних программных продуктов или их компонентов.

Программа “раздробленного вируса” разделена на части, на первый взгляд не имеющие между собой логической связи. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, в какой последовательности и в каком случае или в какое время воссоздать “вирус” и когда размножить его (принцип “тroyанского коня”). Таким образом, вирус почти все время находится в “распределенном” состоянии, лишь на короткое время своей работы собираясь в единое целое. Как правило, создатели “вируса” указывают ему число репродукций, после достижения которого он либо вымирает, либо становится агрессивным и совершает заранее заданные незаконные манипуляции [2, с. 149].

Наиболее часто встречаются следующие вирусные модификации.

2.6.1 Вирусы-“спутники” (companion) — это вирусы, не изменяющие программные файлы. Алгоритм работы этих вирусов состоит в том, что они создают для запускающих командных файлов файлы-спутники, имеющие то же самое имя, но с расширением более высокого командного порядка. При запуске такого файла ЭВМ первым запускает файл, имеющий самый высокий уровень порядка, т. е. вирус, который затем запустит и командный файл.

2.6.2. Вирусы-“черви” (worm) — вирусы, которые распространяются в компьютерной сети и, так же как и вирусы-“спутники”, не изменяют “родительские” программы, файлы или секторы на дисках. Они проникают в память компьютера из компьютерной сети и, вычисляя адреса других компьютеров, рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках операционной системы, но могут и вообще не обращаться к ресурсам вычислительной системы (за исключением оперативной памяти).

2.6.3 “Паразитические” — все вирусы, которые при распространении своих копий обязательно изменяют содержимое программ, файлов или дисковых секторов. В эту группу относятся все вирусы, которые не являются “червями” или “спутниками”.

2.6.4 “Студенческие” — крайне примитивные простые вирусы, содержащие большое число ошибок в алгоритме их строения (безграмотно написанные) и вызывающие локальные “эпидемии”. Как правило, такие вирусы не получают широкого распространения, быстро обнаруживаются и уничтожаются, однако, успев причинить вред в районе своего размножения.

2.6.5 “Stealth”-вирусы (вирусы-невидимки или маскирующиеся вирусы), представляющие собой весьма совершенные программы, которые при исправлении пораженных программ подставляют вместо себя здоровые программы или их части. Кроме того, эти вирусы при обращении к программам используют достаточно оригинальные алгоритмы, позволяющие “обманывать” антивирусные программы. Эти алгоритмы, скрывающие (маскирующие) присутствие вируса на зараженной машине, нельзя обнаружить, например, просто просматривая файлы на диске. Их создатели применяют весьма разнообразные способы маскировки, начиная от простейшего перехвата более 20 функций DOS (вирус “V-4096”) и кончая маскировкой на уровне дискового драйвера (семейство “Dir”), на уровне прерывания Int 13h (вирус “EXE-222”) или даже на уровне контроллера винчестера (вирус “Htm”). Заметим, что первые вирусы не обладали такими возможностями и их легко можно было обнаружить при визуальном просмотре исполняемых файлов в зараженной компьютерной среде. Применение даже простейших антивирусных средств немедленно останавливало распространение таких вирусов, и они в последующем перестали использоваться преступниками. Появление антивирусных программ привело к новому витку в развитии технологии написания вирусов, где появление вирусов-невидимок стало естественным шагом в таком развитии. Вирусы, использующие приемы маскировки, нельзя увидеть средствами операционной системы. Например, если просмотреть зараженный файл, нажав клавишу F3 в системе Norton Commander, то на экране будет показан файл, не содержащий вируса. Это происходит потому, что вирус, активно работающий вместе с операционной системой, при открытии файла на чтение немедленно удалил свое тело из зараженного файла, а при закрытии файла заразил его опять. Это только один из возможных приемов маскировки, существуют и

другие. Таким же способом маскируются и загрузочные вирусы. При попытке прочитать зараженный BOOT сектор они подсовывают оригинальный, незараженный.

Способность к маскировке оказалась слабым местом Stealth-вирусов, позволяющим легко обнаружить их наличие в программной среде компьютера. Достаточно сравнить информацию о файлах, выдаваемую DOS, с фактической, содержащейся на диске: несовпадение данных однозначно говорит о наличии вируса, т. е. способность к маскировке демаскирует эти вирусы [39, с. 8-9].

2.6.6 Вирусы-“призраки” (мутанты) — достаточно трудно обнаруживаемые самокодирующиеся вирусы, не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же вируса-“призрака” не будут иметь ни одного совпадения. Это достигается не только шифрованием основного тела вируса, но и модификациями кода программы-расшифровщика. Иными словами, вирусы-мутанты содержат в себе алгоритмы шифровки-расшифровки, обеспечивающие то, что два экземпляра одного и того же вируса, заразившие два файла, не имеют ни одной повторяющейся цепочки байт (ни одного совпадения)! Проблема поиска и удаления этого и предыдущего классов вирусов заставляют вирусологов отходить от классических антивирусных программных средств, анализирующих сигнатуры известных вирусов, и искать новые методы борьбы с ними [39, с. 9].

2.6.7 Комбинированные вирусы. Вирусы, имеющие отдельные признаки вирусов, рассмотренных нами выше, в определенной алгоритмической совокупности. Например, к этой группе специалистами относятся вирусы, обнаруженные в ноябре 1994 г. в российских компьютерных системах, — вирус OneHalf (“половинка”) и его разновидности OneHalf.3544 и OneHalf.3577, которые представляют собой категорию очень опасных полиморфных файлово-загрузочных стелс-вирусов [41, с. 2].

Специалисты приходят к единому мнению о том, что, по-видимому, в перспективе будут появляться принципиально новые виды “вирусов”. Например, такие, как “троянский конь” в электронных цепях вирусного типа. В данном случае будет иметь место уже не вирусное программное средство, а вирусное микроразнообразие, которым является интегральная микросхема (“чип”), которая является неотъемлемой частью любого компьютерного устройства. Конечно, ничто не может непосредственно “заразить” микросхему, но ведь можно “заразить” компьютерную систему, используемую для программирования и серийного производства микросхем [2, с. 149; 77, с. 35; 79, с. 3].

Рассмотрим более детально пути распространения компьютерного “вируса”. Они основываются на способности “вируса” использовать любой носитель передаваемых данных в качестве “средства передвижения”, т. е. с начала заражения имеется опасность, что ЭВМ может создать большое число средств передвижения и в последующие часы вся совокупность файлов и программных средств окажется зараженной. Таким образом, дискета или магнитная лента, перенесенная на другие ЭВМ, способны “заразить” их и наоборот, “заражение” происходит, когда “здоровая” дискета или магнитная лента вводится в “зараженный” компьютер. Удобными для распространения обширных “эпидемий” оказываются телекоммуникационные сети. Достаточно одного контакта, чтобы персональный компьютер был “заражен” или “заразил” тот, с которым контактировал. Однако самый частый способ “заражения” — это копирование программ, что является обычной практикой у пользователей персональных компьютеров. Скопированными оказываются и “зараженные” программы.

Как правило, с первой компьютерной “эпидемией” многие авторы научно-популярной литературы связывают имя Роберта Морриса, студента Корнеллского университета США, в результате действий которого “зараженными” оказались важнейшие компьютерные сети восточного и западного побережий США. “Эпидемия” охватила более 6 тыс. компьютеров и 70 компьютерных систем. Пострадавшими оказались, в частности, компьютерные центры НАСА, Ливерморской лаборатории ядерных исследований, Гарвардского, Питсбургского, Мэрилендского, Висконсинского, Калифорнийского, Стэнфордского университетов [2, с. 294]. Однако изобретателем “вируса” является другой человек. В августе 1984 г. сотрудник Лехайского университета (США) Фред Коуэн, выступая на VII конференции по безопасности информации, рассказал про свои опыты с тем, что один его друг назвал “компьютерным вирусом” [39, с. 3]. Когда началось практическое применение “вирусов”, неизвестно, поскольку банки, страховые компании, предприятия, учреждения, организации, обнаружив, что их компьютеры “заражены вирусом” и

опасаясь потери клиентов, не допускали при этом утечки информации и не обращались в правоохранительные органы.

В заключение отметим, что способ совершения преступлений посредством компьютерного вируса может применяться преступником как самостоятельно, так и в составе комплексных способов, которые будут рассмотрены нами далее по тексту. В последнем случае при сочетании этого способа с другими он всегда будет выполнять роль маскирующего фактора в преступлении с целью его сокрытия (как, например, поджог хранилища материальных ценностей после их частичного или полного похищения).

3. “Асинхронная атака”. Такой способ совершения преступления очень сложен и требует хорошего знания операционной системы. Операционная (мониторная) система (operating system (OS)) — это комплекс программных средств, обеспечивающих управление информационными процессами при функционировании компьютерной системы [68, с. 361]. Основная задача операционной системы состоит в обеспечении максимальной производительности компьютерной системы путем реализации различных кибернетических функций: планирования, управления, коммуникации и т. д.

В зависимости от модели и специфики компьютера используют те или иные операционные системы. Организация последних настолько сложна, что они не могут быть созданы одним, даже весьма квалифицированным программистом. Их разработкой занимаются авторские коллективы профессиональных программистов — иногда в течение нескольких лет. Поэтому столь сложные программные продукты практически ни при каких условиях невозможно проверить на предмет достоверности их работы и логической завершенности. Иначе говоря, особенности функционирования операционной системы при всех условиях остаются неизвестными. Этим и пользуются преступники при организации “асинхронных атак”.

Используя асинхронную природу функционирования операционной системы, преступник заставляет последнюю работать при ложных условиях, из-за чего управление обработкой информации частично или полностью нарушается. Если преступник, совершающий “асинхронную атаку”, достаточно искусен, то он может использовать данную ситуацию, чтобы внести изменение в операционную систему или направить ее функционирование на выполнение своих корыстных целей, причем вне операционной системы эти изменения не будут заметны.

Один из простейших способов “асинхронной атаки” основан на том, что при обработке любого шага задания возможно обнаружение ошибок, допущенных при программировании. В этом случае выполнение задачи заканчивается, и на печатающее устройство или дисплей выводится сообщение об ошибке: происходит процесс автоматического прерывания (interrupt), представляющий собой совершение операции процессором, при которой регистрируется его состояние, предшествующее прерыванию, и устанавливается новое его состояние [68, с. 290]. То есть в компьютерной системе активируется сигнал, по которому процессор прерывает выполнение текущей последовательности команд и передает управление на программу-обработчик прерывания. После устранения ошибки вся процедура прохождения задачи повторяется. Различают 23 основных прерывания в работе средств компьютерной техники. Например:

- 1) аппаратное прерывание (hardware interrupt) — заключается в прерывании по ошибке при выполнении команды или в прерывании от внешнего устройства;
- 2) асинхронное прерывание (asynchronous system trap) — прерывание, возникновение которого не привязано к определенной точке программы: внешнее прерывание и прерывание, связанное с работой другого процесса;
- 3) программное прерывание (software interrupt) — прерывание, вызванное управляющей машинной командой: причинами прерывания могут быть ошибки в программе (например, деление на ноль, переполнение, нарушение защиты);
- 4) внешнее прерывание (external interrupt) — прерывание, инициируемое внешним устройством, не входящим в состав центрального процессора; прерывание от внешнего устройства [68, с. 290-291].

Объемные, хорошо спроектированные программы обычно устроены так, что через определенное время обработки задачи соответствующий этап ее прохождения со всей вспомогательной информацией записывается на физический носитель. Тогда в случае ошибки нет необходимости

задачу “прогонять” сначала; это делается лишь с последнего безошибочного этапа. “Асинхронная атака” здесь состоит в обеспечении доступа (санкционированного и несанкционированного) к таким промежуточным записям и внесении в них различных изменений, а также в намеренном создании ошибки (чтобы решение вернулось к прежнему этапу и включало в себя произведенные изменения). Это лишь простейшие варианты использования “асинхронной атаки”. Для квалифицированного специалиста-преступника выбор здесь достаточно широк.

Иногда, чтобы внести изменения в операционную систему, преступникам приходится похищать физические носители машинной информации и работать с ними на другом персональном компьютере, а затем тайно возвращать их на место. Иными словами, этот способ совершения преступления основан на совмещении команд двух и более пользователей, чьи программы ЭВМ выполняет одновременно (параллельно) и одной из которых является программа преступника [94, с. 45].

4. Моделирование. Для совершения компьютерных преступлений все более характерным становится использование преступником способа компьютерного моделирования: моделирования поведения устройства или системы с помощью программного обеспечения [68, с. 203]. Моделируются как те процессы, в которые преступники хотят вмешаться, так и планируемые способы совершения преступления. Например, в последнее время преступниками с целью ухода от налогообложения все чаще начинают использоваться так называемая “черная” или “двойная” бухгалтерия, основанная на существовании двух одновременно работающих программ автоматизированного бухгалтерского учета с взаимоперетекающими контрольными данными. В данном случае одна из них функционирует в легальном (законном) режиме, а другая — в нелегальном для проведения незаконных (теневых) бухгалтерских операций. Иногда одновременно с этими программами существует и третья, которая используется только одним лицом, входящим в состав преступных групп и сообществ, выполняющим роль бухгалтера по ведению общественной кассы преступной группировки (“общака”).

Ярким примером этому могут служить материалы одного из уголовных дел, расследование которого было завершено в 1995 г. московскими правоохранительными органами. Рассмотрим его подробнее.

В июне 1994 г. была задержана организованная преступная группа из числа руководителей Московского Т. банка (включая председателя правления банка), которая с ноября 1993 г. осуществляла хищения денежных средств путем заключения фиктивных кредитных договоров со Сбербанком РФ, его отделениями и другими коммерческими банками. При этом использовались нелегальные корреспондентские счета, открытые Московским Т. банком в ряде банков г. Москвы. Таким образом было похищено 18 млрд. руб., которые были проконвертированы и зачислены на счета иностранных фирм в зарубежных банках. Из указанной суммы 22 млн. руб. руководство Московского Т. банка по расходным ордерам обналичило и присвоило.

В данном случае механизм преступной операции достаточно сложен. Преступниками был организован банк с двойной структурой: официальной, легально зарегистрированной в Центральном банке России и имеющей правление со всеми необходимыми службами, но являющейся лишь крышей для теневой, реальной структуры банка, распоряжающейся денежными средствами. Корреспондентский счет в ЦБР официальной структуры банка фактически находился без движения, в то время как теневая структура активно функционировала — было организовано движение денежных средств по открытым ее нелегальным корреспондентским счетам в коммерческих банках Москвы. Теневая структура вложила в уставный капитал банка большую сумму денег, фактически купив его. Она имела свое собрание пайщиков и собственного председателя правления банка. Единственная ее преступная цель была — набрать как можно больше кредитов юридических лиц за минимальный период времени. Все похищенные таким образом денежные средства переводились на счета подставных коммерческих фирм в Р. банке, конвертировались и переводились за рубеж по фиктивным импортным контрактам [12, с. 7-8].

Моделирование в криминальных целях, по нашему мнению, будет шириться по мере снижения стоимости персональных компьютеров и увеличения количества предлагаемых моделирующих программ. Так, в настоящее время уже эксплуатируются специальные языки моделирования, одним из которых является GPSS, позволяющий создавать полноценные пользовательские программные продукты, в том числе и для криминальных целей.

В данном случае особое внимание следует обратить на появившиеся в последнее время в свободной продаже прогрессивные регенерируемые программы игровых моделей защиты, т. е. модели, в которых имеется минимум две стороны. Первая из которых строит систему защиты информации, а вторая — систему ее преодоления (моделируются как возможные действия, так и конкретные прогнозируемые ситуации). Игра начинается с построения первой стороной (потерпевшей) некоторой системы защиты. После чего вторая сторона (преступник) начинает ее преодолевать, а первая — строить новую, более совершенную. Если вторая сторона преодолела защиту, построенную первой стороной, раньше того момента, как построена новая, то первая сторона считается проигравшей. Если к моменту преодоления защиты у первой стороны имеется новая система защиты, то она выиграла. Независимо от исхода первого раунда игра продолжается. Критерием эффективности системы защиты при данном подходе является функция двух аргументов — времени, затрачиваемого первой стороной на построение системы защиты, и времени, затрачиваемого второй стороной на ее преодоление. Можно рассмотреть и более сложные игровые модели, учитывающие не только время, но и стоимость защищаемой информации, затраты на разработку/преодоление системы защиты и т. д. В подобных моделях стоимость информации, защищаемой первой стороной, уменьшается со временем, а одним из аргументов критерия эффективности этой защиты является остаточная стоимость информации после ее “вскрытия” (уничтожения, обхода) второй стороной [22, с. 127-128]. Таким образом происходят тренировки преступников, готовящихся совершить преступление.

4.1 Реверсивная модель. Разновидность способа моделирования. Заключается в следующем. Создается модель конкретной системы, на которую планируется совершить нападение. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем, исходя из полученных данных, подбираются максимально приближенные к действительности желаемые результаты. После чего модель совершения преступных действий “прогоняется” назад, к исходной точке, и преступнику становится ясно, какие манипуляции с входными-выходными данными нужно совершить, чтобы достичь желаемого корыстного результата. Обычно, “прокручивание” модели вперед-назад осуществляется преступником многократно, чтобы выявить возникающие ошибки и просчеты в механизме планируемых преступных действий. Таким образом осуществляется оптимизации действий при проведении криминальных “операций” и минимизируется возможный при этом риск их “провала”.

Классическим примером из зарубежной практики является дело собственника компьютерной службы, бухгалтера по профессии, служившего одновременно бухгалтером теплоходной компании в Калифорнии, США, специализировавшейся на перевозке овощей и фруктов. Он обнаружил пробелы в деятельности ревизионной службы компании и решил использовать этот факт. На компьютере своей службы он смоделировал всю бухгалтерскую систему компании. Прогнав модель вперед и обратно, он установил, сколько фальшивых счетов ему необходимо открыть и какие бухгалтерские операции следует осуществить.

Этот человек организовал 17 подставных компаний и, чтобы создать видимость реальности ситуации, обеспечил каждую из них своим расчетным счетом, начав затем финансовые операции. Модель бухгалтерского баланса подсказала ему, что при имеющихся пробелах в ревизионной службе 5%-ное искажение данных учета не будет заметно. Его действия оказались настолько успешными, что в первый год он похитил 250 тыс. долл. США без какого-либо нарушения финансовой деятельности компании. К тому времени, когда увеличенные выплаты вызвали подозрение у руководства банка, осуществлявшего обслуживание компании, сумма хищения составила миллион долларов [2, с. 154].

4.2 “Воздушный змей”. Данный способ используется преступником для начисления и получения незаконных избыточных денежных сумм на счетах при автоматическом пересчете рублевых остатков за счет предварительного увеличения остаточных сумм, что достигается посредством временного переноса средств со счетов с другим кодом и их последующего возвращения на исходные счета.

Механизм совершения хищения денежных средств заключается в следующем. В двух или нескольких банках открываются счета на некоторые несущественные суммы. Далее деньги переводятся из одного банка в другой и обратно с постепенным увеличением сумм. До того как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходит извещение в данный банк о том, что общая сумма покрывает требование о первом переводе. Этот цикл многократно повторяется (“воздушный змей” поднимается все выше и выше) до тех пор, пока на нужном счете не оказывается достаточная сумма денег (фактически она постоянно

“перескакивает” с одного счета на другой, как бы “парит в воздухе”, постоянно увеличиваясь в размерах). При достижении определенной величины деньги оперативно снимаются с закрытием счетов и впоследствии — отмываются (легализуются). Обычно, как показывает практика, в подобные преступные операции преступниками включается большое число банков. Это обусловлено следующими причинами:

- 1) скорость и величина накопления похищаемой суммы прямо пропорциональны количеству счетов и банков;
- 2) число платежных поручений не достигает подозрительной частоты.

По мнению специалистов, управлять подобным процессом можно только с помощью компьютерной системы, используя элементы моделирования преступной ситуации [76]. Данный способ требует очень точного расчета, но для двух банков его можно осуществить и без использования средств компьютерной техники.

Отметим, что прототипом для возникновения и развития рассматриваемого способа совершения компьютерного преступления, на наш взгляд, послужили хорошо отработанные на практике преступные махинации с поддельными кредитовыми авизо, используемые для хищения денежных средств и основанные на некоторых особенностях безналичных банковских расчетов. Специфика последних заключается в том, что в отличие от наличных платежей при безналичных расчетах и, в частности, банковском переводе средств от плательщика к получателю, момент выхода денег из владения плательщика не совпадает ни по времени, ни в пространстве с моментом получения их адресатом платежа. В этом случае передача денег состоит как бы из двух взаимосвязанных необходимых элементов: с одной стороны, деньги должны быть списаны со счета отправителя, с другой — зачислены на счет получателя. Только при одновременном наличии этих двух условий перевод считается осуществленным. Этим и пользуются преступники. Так, в случае использования ими поддельного кредитового авизо деньги не списываются со счета плательщика в коммерческом банке, осуществляющем финансовую операцию, и не отражаются на балансе расчетно-кассового центра (РКЦ), в котором находится корреспондентский счет плательщика. Таким образом, перевод денег отсутствует, несмотря на то, что данная сумма зачисляется РКЦ на корреспондентский счет коммерческого банка — получателя платежа. Именно эта операция и создает неверное представление о возникновении денег “из ничего”, “из воздуха”. В действительности же РКЦ, зачисляя деньги на корсчет банка-получателя, фактически незаконно финансирует его и фирму-получателя, одновременно являясь потерпевшим.

4.3 “Ловушка на живца” (“подсадная утка”). Еще одна разновидность способа моделирования. Заключается в том, что преступником создается специальная программа, которая затем записывается на физический носитель и под любым предлогом вручается или подкидывается потерпевшей стороне с расчетом на то, что ее по каким-либо причинам заинтересует данная программа и она постарается ознакомиться с ней. Алгоритм программы построен таким образом, что при ее работе в определенный момент времени автоматически моделируется системная поломка компьютерной системы, на которой был запущен данный программный продукт с целью проверки его качества и работоспособности. После чего указанная программа записывает данные и информацию, которые могут заинтересовать преступника. После того как программа выполнила заданные ей функции, она изымается у потерпевшей стороны с использованием различных способов. Обычно, по причине высокой стоимости программного обеспечения, организации легко соглашаются на приобретение данной программы, которая иногда предоставляется преступником, якобы с целью ее рекламы, бесплатно или за незначительное вознаграждение.

5. Копирование (тиражирование). Этот способ совершения преступления заключается в действиях преступника, направленных на незаконное копирование (тиражирование) программных средств компьютерной техники, а также топологий интегральных микросхем. Под топологией интегральной микросхемы с уго-ловно-правовой точки зрения понимается зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы (ИМС) и связей между ними, а под самой ИМС понимается микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функций электронной схемы, элементы и связи которой неразрывно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие [28, ст. 1]. Копирование осуществляется преступником посредством воспроизведения данных с сохранением исходной информации на любом материальном носителе. Например, процесс копирования файлов, осуществляется преступником посредством обмена наборами данных между внешними

(периферийными) устройствами компьютерной системы с использованием стандартных программных средств операционной системы компьютера (либо иных), в частности в СМ ЭВМ — программой PIP, а в MS-DOS ПЭВМ — программой COPY [68, с. 170].

В данном случае под файлом понимается идентифицированная совокупность экземпляров описанного в программе типа данных, находящихся во внешней памяти и доступных программе посредством специальных операций [68, с. 422].

По мнению специалистов, с криминалистической точки зрения повышенная социальная опасность компьютерных преступлений, совершаемых с использованием способа копирования, обусловлена следующими обстоятельствами:

- 1) высокой плотностью данных и информации, записанных на материальном носителе либо находящихся в оперативной памяти компьютерной системы;
- 2) быстротой и простотой процесса совершения Преступных действий;
- 3) достаточно широкими возможностями дублирования любых массивов данных без оставления следов на месте происшествия [82, с. 11].

Существуют две разновидности применения преступником указанного способа. В первом случае копирование осуществляется посредством законного (санкционированного) доступа к средствам компьютерной техники, во втором — посредством несанкционированного доступа с использованием способов, рассмотренных нами выше. В последнем случае будет иметь место применение комплексного метода совершения преступления (совокупность двух и более способов совершения преступления), которые будут рассмотрены нами в следующей, пятой группе.

Используя способ копирования данных и информации, преступникам, в частности, удается получать законные денежные вознаграждения за фиктивное выполнение заранее указанных в договоре услуг, например по разработке программного обеспечения. Обычно в таких случаях между преступником (исполнителем) и потерпевшей стороной (заказчиком) заключается законный договор на разработку компьютерных программ, которые фактически преступником не разрабатываются, а незаконно копируются (присваиваются) посредством различного рода манипуляций. Приведем один из примеров и рассмотрим механизм подобных сделок.

Как свидетельствуют материалы уголовного дела, возбужденного по факту хищения денежных средств в особо крупных размерах в отношении ряда работников кооператива “Р.” и коммерческой фирмы “О.”, в июне 1989 г. генеральный директор данной фирмы Л. через посредническую государственную организацию, в полном соответствии с Положением о фирме, заключил контракт с австрийской фирмой “Ф.” об импортной поставке 10 тыс. компьютеров на общую сумму 523 млн. руб., с целью их последующей реализации на внутреннем рынке по существующим ценам, намереваясь в конечном итоге получить с учетом всякого рода накладных расходов чистую прибыль в размере не менее 40 млн. руб. (10% от инвестируемой в сделку суммы). Одновременно с этим он заключил ряд договоров с различными кооперативами г. Москвы о разработке и поставке “О.” оригинального программного обеспечения для оснащения им ожидаемой партии персональных компьютеров, чтобы сбыть покупателям компьютеры с программным обеспечением с целью получения дополнительной прибыли. Одним из таких кооперативов явился кооператив “Р.”.

Не имея фактической возможности осуществить разработку программного обеспечения, члены указанного кооператива совместно с неработающими в кооперативе лицами получили в банке перечисленные “О-м” на расчетный счет “Р.” согласно договору 4 млн. руб., которые присвоили. В дальнейшем через работников НПО “П-ка” они произвели тиражирование известной сервисной программы “Norton Commander” (производства США) на 1,5 тыс. дискет и поставили их “О.”. Таким образом, формально условия договора были выполнены, т. е. фирма-заказчик получила необходимое количество дискет с программным обеспечением. Связанные с этой операцией затраты составили 60 тыс. руб., кроме того, 100 тыс. руб. было передано Л. и 400 тыс. руб. — его заместителю, а остальные деньги поделены. Сам Л. пояснил на следствии, что ему было безразлично, какое программное обеспечение будет поставлено по договору, т.к. затраты окупятся бы в результате продажи персональных компьютеров, оснащенных программным обеспечением, а заказчики, учитывая дефицит на компьютерную технику подобного класса, приобрели бы ее с

любым программным обеспечением. Поэтому договаривающиеся стороны каких-либо финансовых претензий друг к другу не имели.

В ноябре того же 1989 г. Л. заключил с тем же кооперативом "Р." повторный договор аналогичного типа. В нем, как и в первом случае, рассмотренном нами выше, не производя разработку программного обеспечения, работники кооператива уже с ведома Л. растиражировали программу "Autocad" (производства США) и поставили "О." еще 1,5 тыс. дисков, присвоив из перечисленных согласно договору 4 млн. руб.

6. Преодоление программных средств защиты. Этот способ является вспомогательным и предназначен для подготовки совершения компьютерного преступления способами, рассмотренными нами выше. Он заключается в действиях преступника, направленных на умышленное преодоление программных средств защиты компьютерной техники и имеет несколько разновидностей.

6.1 Незаконное создание копии ключевой дискеты. Является одним из способов преодоления средств защиты компьютерной техники. Осуществляется преступником путем электромагнитного переноса всей структуры и информации, расположенных на ключевой дискете-оригинале, защищенной от копирования программными средствами, на дискету-копию, в результате чего аутентификационная часть системы защиты воспринимает копию ключевой дискеты как оригинал. Для получения работоспособной дискеты-копии достаточным условием является полное повторение дискеты-оригинала со всеми находящимися на ней характеристиками, проверяемыми аутентификационной частью системы защиты. Установление этих характеристик и выбор правильного метода их копирования являются главными задачами, которые решаются преступником в данном случае. Заметим, что решение указанных задач для каждой системы защиты требует определенного профессионального опыта и непосильно лицам, впервые столкнувшимся с ними. Эти задачи могут быть решены только двумя способами: программным и программно-аппаратным.

При программном — копии дискет изготавливаются с помощью специальных программных средств типа DISKCOPY или COPYII PC (89, с. 80-83]. В некоторых случаях для обеспечения качественной работоспособности дискеты-копии, полученной с использованием вышеперечисленных программ, для ее дальнейшей отладки используется программное средство DISK EXPLORER [89, с. 72-80].

При программно-аппаратном способе реализации дискеты копируются с помощью специальных программно-аппаратных устройств типа платы COPYII PC OPTION BOARD DELUXE. Этот способ является достаточно простым по сравнению с первым и позволяет (при хорошей квалификации преступника) для большинства известных систем защиты создавать копии ключевых дискет за 5-7 минут [89, с. 106].

6.2 Модификация кода системы защиты. Заключается в модификации (изменении) кода модуля системы защиты, выполняющего следующие функции:

- 1) проверку ключевой дискеты;
- 2) корректировку счетчика установок на жесткий магнитный диск (винчестер), защищенного от копирования программного средства с ключевой дискеты;
- 3) проверку санкционированности запуска защищенного информационного ресурса.

Обычно модификация сводится к простому обходу кода модуля, выполняющего перечисленные выше функции. В некоторых случаях модуль подвергается существенным изменениям, позволяющим обойти проверки систем защиты. Основная задача заключается в определении логики работы модуля. Последующее же внесение изменений в него остается "делом техники" и не представляет особого труда для преступника, разгадавшего логику построения защиты. Чтобы выполнить указанные действия, необходимо провести трассировку (распечатку выполняемых программой команд и изменений переменных или информации о других событиях, связанных с выполнением программы, — см.: 68, с. 406) или дисассемблирование (программный перевод объективного программного модуля в эквивалентную программу, созданную на языке программирования Ассемблер, — см.:

68, с. 85) этого модуля с целью определения и деактивации той его части, которая выполняет защитные функции. Эти действия достаточно трудоемкие и могут быть выполнены только лицом, имеющим достаточный опыт и квалификацию по специальности системного программиста или аналитика. Время преодоления системы защиты в данном случае будет определяться неделями [89, с. 108].

6.3 Моделирование обращений к ключевой дискете. Многие программные средства защиты информации логически используют не прямую, как это принято, работу с контроллером (специализированным процессором, предназначенным для управления внешними (периферийными) устройствами и позволяющим освободить центральный процессор от выполнения этих функций, — см.: 68, с. 166), а средства системы BIOS (Basic Input-Output System — базовой системы ввода-вывода информации, представляющей собой часть программного обеспечения, входящего в состав компьютерной системы, отвечающей за тестирование и начальную загрузку, поддержание стандартного интерфейса ЭВМ с периферийными устройствами и аппаратно воплощенную в постоянном запоминающем устройстве (ПЗУ), — см.: 39, с. 162) — прерывание 13h. Этим и пользуются преступники, программно моделируя результат обращения ЭВМ к ключевой дискете путем перехвата прерывания 13h. Время преодоления защиты составляет при этом от одного дня до одной недели [89, с. 109].

6.4 Использование механизма установки/снятия программных средств защиты информации. Некоторые программные средства защиты используют при их установке на винчестер привязку к физическому расположению файла на диске. Одновременно с этим в алгоритм работы этих средств включаются функции, обеспечивающие их снятие с винчестера с одновременным восстановлением исходного состояния счетчика установок, т. к. защищенные программные средства нельзя перемещать путем использования стандартных средств сохранения/восстановления файлов. Используя же функцию снятия защищенной программы с винчестера, можно тем самым получить возможность незаконного тиражирования защищенных программных продуктов в корыстных целях. Для этого преступником осуществляется следующий алгоритм действий:

- 1) получается санкционированный или несанкционированный доступ к защищенному программному средству, расположенному на винчестере;
- 2) анализируется структура размещения и содержание всех файлов (в том числе скрытых), созданных на винчестере программой установки;
- 3) выполняется копирование защищенной программы с винчестера (при этом восстанавливается исходный счетчик установок);
- 4) восстанавливаются сохраненное состояние системы и ее содержимое.

В результате всех этих действий получается ключевая дискета с исходным счетчиком установок и нелегальная копия программного продукта на винчестере. Отметим, что данный процесс сохранения/восстановления информации требует от преступника знаний структуры файловой системы DOS (дискетной операционной системы), умений использования программных средств из комплекта Norton Utilities Advanced Edition и аппаратного устройства записи информации на магнитную ленту — стриммера, позволяющего сохранить/восстановить все содержимое диска и прежнюю структуру размещения на нем всей информации. Время преодоления защиты в этом случае составляет порядка нескольких часов [89, с. 10].

6.5 Снятие системы защиты из памяти ЭВМ. Данный способ заключается в следующем. Система защиты через определенное время автоматически загружает в память ЭВМ защищаемое программное средство, расшифровывает его и передает управление расшифрованному коду. В этот момент в оперативной памяти компьютерной системы находится полностью расшифрованная программа и для получения несанкционированной копии остается только сохранить ее в каком-либо файле. Этим и пользуются преступники. Например, получение несанкционированной копии командно-управляющего COM-файла осуществляется путем перехвата первого прерывания (например, INT 21H), возникающего в ходе выполнения защищаемой программы. А для получения несанкционированной копии EXE-файла — осуществляются следующие действия:

- 1) активизируется защищенная программа, начиная с ее различных адресов с: сохранением образа памяти в двух файлах;
- 2) путем сравнения последних в п. 1, определяются смещения перемещаемых адресов с одновременным их вычислением;
- 3) формируется таблица перемещений по п. 2 и заголовок EXE-файла.

Для этих целей преступниками используется специальное инструментальное программное средство CERBERUS KIT. Время преодоления защиты при этом составляет несколько часов [89, с. 111].

Считаем необходимым отметить следующее. Посредством использования способов копирования при совершении компьютерного преступления, преступникам удается получать несанкционированные копии данных и информации с последующим их использованием в корыстных целях. Например, по данным зарубежной печати, рост популярности среди населения ФРГ кредитных электронных карточек привел к тому, что уже в 1990 г. было зарегистрировано 4601 преступление, связанное с их подделкой путем незаконного копирования оригиналов с использованием средств компьютерной техники; в США — был изобличен преступник, который самостоятельно изготовил и использовал в корыстных целях 7 тыс. персональных кредитных карточек. В результате чего преступниками без особого труда похищались крупные наличные суммы денег из уличных банкоматов. При этом, по данным уголовной полиции ФРГ, лишь 31% преступников были обнаружены и уличены правоохранительными органами в содеянном [46, с. 5; 76, с. 8-9]. По нашему мнению, аналогичная ситуация складывается и в России. Об этом, в частности, свидетельствуют и данные оперативно-розыскной деятельности по отдельным регионам страны, в которых начали активно применяться безналичные расчеты с использованием “электронных денежных средств”.

Рассмотренные нами выше способы совершения компьютерных преступлений, относящиеся к подгруппе преодоления программных средств защиты представляют собой переходную категорию между первыми четырьмя группами способов и пятой группой. - К пятой и последней группе способов совершения компьютерных преступлений мы относим комплексные методы, под которыми понимаются использование преступником двух и более способов, а также их различных комбинаций при совершении преступления. Эти способы были подробно рассмотрены нами в первых четырех группах. Некоторые из них оказываются вспомогательными, работающими на основной способ, выбранный преступником в качестве центрального, исходя из конкретной преступной цели и ситуации. Проиллюстрируем это на конкретных примерах по материалам уголовных дел.

Например, с использованием способов несанкционированного доступа и манипуляций ценными данными в конце сентября 1993 г. в г. Москве было совершено покушение на хищение в особо крупных размерах 68 млрд. 309 млн. 768 тыс. руб. из Главного расчетно-кассового центра (ГРКЦ) Центрального банка России (ЦБР), расследованное Следственным управлением ГУВД г. Москвы. Криминальная операция была организована следующим образом. В правоохранительные органы поступила информация о незаконном зачислении на корреспондентский счет коммерческого банка (КБ) “С-вест” денежных средств в размере 10 млрд. 70 млн. 100 тыс. рублей. Предварительной проверкой было установлено, что указанная сумма денег поступила 15 сентября 1993 г. с одного из счетов РКЦ г. Москвы. С этого же счета в тот же день незаконно были списаны и сразу же зачислены на корреспондентские счета восьми московских коммерческих банков денежные средства на общую сумму 58 млрд. 239 млн. 668 тыс. руб.

В ходе дальнейшей проверки было установлено, что зачисление средств произошло из-за умышленного добавления к массиву входных данных программного комплекса “Операционный день РКЦ” дополнительных записей электронных банковских документов. Эти документы впоследствии были обработаны компьютером Межрегионального центра информатизации при ЦБР и сделаны проводки по начислению средств. Фальшивые записи были введены под номером участника, обслуживаемого ГРКЦ ЦБР по Москве, по выписке, которая формируется после передачи электронных документов из ГРКЦ в МЦИ ЦБР.

На умышленность проведенной операции прямо указывает факт несохранения электронных банковских документов за 16 сентября 1993 г., вопреки установленным правилам [12, с. 6-7].

В ходе проведенного следствия выяснилось следующее. Указанные электронные операции преступниками были осуществлены с использованием широко распространенных средств компьютерной техники: персональных компьютеров моделей IBM PC/AT-286 и IJF SUPER286, печатающих устройств (принтеров) моделей Citizen и HP Desk Jet-500C, дискет (магнитных носителей машинной информации) и листингов (распечаток). Один из компьютеров был подключен через модемный модуль (модем) к городской телефонной сети и имел зарегистрированный пользовательский номер абонента в лице коммерческой фирмы "П.-Т.". Используя в качестве маскировки способ манипуляции данными, преступниками было произведено дробление указанной выше суммы на неравные долевые части с зачислением на соответствующие корреспондентские счета КБ. При этом коммерческие банки преступниками подбирались с таким расчетом, чтобы без существенных препятствий в кратчайший срок можно было бы снять переведенную на счет сумму наличными. Таким правом обладают только крупные коммерческие банки, оперативно работающие со своими клиентами. Заметим, что для дальнейшего сокрытия преступления, преступниками был применен следующий прием — они не сразу перевели раздробленные суммы на заранее подготовленные счета, а в течение нескольких часов перекидывали данные суммы по разным счетам клиентов, обслуживаемых ГРКЦ Центрального банка России по г. Москве, прогоняли их по цепочкам счетов.

В результате принятых правоохранительными органами мер, 15 октября 1993 г. в КБ "С-вест" была предотвращена попытка незаконного получения 10 млрд. 70 млн. 100 тыс. руб. по двум фиктивным платежным документам, подготовленным с использованием компьютерной техники, представленным директором дочернего предприятия "А. Брок.". На следующий день все незаконно начисленные на корреспондентские счета коммерческих банков денежные средства были стонированы [12, с. 6-7].

В качестве примера можно привести и классическую схему "взлома" компьютерной сети австрийского банка отечественными преступниками по заказу московской коммерческой структуры в целях блокирования работы данного банка в течение суток.

Как правило, подобная криминальная операция готовится в течение нескольких месяцев и обходится "заказчику" в 25 тыс. долл. На первоначальном этапе вербуются лица (путем подкупа или вымогательства) из числа сотрудников банков: один из которых впоследствии будет потерпевшей стороной, вторые — получатели слагаемых похищенной суммы, а третьи — банки, в которых похищенные суммы будут обналичены и сняты со счетов (иногда с одновременной конвертацией в ту или иную валюту).

Далее, для подстраховки вербуется специалист телефонной станции населенного пункта, из которого будет осуществляться общее управление криминальной операцией. В данном пункте на подставное лицо снимается квартира, в которой устанавливается необходимое оборудование, включающее в себя компьютеры, средства связи и автономные источники электропитания на случай внезапного обесточивания бытовой электросети. В данной квартире будет работать главный исполнитель. Помимо него, в разных районах населенного пункта задействуются еще порядка 10-12 персональных компьютеров с операюрами, т. к. одна ЭВМ не обеспечит успешное проведение операции. Таким образом, количество участников "операции" может достигать 30 человек. Однако об истинной цели знают лишь 5 человек — главный исполнитель и его непосредственные юмощники, тогда как остальные используются "втемную" — иждый из них знает лишь о своей конкретной задаче.

Криминальная операция электронного взлома называется "бухингом" и осуществляется не через компьютерную сеть, где легко быть обнаруженным, а напрямую — по серийному; телефонному номеру типа "09" (многоканальному), по котором] могут одновременно работать несколько абонентов. В заданный час "X" 11-13 компьютеров одновременно предпринимают попытку несанкционированного доступа в банковскую сеть потерявшей стороны. При таком количестве одновременно "атакующих" даже самые надежные системы защиты от несанкционированного доступа не успевают адекватно отреагировать на созданную нештатную (аварийную) ситуацию. Это приводит к тому, что только несколько компьютеров отсекаются системой защиты, тогда как остальные получают требуемый доступ. Далее ситуация развивается следующим образом. Один из "прорвавшихся" компьютеров блокирует систему статистики сети, которая фиксирует все попытки доступа. После чего другие "прорвавшиеся" компьютеры не могут быть обнаружены и зафиксированы. Часть из них приступает к непосредственному "взлому" аужного сектора банковской сети, а остальные занимаются фиктивными бухгалтерскими операциями с целью дезорганизации работы банка и сокрытия преступления.

Если в момент “взлома” сети несанкционированный доступ был обнаружен, то, как правило, события начинают развиваться по следующему сценарию, также предусмотренному преступниками, а именно: сотрудник службы безопасности потерпевшего учреждения с помощью специальной аппаратуры связи немедленно посылает запрос на АТС, через которую идет сигнал, с просьбой идентифицировать телефонный номер абонента главного исполнителя. В этом случае начинает действовать сообщник из числа работников АТС, который называет другой абонентский номер, например, ближайшего отделения милиции, в то время как исполнитель — сразу же “выходит” из операции.

Если же “бухинг” проходит успешно, то главный исполнитель в период прохода фиктивных платежных поручений вводит через свой компьютер основное платежное поручение в соответствующий “взломанный” сектор сети банка и ставит его первоочередным на обработку и отправку по указанным адресам. После него регистрируют фиктивные поручения с целью сокрытия основной “проводки”. Сразу после оплаты основного платежного поручения фиктивные дезорганизуют систему взаиморасчетов банка со своими клиентами и на некоторое время полностью парализуют ее. Условно это выглядит следующим образом. В банк “А” (потерпевшая сторона) приходит платежное поручение из банка “В”, у которого с “А” имеются корреспондентские отношения. Операция перевода денежных средств занимает несколько минут. Затем сумма немедленно делится на неравные долевые слагаемые и переводится в банки “С”, имеющие корреспондентские отношения с банком (банками) “В”, но не имеющие таковых с “А”. Данный алгоритм переброса денег повторяется несколько раз с целью последующего сокрытия преступления, после чего суммы переводятся в зарубежные банки, конвертируются в соответствующую валюту, снимаются со счетов и легализовываются. В течение месяца со дня совершения преступления уже “чистые” деньги законным путем переводятся в требуемую страну на счет “заказчика” [36, с. 5].

В последнее время, как свидетельствует анализ уголовных дел, в криминальной среде активизировался процесс легализации преступно нажитых капиталов, мошеннических манипуляций с банковскими чеками, персональными кредитными карточками на основе магнитного носителя и микропроцессорного устройства, а также другими документами перевода безналичных денежных средств в наличные и обратно. В связи с чем преступниками стали использоваться следующие новые комплексные способы, предполагающие собой проведение различных манипуляций с электронными кредитными карточками, которые представляют собой не что иное, как средство компьютерной техники, которое выдается банками всего мира своим клиентам для проведения безналичных расчетно-кассовых операций, например оплаты товаров и услуг. Значительная распространенность и повышенная общественная опасность указанных преступных посягательств убедительно подтверждаются следующими данными: например, в 1991 г. только через систему “Интуркредит” с использованием кредитных карточек было осуществлено более * 1,2 млн. сделок на общую сумму свыше 200 млн. долл. США, при этом около 120 тыс. сделок были признаны по различным причинам недействительными, ущерб составил — свыше 2 млн. долл. В данных случаях преступниками обычно используются комбинации различных способов для осуществления своих корыстных целей. На практике ими активно применяется сочетание многих способов, например “за дураком” и манипуляция данными, выраженные в том, что преступник, обычно работник торговых предприятий и сферы обслуживания, пользуясь невнимательностью клиента (или умышленно отвлекая его — “за дураком”), производит несколько дополнительных несанкционированных оттисков на приемном компьютерном устройстве оплаты услуг или товаров, которые впоследствии используются им для оплаты присвоенных материальных ценностей или услуг.

Иногда преступником используется и метод подделки кредитных карточек путем изготовления их фальшивых копий, посредством дублирования законного оригинала на том компьютерном устройстве, на котором был изготовлен оригинал (что и было рассмотрено нами выше). Здесь мы имеем дело с одновременным использованием способов копирования и “маскарад”, иногда к ним добавляется какой-либо из способов несанкционированного доступа.

В заключение мы хотели бы особо подчеркнуть, что по данным проведенного нами опроса, всего 8% респондентов осведомлено о существовании тех или иных способов совершения компьютерных преступлений, что еще раз подчеркивает актуальность проведенного нами исследования.

Предупреждение компьютерных преступлений

Международный опыт борьбы с преступностью свидетельствует о том, что одним из приоритетных направлений решения задачи эффективного противодействия современной преступной деятельности является активное использование правоохранительными органами различных мер профилактического характера [25]. Последние имеют решающее значение в сложном процессе предотвращения преступлений и представляют собой деятельность, направленную на выявление и устранение причин, порождающих преступления, и условий, способствующих их совершению. По мнению специалистов, результаты профилактической работы при ее правильной организации и целенаправленном осуществлении, оказывают существенное положительное влияние на уровень, структуру и динамику преступности, обеспечивают последовательное снижение количества совершаемых преступлений и имеют важное криминалистическое значение. Это обусловлено тем, что профилактические меры направлены против самих истоков преступности [54]. Поэтому в практической деятельности органов внутренних дел по борьбе с преступностью, по нашему мнению, состоянию профилактической работы должно придаваться особое значение.

В связи с тем что научно-методическим обеспечением практической деятельности правоохранительных органов занимается криминалистическая наука, то, на наш взгляд, разрабатываемые ею в современных условиях научные методы и средства должны способствовать активизации процесса предупреждения преступлений, и особенно их новых видов. По мнению многих ученых-криминалистов, предупреждение преступлений является одной из основных категорий, входящих в определение понятия криминалистики как науки и обуславливающих предмет ее изучения. Так, например, криминалистика определяется как «наука о закономерностях движения уголовно-релевантной информации при совершении и расследовании преступлений и основанных на них методах раскрытия, расследования и предупреждения преступлений [67, с. б]. Поэтому методика предупреждения преступлений является важной составной частью методологии криминалистики и включается в общее понятие методики борьбы с отдельными видами преступлений, к которым относятся и компьютерные преступления.

Между тем, как показывает проведенное нами исследование, многие работники органов внутренних дел и прежде всего следственных аппаратов, непосредственно осуществляющих борьбу с преступностью, слабо подготовлены профессионально для осуществления достаточно трудоемких и сложных мероприятий по предупреждению компьютерных преступлений. На наш взгляд, это в значительной степени обусловлено тем, что в настоящее время не существует сколь-нибудь конкретных и полных по содержанию методических разработок по организации и тактике предупреждения преступлений рассматриваемой категории. Одновременно с этим, принимая во внимание специфичность и новизну компьютерных преступлений, выраженных, в частности, в повышенной трудности их выявления, раскрытия и расследования, считаем необходимым подробно остановиться на исследовании вопросов, касающихся не только криминалистических, но также правовых и организационно-технических аспектов их предупреждения. Необходимость подобного шага подтверждается и зарубежным опытом борьбы с компьютерной преступностью. Большинство зарубежных специалистов прямо указывает на то, что предупредить компьютерное преступление всегда намного легче и проще, чем потом его раскрыть и расследовать.

На основе данных, полученных в ходе анализа отечественной и зарубежной специальной литературы и публикаций в периодической печати по вопросам теории и практики борьбы с компьютерной преступностью, нами выделяются три основные группы мер предупреждения компьютерных преступлений, составляющих в своей совокупности целостную систему борьбы с этим социально опасным явлением, а именно:

- 1) правовые;
- 2) организационно-технические;
- 3) криминалистические.

Рассмотрим каждую из указанных групп более подробно. К правовым мерам предупреждения компьютерных преступлений в первую очередь относятся нормы законодательства, устанавливающие уголовную ответственность за указанные выше противоправные деяния. История развития законодательства зарубежных стран в этом направлении показывает, что впервые подобный шаг был предпринят законодательными собраниями американских штатов

Флорида и Аризона уже в 1978 г. Принятый закон назывался “Computer crime act of 1978” и был первым в мире специальным законом, устанавливающим уголовную ответственность за компьютерные преступления. В частности, в соответствии с ним противоправные действия, связанные с модификацией, уничтожением, несанкционированным доступом или изъятием компьютерных данных, программ или сопутствующей документации признавались преступлением и наказывались пятью годами лишения свободы либо штрафом в размере 5000 долл. или тем и другим одновременно в зависимости от тяжести причиненного жертве ущерба.

Те же действия, совершенные с целью хищения какой-либо собственности, наказывались 15 годами лишения свободы либо денежным штрафом в размере 10000 долл. или и тем и другим одновременно [32, с. 36].

Затем практически во всех штатах США (в 45 штатах) были приняты аналогичные специальные законодательства. Эти правовые акты стали фундаментом для дальнейшего развития законодательства в целях осуществления мер предупреждения компьютерных преступлений. На их правовой базе в первой половине 80-х гг. было разработано федеральное законодательство США, посвященное регулированию правовых вопросов этой проблемы. Данное законодательство было принято Федеральным собранием США в 1984 г. и называлось “Comprehensive crime control act of 1984”. В него, в частности, входил 1-й федеральный закон США по борьбе с компьютерной преступностью, который получил название “Закон об использовании электронных устройств, обеспечивающих несанкционированный доступ к ЭВМ, злоупотреблениях и мошенничестве с помощью компьютеров”. В этом законе были сформулированы три типа преступлений, совершенных с помощью компьютеров, а именно'

1) незаконный доступ к компьютерным системам в целях совершения незаконных операций;

2) умышленное нанесение ущерба с помощью незаконного проникновения в банк данных;

3) изменение программного обеспечения [32, с. 37]. С принятием указанного федерального законодательства правовая охрана компьютерных систем от различного рода посягательств строилась в основном на основе запрещения несанкционированного доступа и получения информации определенного рода. Например, в соответствии с частью 1030(a) этого закона, “всякий, Сознательно получивший доступ в компьютерную систему без разрешения или имеющий разрешение, но использующий такой случай с целью, для которой такое разрешение не предполагалось, и получивший информацию, содержащуюся в файлах, подлежит наказанию...” [71, с. 248—249]. Последнее, в соответствии с различиями законодательства в разных штатах, решается по-разному и сопряжено с рядом трудностей при определении судом меры наказания.

Прежде всего это выражено в том, что доказывание совершения, например, “воровства” требует в процессе расследования определения стоимости похищенного, что само по себе представляется затруднительным. Сложность решения этой задачи вызвана неоднородностью объекта преступного посягательства в компьютерных преступлениях. Дело в том, что в разных штатах США, как и в ряде других зарубежных стран, например, в Канаде, Великобритании, ФРГ, Японии, Швеции, Финляндии, Австралии, Норвегии, Дании и Португалии в совокупности выделяются три объекта уголовно-правовой охраны в случае компьютерных посягательств: услуги, имущество и информация [80, с. 18].

Определение стоимости похищенных (непредоставленных) услуг и имущества не представляет для следствия трудности и определяется с помощью обычных методик расследования хищений.

Сложнее обстоит дело с определением стоимости информации, напрямую связанное с доказыванием “воровства” информации, которое в свою очередь требует доказывания факта лишения собственника его имущества. Сложность здесь заключается в том, что специфика информации как превращенной формы человеческих знаний создает возможность ее копирования у собственника без самого факта физического изъятия [71, с. 249]. Вместе с этим, с криминалистической точки зрения, уникальность данного явления заключается в том, что лицо, не имеющее санкционированного доступа к средствам компьютерной техники (СКТ), может получить любую информацию и данные, хранящиеся в памяти компьютерной системы, без применения каких-либо насильственных и откровенно уголовных действий: информация может быть изменена, похищена либо уничтожена с помощью СКТ. Проблема здесь, по нашему мнению, заключается в

том, можно ли рассматривать действия лица по незаконному вторжению в компьютерную систему в качестве посягательства на чужую собственность.

В данном случае, по мнению некоторых исследователей, информация, как объект посягательства, представляет собой товар особого информационного рода и обладает, как и всякий обычный товар, потребительской и меновой стоимостью. При этом меновая стоимость включает в себя инвестиции, вложенные в его создание, собирание и монтаж, а также стоимость восстановления поврежденной информации и потенциальные потери от ее незаконного присвоения. Однако эти расходы на собирание информации и обеспечения ею собственника (пользователя) не исчерпывают ее стоимости. «Ведь информационный продукт предоставляет пользователю определенную информацию, из которой он может воссоздать нужное ему знание. Именно такой продукт пользователь готов оплачивать, соразмеряя плату с той выгодой, которую ему приносит получаемое знание» [71, с. 249].

По нашему мнению, данная концепция информации как превращенной формы знания объясняет зависимость величины стоимости информации не только от затрат на ее производство и обслуживание, но и от таких ее параметров, как актуальность и адресность. Под актуальностью в данном случае понимается новизна и своевременность, соответствие знаний, содержащихся в информации, решаемым задачам, а под адресностью — ориентация информации на конкретного ее получателя (пользователя). Здесь же отметим, что оба этих параметра зависят от каждой конкретной ситуации и не являются постоянными. Вот почему установление действительного ущерба в случаях хищения информации затруднительно. Тем не менее мы не сомневаемся в том, что в скором времени будет все же разработана специальная методика определения общей стоимости информации, отсутствие которой в настоящее время значительно снижает эффективность применения правовых мер предупреждения компьютерных преступлений.

Все вышесказанное в полной мере относится и к нашему отечественному законодательству, которое движется в этом направлении, на наш взгляд, очень робкими шагами. Первым из них по праву можно считать издание 22 октября 1992 г. двух Указов Президента Российской Федерации «О правовой охране программ для электронновычислительных машин и баз данных» и «О правовой охране топологий интегральных микросхем», регламентирующих порядок установления и правовую защиту авторских прав на программные средства компьютерной техники и топологии интегральных микросхем с 1 января 1994 г. (аналогичные законодательные акты были приняты в зарубежных странах намного ранее, например в США — в 1984 г., в Нидерландах — 7 ноября 1987 г., и получили название «Закон о защите электронных компонентов: электронных схем, печатных плат и интегральных схем ЭВМ». — см.: 33, с. 9).

Вторым прогрессивным шагом в этом направлении является принятие Государственной Думой и Федеральным Собранием Российской Федерации сразу двух Законов: 20 января — «О связи» и 25 января 1995 г. «Об информации, информатизации и защите информации», вступивших в силу с момента их опубликования. Вышеприведенные нормативные акты уже позволяют регулировать правовые отношения в сфере информационного обмена и обработки информации, в т. ч. с использованием средств новых информационных технологий, например:

— дают юридическое определение основных компонентов информационной технологии как объектов правовой охраны;

— устанавливают и закрепляют права и обязанности собственника на эти объекты;

— определяют правовой режим функционирования средств информационных технологий;

— определяют категории доступа определенных субъектов к конкретным видам информации;

— устанавливают категории секретности данных и информации;

— дают определение и границы правового применения термина «конфиденциальная информация», а также возлагают обязанности на конкретных субъектов по ее защите от различных факторов [30; 31]. (Аналогичные законы действуют в развитых зарубежных странах уже более двадцати лет, например в Швеции — с 1973 г., в США — с 1974 г., в ФРГ — с 1976 г. — см.: 34, с. 17).

Решающим законодательным аккордом по рассматриваемому кругу проблем можно считать принятие в июне 1996 г. Уголовного кодекса Российской Федерации, устанавливающего уже уголовную ответственность за компьютерные преступления в Российской Федерации и выделяющего информацию в качестве объекта уголовно-правовой охраны [92, гл. 28].

Вступление в силу с 1 января 1997 г. данного закона в Российской Федерации будет иметь, на наш взгляд, очень важное значение и приведет к коренной перестройке и ломке многих, годами устоявшихся понятий и определений уголовно-правовой базы в нашей стране. Этим актом отечественное уголовное законодательство приводится в соответствие с общепринятыми международными правовыми нормами развитых в этом отношении зарубежных стран. В свою очередь это неизменно повлечет за собой принятие нового уголовно-процессуального законодательства, регламентирующего все возможные следственные действия и механизм их осуществления применительно к специфике нового вида преступлений. И, безусловно, потребует соответствующих криминалистических разработок в области криминалистической техники, методики, тактики, судебной экспертизы, направленных на научную разработку проблем борьбы с компьютерными преступлениями.

Между тем общеизвестно, что одними правовыми мерами сдерживания не всегда удастся достичь желаемого результата в деле предупреждения преступлений. Тогда следующим этапом становится применение мер организационно-технического характера для защиты средств компьютерной техники от противоправных посягательств на них (под защитой понимаются ограничения доступа или использования всей или части компьютерной системы — см.: 68, с. 109). Эти меры могут играть серьезную общепрофилактическую роль в борьбе с компьютерными преступлениями при их умелом и комплексном использовании.

По мнению отечественных исследователей, давно уже “пора встать на точку зрения о том, что в охране нуждаются не только материальные ценности, но и информационные ресурсы, а контроль за их сохранностью — такая же профилактическая мера в отношении компьютерных преступлений, как и профилактика в любой другой сфере” [99, с. 39]. “Защите подлежит . любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу” — гласит ст. 21 Федерального Закона “Об информации...” [31, ст. 21].

Как уже отмечалось нами выше, многие зарубежные страны имеют достаточно большой опыт в этом направлении, тогда как в России ими стали заниматься всерьез лишь с начала 90-х гг. Поэтому, как нам представляется, в сложившейся ситуации нет необходимости “изобретать велосипед”, а нужно умело адаптировать имеющийся положительный зарубежный опыт применительно к отечественной практике. Применение последнего позволит в кратчайшие сроки и с минимальными экономическими затратами создать собственную эффективную систему обеспечения безопасности компьютерных систем в общегосударственном масштабе, не уступающую по своим характеристикам зарубежным аналогам. В конечном итоге, по нашему мнению, это должно привести к существенному снижению ущерба, причиняемого компьютерными преступлениями.

Рассмотрим отдельные положительные, на наш взгляд, организационно-технические меры предупреждения компьютерных преступлений, применяемые в развитых зарубежных странах.

В настоящее время руководство профилактикой компьютерных преступлений в этих странах осуществляется по следующим направлениям:

- 1) соответствие управленческих процедур требованиям компьютерной безопасности;
- 2) разработка вопросов технической защиты компьютерных залов и компьютерного оборудования;
- 3) разработка стандартов обработки данных и стандартов компьютерной безопасности;
- 4) осуществление кадровой политики с целью обеспечения компьютерной безопасности [71, с. 254].

Например, национальным бюро стандартов США были разработаны базовые требования безопасности, предъявляемые к компьютерным сетям. В их числе:

- пригодность — гарантия того, что сеть пригодна для обеспечения санкционированного доступа;
- контролируемая доступность — гарантия, что сеть обеспечит доступ только санкционированному пользователю для решения санкционированных задач;
- неприкосновенность — защита данных от несанкционированного их изменения и уничтожения;
- конфиденциальность — защита данных от несанкционированного раскрытия;
- безопасность передачи данных — гарантия того, что идентификация пользователей, качество передаваемых данных, время и продолжительность передачи данных обеспечены.

На основе данных требований были созданы соответствующие механизмы технического контроля, отвечающие следующим критериям:

- 1) целостность — базовая надежность, гарантирующая, что механизм работает как должно;
- 2) возможность проверки — способность записывать информацию, которая может иметь значение в раскрытии и расследовании попыток посягательства на средства компьютерной техники и других событий, относящихся к вопросам безопасности системы.

В результате практической реализации этих мер стало возможно;

- контролировать физический доступ к средствам компьютерной техники (СКТ);
- контролировать электромагнитное излучение аппаратных СКТ;
- наблюдать за возможной угрозой СКТ и фиксировать каждую такую попытку (методом мониторинга) [71, с. 254].

Как видно из вышеприведенного, цели и основные положения защиты информации в зарубежных странах по ряду базовых позиций совпадают с российскими и предполагают:

- а) предотвращение утечки, хищения, утраты, искажения и подделки информации;
- б) предотвращение угроз безопасности личности, общества и государства;
- в) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и системы;
- г) обеспечение правового режима функционирования документированной информации как объекта собственности;
- д) сохранение государственной тайны и конфиденциальности документированной информации;
- е) обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения [31, ст. 20].

По методам применения тех или иных организационно-технических мер предупреждения компьютерных преступлений специалистами отдельно выделяются три их основные группы:

- 1) организационные;
- 2) технические;

3) комплексные (сочетающие в себе отдельные методы двух первых групп).

Организационные меры защиты СКТ включают в себя совокупность организационных мероприятий по подбору, проверке и инструктажу персонала, участвующего на всех стадиях информационного процесса; разработке плана восстановления информационных объектов после выхода их из строя; организации программно-технического обслуживания СКТ; возложению дисциплинарной ответственности на лиц по обеспечению безопасности конкретных СКТ; осуществлению режима секретности при функционировании компьютерных систем; обеспечению режима физической охраны объектов; материально-техническому обеспечению и т. д. и т. п. Организационные мероприятия, по мнению многих специалистов, занимающихся вопросами безопасности компьютерных систем, являются важным и одним из эффективных средств защиты информации, одновременно являясь фундаментом, на котором строится в дальнейшем вся система защиты [99, с. 40].

Анализ материалов отечественных уголовных дел позволяет сделать вывод о том, что основными причинами и условиями, способствующими совершению компьютерных преступлений в большинстве случаев стали:

1) неконтролируемый доступ сотрудников к пульту управления (клавиатуре) компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе осуществления финансовых операций;

2) бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать указанную в п. 1 ЭВМ в качестве орудия совершения преступления;

3) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

4) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

5) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации и ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа;

6) отсутствие категоричности допуска сотрудников к документации строгой финансовой отчетности, в т. ч. находящейся в форме машинной информации;

7) отсутствие договоров (контрактов) с сотрудниками на Предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

Применяемые в большинстве организаций системы позволяют обычно использование таких мер безопасности, как пароли, недоступность программных и информационных файлов, а также другие меры, которые почти не практикуются, либо используются в ограниченном масштабе. Причины этого различные. Одна из основных — финансовая, поскольку, внедрение защитной системы является делом дорогостоящим. Кроме того, в целях экономии на одном и том же компьютере нередко совершаются многопрофильные операции, что в свою очередь повышает риск несанкционированного доступа. Контроль и проверки правильности использования компьютеров также требуют дополнительных финансовых затрат, и если в течение нескольких лет не происходит никаких инцидентов, то контроль либо ослабевает, либо не осуществляется вообще. В то же время для эффективной безопасности от компьютерных преступлений всего лишь необходимо:

1) просмотреть всю документацию в учреждении, организации;

2) ознакомиться с функциями и степенью ответственности каждого сотрудника;

3) определить возможные каналы утечки информации;

4) ликвидировать обнаруженные слабые звенья в защите.

Для любой организации практически существуют два варианта доступа к средствам компьютерной техники, которые и будут в дальнейшем определять весь комплекс защитных мероприятий.

В первом варианте организация приобретает собственную ЭВМ, которую и использует для решения своих задач, являясь ее единственным пользователем. В этом случае все вопросы компьютерной безопасности более или менее контролируемы.

Во втором случае организация становится (наряду с другими) пользователем какой-либо разветвленной коллективной компьютерной сети. Это может быть сделано с помощью разделения пользователей по времени (один компьютер на несколько организаций), сетевой системы в рамках организации или путем создания совместной сети пользования с другими общественными, государственными или коммерческими организациями, в результате чего происходит объединение их информационных ресурсов, а следовательно, многократно возрастает и риск стать потерпевшей стороной от компьютерного преступления из-за практически неконтролируемого в настоящее время доступа к информации и СКТ.

Зарубежный опыт показывает, что наиболее эффективной мерой в этом направлении является введение в штатное расписание организаций должности специалиста по компьютерной безопасности (администратора по защите информации) либо создание специальных служб как частных, так и централизованных, исходя из конкретной ситуации. Наличие такого отдела (службы) в организации, по оценкам зарубежных специалистов, снижает вероятность совершения компьютерных преступлений вдвое [74, с. 7]. По нашему мнению, в соответствии с этим опытом, целесообразно выделение ставок подобных должностей и в российских учреждениях и организациях. В обязательном порядке это мероприятие должно осуществляться на крупных вычислительных центрах, электронных "почтовых ящиках", особенно коллективного пользования, а также в кредитно-финансовых учреждениях и организациях (коммерческих банках, концернах, компаниях и др.). В последних, по нашему мнению, должны создаваться специальные отделы компьютерной безопасности в рамках действующих служб экономической безопасности и физической защиты, деятельностью которых должен руководить один из специально назначенных для этих целей заместителей начальника службы безопасности, имеющий в своем распоряжении соответствующие людские, финансовые и технические ресурсы для решения поставленных задач.

В функциональные обязанности указанных лиц прежде всего должны входить следующие позиции осуществления организационных мер обеспечения безопасности СКТ: |

1) обеспечение поддержки со стороны руководства конкретной организации требований защиты СКТ;

2) разработка комплексного плана защиты информации;

3) определение приоритетных направлений защиты информации в соответствии со спецификой деятельности организации;

4) составление общей сметы расходов финансирования охранных мероприятий в соответствии с разработанным планом

(п. 2) и утверждение ее в качестве приложения к плану руководством организации;

5) определение ответственности сотрудников организации за безопасность информации в пределах установленной им компетенции путем заключения соответствующих договоров между сотрудником и администрацией;

6) разработка, внедрение и контроль за исполнением различного рода инструкций, правил и приказов, регламентирующих формы допуска, уровни секретности информации, конкретных лиц, допущенных к работе с секретными (конфиденциальными) данными и т. п.;

7) разработка эффективных мер борьбы с нарушителями защиты СКТ [99, с. 41].

При этом, как показывает практика, наиболее надежным средством повышения эффективности мер безопасности СКТ является обучение и ознакомление работающего персонала с применяемыми в конкретной организации организационно-техническими мерами защиты.

Кроме этого, в обязательном порядке должны быть реализованы следующие организационные мероприятия:

1) для всех лиц, имеющих право доступа к СКТ, должны быть определены категории допуска, т. е. необходимо определить область служебных интересов каждого лица, виды информации, к которым он имеет право доступа, а также вид разрешения этого доступа, определяемый полномочиями лица на совершение тех или иных манипуляций со средствами компьютерной техники, исходя из его прямых функциональных обязанностей;

2) определена административная ответственность для лиц за сохранность и санкционированность доступа к имеющимся информационным ресурсам. При этом за каждый их вид ответственность должно нести одно конкретное лицо;

3) налажен периодический системный контроль за качеством защиты информации посредством проведения регламентных работ как самим лицом, ответственным за безопасность, так и с привлечением компетентных специалистов (экспертов) из других организаций;

4) проведена классификация информации в соответствии с ее важностью, дифференциация на основе этого мер защиты;

определен порядок ее охраны и уничтожения;

5) организована физическая защита СКТ (физическая охрана) [99, с. 42].

По нашему мнению, помимо организационно-управленческих мер, существенную общепрофилактическую роль в борьбе с компьютерными преступлениями могут играть также меры технического характера. К ним относятся технические методы защиты средств компьютерной техники, например: защита от НСД, от стихийных бедствий и аварий (пожары, наводнения, отключения энергопитания и т. п.), от хищений СКТ, саботажа, диверсий (взрывов); резервирование особо важных СКТ; правильная организация коммуникационных сетей и ресурсов; установка охранно-пожарной сигнализации и других рубежей обороны и т. д. Условно их можно подразделить, по нашему мнению, на три основные группы в зависимости от характера и специфики охраняемого объекта, а именно: аппаратные, программные и комплексные.

Аппаратные методы предназначены для защиты аппаратных средств и средств связи компьютерной техники от нежелательных физических воздействий на них сторонних сил, а также для закрытия возможных нежелательных каналов утечки конфиденциальной информации и данных, образующихся как за счет побочных электромагнитных излучений и наводок, виброакустических сигналов, так и других, подробно рассмотренных нами во второй и третьей главах. Практическая реализация данных методов обычно осуществляется с помощью применения различных технических устройств специального назначения. К ним, в частности, относятся:

1) источники бесперебойного питания аппаратуры, а также различные устройства стабилизации, предохраняющие от резких скачкообразных перепадов напряжения и пиковых нагрузок в сети электропитания (например, устройство PILOT);

2) устройства экранирования аппаратуры, линий проводной связи и помещений, в которых находится компьютерная техника:

а) пассивные типа “Корунд-М”, “Гранит-8”, “Букет”, подавляющие акустический сигнал на 60-80 дБ, а также “Сигнал-3”, сочетающий в себе элементы пассивной защиты и индикацию на подключение к защищаемой линии устройства съема информации, либо — различного рода экраны, сетки и специальные пленки;

б) активные — генераторы шума типа ГШ-01, ГНОМ-3, ГНОМ-4, создающие вибрационные и акустические помехи в элементах строительных конструкций и инженерно-технических

коммуникациях; скремблеры типа СТА-1000, ACS-2 (зарубежного производства и SCR-M1.2 (отечественного) с эхоподавлением и кодированием телефонной и факсимильной информации при работе абонентов в дуплексном режиме, имеющие открытый ключ и обладающие высокой криптостойкостью; различного рода фильтры, предотвращающие съём информации со слабо- и высокоточных коммуникаций (например: фильтр сетевой ФС-Б2, отсекающий — ФОЛ и т. п.);

3) устройства комплексной защиты телефонии;

4) устройства, обеспечивающие только санкционированный физический доступ пользователя на охраняемые объекты СКТ (шифрозамки, устройства идентификации личности и т. д. и т. п.);

5) устройства идентификации и фиксации терминалов и пользователей при попытках несанкционированного доступа к компьютерной сети;

6) средства охранно-пожарной сигнализации;

7) средства защиты портов компьютерной техники и т. д. Заметим, что последние наиболее эффективны для защиты компьютерных сетей от несанкционированного в них доступа. Эти средства в настоящее время наиболее распространены в зарубежных странах и пользуются достаточной популярностью. Они называются Port protection devices и представляют собой компьютеры, “сторожащие” входы в главный компьютер. Данное устройство состоит из микропроцессора, идентифицирующего пользователя и принимающего решение о его допуске к компьютерной системе, а также устройства памяти, содержащего зарегистрированные коды пользователей, имеющих право на доступ [87, с. 76-78].

Средства защиты портов выполняют несколько защитных функций, а именно:

1) “Сверка кода”. Компьютер защиты порта сверяет код санкционированных пользователей с кодом в запросе. Если пользователь не идентифицирован, компьютер автоматически разрывает связь с вызывающим абонентом, что предохраняет компьютерную систему от такого способа совершения компьютерного преступления, как “за хвост”, используемого преступниками лично или с помощью специально созданной программы, автоматически подбирающей код доступа к компьютерной системе.

2) “Камуфляж”. Некоторые средства защиты портов камуфлируют существование портов на линии телефонной связи путем синтеза человеческого голоса, отвечающего на вызов абонента. Поскольку большинство персональных компьютеров имеет встроенные модемы, то таким образом защищенные порты для них недоступны.

3) “Звонок навстречу”. Данная защитная функция направлена против способа совершения компьютерного преступления методом “маскарад”. Напомним, что этот способ заключается в том, что преступник каким-либо образом узнает код законного зарегистрированного пользователя и осуществляет с его помощью несанкционированный доступ к СКТ с помощью любого телефонного абонента, выдавая себя за законного пользователя. В ответ на это — средство защиты портов, в памяти которого хранятся не только коды доступа, но и идентификационные номера телефонов, разрывает связь и автоматически осуществляет установление связи с пользователем по второму реквизиту.

4) Ведение автоматического “электронного журнала” доступа в компьютерную систему с фиксацией основных действий пользователя (стирание, изменение, запись информации). Некоторые средства защиты портов обладают способностью собирать и распечатывать информацию о пользовании системой, в том числе и о неправомерных попытках доступа [71, с. 256].

Функции защиты “звонок навстречу” и “электронный журнал” иногда сочетаются для фиксации номеров телефонных абонентов, предпринявших попытки несанкционированного доступа в систему, с одновременным включением звуковой и световой сигнализации оповещения персонала служб компьютерной безопасности о попытке проникновения на охраняемый объект.

Программные методы защиты предназначаются для непосредственной защиты информации по трем направлениям (уровням): а) аппаратуры; б) программного обеспечения; в) данных, а также

для обеспечения должного контроля за правильностью осуществления процессов ее ввода, вывода, обработки, записи, стирания, чтения и передачи по каналам связи.

Так, например, защита информации на уровне данных и управляющих команд направлена на:

- 1) защиту информации при ее передаче по каналам связи между пользователем и ЭВМ или между различными ЭВМ;
- 2) обеспечение доступа только к разрешенным данным, хранящимся в ЭВМ, и выполнение только допустимых операций над ними.

Для защиты информации при ее передаче обычно используют различные методы шифрования данных перед их вводом в канал связи или на физический носитель с последующей расшифровкой. Как показывает практика, методы шифрования позволяют достаточно надежно скрыть смысл сообщения. Например в США, в соответствии с директивой Министерства финансов, начиная с 1984 г. все общественные и частные организации были обязаны внедрить процедуру шифрования коммерческой информации по системе DES (Data Encryption Standard), официально утвержденной Национальным бюро стандартов США еще в 1978 г. [89, с. 33, 42]. А с 1987 г. начал действовать принятый Международный стандарт ISO 8372, разработанный на базе алгоритма криптографического преобразования DES [99, с. 46]. В настоящее время к нему добавился еще один официально зарегистрированный стандарт шифрования данных RSA, разработанный компанией Data Security Inc. (Калифорния, США) на основе криптоалгоритма Clipper и названный так по начальным буквам фамилий его изобретателей: Rivest, Shamir and Adleman. По мнению специалистов, RSA является одним из наиболее развитых методов криптографической защиты информации с открытым ключом, на основе которого организуются эффективнейшие и перспективные системы защиты данных [89, с. 39-41]. Заметим, что в таких системах для зашифрования данных используется один ключ, а для расшифрования — другой (ключевая пара, формируемая получателем, а не отправителем, как это делается в системе электронно-цифровой подписи (ЭЦП), которая будет рассмотрена нами далее по тексту). Первый ключ не является секретным и может быть опубликован для использования всеми пользователями системы, шифрующей данные, либо взят из уже подписанного документа. Расшифрование же последних с помощью известного ключа невозможно, т. к. для этих целей их получатель использует второй ключ, который является секретным. Естественно, ключ расшифрования при этом не может быть определен из ключа зашифрования. Криптостойкость алгоритма RSA основывается на предположении, что исключительно трудно определить секретный ключ по известному, поскольку для этого необходимо решить задачу о существовании делителей целого числа. Не вдаваясь в тонкости математической науки, отметим, что данная задача не допускает в настоящее время эффективного решения. Более того, сам вопрос существования эффективных алгоритмов решения NP-полных (полиномиальных) задач является открытым [89, с. 29].

В России в июле 1991 г. также был введен в действие ГОСТ 28147-89 криптографирования информации, представляющий собой единый алгоритм криптографического преобразования данных для систем обработки информации в сетях ЭВМ, отдельных вычислительных комплексах и ЭВМ, функционирующий на базе отечественного алгоритма Krypton, аналогичного по своим основным техническим параметрам DES [19; 89, с. 34-38]. Отметим, что российский стандарт свободен от недостатков стандарта DES и в то же время обладает всеми его преимуществами. Кроме того, в стандарт заложен метод, с помощью которого можно зафиксировать необнаруженную случайную или умышленную модификацию зашифрованной информации, повышающую эффективность его использования. Функционирующая на базе указанного стандарта система защиты KRYPTON, является, по мнению российских специалистов, наиболее надежной по сравнению с зарубежными аналогами типа LATCH, RANK, ASSA и другими [19; 89, с. 25]. KRYPTON обеспечивает надежную защиту данных с гарантированной стойкостью и представляет собой программно-аппаратный комплекс, предназначенный для криптографической защиты данных, размещенных на жестком магнитном диске компьютера. Аппаратура системы была разработана МП «АНКАД», а программное обеспечение — СП «ДИАЛОГ» [19; 89, с. 26]. Из числа отечественных производителей подобной продукции нами выделяется фирма «АНКЕЙ», занимающаяся вопросами обеспечения безопасности компьютерной сети Главного расчетно-кассового центра Центрального банка Российской Федерации в г. Москве. Для этих целей фирмой используется отечественная плата криптографического преобразования «Криптон-3». Обслуживание компьютерной сети осуществляется в рамках проекта «Автоматизированная система расчетов в Московском регионе», утвержденного Минфином России и правительством Москвы. В разработанной фирмой «АНКЕЙ» системе компьютерной безопасности и защиты банковской информации, действующей с июня 1993

г., помимо программного метода криптографирования информации, применены методы аппаратной защиты путем 4-кратного дублирования каналов связи. При прохождении каждого платежного документа, соответствующего европейскому стандарту EDIFACT по количеству полей, их описанию и т. д. (базовый протокол для электронного документооборота, представляющий собой совокупность семантических и синтаксических правил, определяющих работу функциональных устройств коммуникационной компьютерной сети в процессе связи — см.: 68, с. 309), в банке осуществляется около 10 дополнительных проверок, а после проведения каждой транзакции производится смена ключей шифрования документов.

Помимо использования криптоалгоритмов, существует еще целый набор программных средств, позволяющих шифровать информацию и учитывающих различные условия анализа шифротекста при попытке его вскрытия. К ним, в частности, можно отнести и общеизвестную программу Diskreet из программного пакета Norton Utilities, позволяющую, кроме шифрования магнитных носителей информации, выполнять функцию блокировки клавиатуры и экрана ЭВМ (гашение видеоотображения ценной информации), а также предусматривающую защиту информационных объектов на уровне файлов или виртуальных (логических) дисков винчестера. Для возобновления нормальной работы в ЭВМ требуется ввести пароль.

Все программы защиты, осуществляющие управление доступом к машинной информации, функционируют по принципу ответа на вопросы: кто может выполнять, какие операции и над какими данными. В данном случае в качестве объекта охраны, доступ к которому контролируется, может выступать файл, запись в файле или отдельное поле записи файла, а в качестве факторов, влияющих на принятие программой защиты решения о доступе, — внешнее событие, значение данных, состояние компьютерной системы, полномочия пользователя, предыстория обращения, семантические отношения между данными [68, с. 109-110, 357]. В связи с чем доступ может быть определен как:

- общий (безусловно предоставляемый каждому пользователю);
- отказ (безусловный отказ, например разрешение на удаление порции информации);
- зависимый от события (управляемый событием), предусматривает блокировку обращения пользователя, например в определенные интервалы времени или при обращении к компьютерной системе с определенного терминала;
- зависимый от содержания данных (в этом случае решение о доступе основывается на текущем значении данных, например некоторому пользователю запрещено читать те или иные данные);
- зависимый от состояния (динамического состояния компьютерной системы), осуществляется в зависимости от текущего состояния компьютерной системы, управляющих программ и системы защиты, например может быть запрещен доступ к файлу, если носитель машинной информации не находится в состоянии “только чтение” либо пока не будет открыт логический диск, содержащий этот файл;
- частотно-зависимый (например, доступ разрешен пользователю только один или определенное число раз — таким образом предотвращается возможность динамического управления событиями);
- по имени или другим признакам пользователя (например, пользователю должно быть более 18 лет);
- зависимый от полномочий (предусматривает обращение пользователя к программам, данным, оборудованию в зависимости от предоставленного режима, например может быть разрешено “Только чтение”, “чтение и запись”, “только выполнение”);
- зависимый от предыстории обращения и учитывающий семантические отношения между данными вместе с управлением доступом, зависящим от полномочий (составляет защиту контекстно зависимой информации, которая препятствует раскрытию защищаемого информационного ресурса посредством логического вывода (при обработке статистических запросов, при выдаче последовательности запросов к логически связанным элементам данных и т.

д.). В этом случае доступ программой проводится анализ контекста, включающего предыдущие запросы, их обработку, среду текущего запроса и семантические отношения между данными [42, с. 234];

— по разрешению (по паролю или другому идентификатору: карточка, значок и т. д.), где под идентификацией понимается; процедура установления подлинности пользователя, осуществляющего доступ к компьютерной системе [см.: 34, с. 19-21];

— по процедуре (в этом случае система имеет свою собственную процедуру: автоматически генерирует собственные правила обеспечения безопасности данных) [34, с. 22-23].

Другой подход к построению средств защиты доступа основан на контроле информационных потоков и разделении субъектов и объектов доступа на классы секретности (категории и уровни допуска, учитывающие полномочия пользователей и семантику информации). Указанные средства контроля разрешают поток информации для чтения, если уровень информационного объекта-источника соответствует или не превосходит категорию субъекта-получателя информации, и для записи, если категория субъекта-источника соответствует или превышает уровень секретности информационного объекта. Оптимальным вариантом здесь, по нашему мнению, является введение для каждого пользователя индивидуальных ключевых дискет, предложенных В.Н. Черкасовым [99, с. 45]. При этом имеется в виду, что все защищаемые программы должны быть перекодированы, а информация, требуемая для перевода их в человекочитаемую форму, содержится только на ключевом носителе информации, причем одновременно являющегося и идентификатором личности пользователя, имеющего право доступа только к тем программным средствам, к которым “подходит” ключ и работа с которыми ему разрешена.

Средства регистрации, как и средства контроля доступа к информационным ресурсам, также относятся к эффективным мерам противодействия попыткам несанкционированного доступа. Однако, если средства контроля доступа предназначены непосредственно для этого, то задача средств регистрации заключается в обнаружении и фиксации уже совершенных действий преступника или попытках их совершения. Для этих целей наиболее перспективными, на наш взгляд, являются новые операционные системы специального назначения, широко применяемые в зарубежных странах и получившие название мониторинга (автоматического наблюдения за возможной компьютерной угрозой). Мониторинг осуществляется самой операционной системой (ОС), причем в ее обязанности входит контроль за процессами ввода-вывода, обработки и уничтожения машинной информации. ОС фиксирует время несанкционированного доступа и программных средств, к которым был осуществлен доступ. Кроме этого, она производит немедленное оповещение службы компьютерной безопасности о посягательстве на безопасность компьютерной системы с одновременной выдачей на печать необходимых данных (листинга) [71, с. 255].

В последнее время в США и ряде европейских стран для защиты компьютерных систем действуют также специальные подпрограммы, вызывающие самоуничтожение основной программы при попытке несанкционированного просмотра содержимого файла с секретной информацией по аналогии действия “логической бомбы”. По мнению зарубежных специалистов, подобные программные средства защиты выполняют весьма важные функции в деле предупреждения компьютерных преступлений. Нами отмечается тот факт, что к сожалению, подобными отечественными разработками в настоящее время никто конкретно не занимается, вследствие чего на практике широко используются зарубежные образцы. Подобные отечественные разработки находятся лишь на первоначальном теоретическом уровне их осмысления, далеко от повседневных нужд практических пользователей и собственников компьютерных систем (в основном также зарубежного производства).

По мнению отечественных исследователей, занимающихся вопросами безопасности компьютерных систем лишь в рамках исключительно одной своей отрасли, и в частности Черкасова В.Н., при безбумажной технологии должны быть созданы условия, исключающие как случайные (непреднамеренные) ошибки, так и умышленные искажения вводимой информации. По его мнению, этим целям должен служить ряд профилактических мероприятий, среди которых наиболее распространены следующие:

1) программы регистрации первичных данных, исключающие возможность пропуска обязательных реквизитов данных и содержащие условия блокировки ввода-вывода информации и подсказку пропущенных реквизитов;

2) подтверждение личности, регистрирующей первичные данные (авторизация данных), основанное на идентификации личности, производящей ввод-вывод данных, и предусматривающее возможность блокировки средств компьютерной техники при невыполнении предъявляемых условий идентификации;

3) программы защиты зарегистрированных первичных данных от преднамеренного или случайного их искажения, уничтожения, а также от несанкционированного получения сведений о зарегистрированных данных. Исправлять машинную запись первичных данных может только лицо, имеющее специальные полномочия, а основным подтверждением достоверности машинной записи при этом является однозначное доказательное определение личности, производившей регистрацию первичных данных [99, с. 43].

В настоящее время специалистами выделяется четыре основных способа идентификации личности пользователя, а именно:

1) по предмету, которым владеет человек;

2) по паролю, личному идентификационному коду, который вводится в ЭВМ с клавиатуры;

3) по физическим (антропометрическим) характеристикам личности, присущим индивидуально только ей;

4) по электронной цифровой подписи (ЭЦП), основанной на использовании криптографической системы с открытым ключом (99, с. 44).

Последние два способа считаются самыми перспективными и надежными в плане достоверности идентификации личности. К первому из них относятся все существующие биометрические системы санкционированного доступа, основанные на идентификации личности по таким характеристикам, как голос, размер ладони, отпечатки пальцев рук, сетчатка глаза, почерк, фотоснимок и т. п. Ко второму способу относится ЭЦП, широко используемая в зарубежных странах. Она позволяет:

— гарантировать авторство сообщения;

— реализовать юридическое заверение подписи и подлинности документа, переданного по каналам радиоэлектронных коммуникаций;

— повысить защищенность данных и информации, передаваемых по каналам связи.

При этом электронная подпись дает возможность не только гарантировать аутентичность документа в части его авторства путем электронно-цифровой фиксации основного текста и личностных характеристик подписи, но и установить неискаженность (целостность) содержащейся в нем информации, а также зафиксировать попытки подобного искажения. Электронная подпись, состав которой непосредственно зависит от заверяемого текста, соответствует только этому тексту, при условии, что его никто не изменял. Проверочная сумма (хэшфункция) измененного (фальсифицированного) электронного документа будет отличаться от проверочной функции, которая получается в результате обработанного преобразования электронной подписи. Переданный получателю подписанный документ состоит из текста, электронной подписи и сертификата пользователя, который содержит в себе гарантированно подлинное данные пользователя, в том числе его отличительное имя и открытый ключ расшифрования для проверки подписи получателем либо третьим лицом, осуществившим регистрацию сертификата [77, с. 33-34].

Следует отметить, что в настоящее время по инициативе Федерального агентства правительственной связи и информации (ФАПСИ) при Президенте России создана специальная межведомственная рабочая группа для выработки комплексной концепции российского стандарта

ЭЦП, в работе которой принимают участие все заинтересованные ведомства и организации: Высший арбитражный суд, Минфин, Минюст, Госстандарт и др. [99, с. 44].

При рассмотрении вопросов, касающихся программной защиты информационных ресурсов, нами особо выделяется проблема их защиты от компьютерных вирусов как способа совершения компьютерного преступления. Многими специалистами отмечается в этом направлении общая для всех классов и типов ЭВМ высокая опасность “заражения” компьютерным вирусом. Одновременно с этим нами специально обращается внимание на специфическую сторону этой проблемы для персональных компьютеров (ПК) как объектов, наиболее подверженных этим противоправным деяниям по ряду причин, напрямую зависящих от их тактико-технических характеристик, а именно:

- 1) массовость использования ПК (практически во всех сферах человеческой деятельности);
- 2) универсальность — использование одной и той же модели для решения различных задач;
- 3) хорошо развитый интерфейс (совокупность средств и правил, обеспечивающих взаимодействие устройств компьютерной системы и (или) программных средств с пользователем — см.: 62, с. 127) — возможность использования ПК любым лицом без специальных познаний и навыков в работе с ЭВМ;
- 4) достаточно высокий уровень развития периферии — возможность сопряжения (подключения) с ПК различных внешних электронных устройств, позволяющих, в частности производить свободное и быстрое сопряжение ПК с любыми каналами всех имеющихся средств связи без соответствующей их обоюдной подстройки и наладки (адаптации);
- 5) блочно-модульный принцип организации аппаратных ресурсов в архитектуре строения ЭВМ, позволяющий в течение буквально считанных минут устранять все возникающие сбои в работе и другие неполадки (поломки);
- 6) портативность и мобильность — возможность беспрепятственного перемещения ПК в активном рабочем режиме в пространстве и одновременное их использование в любых условиях;
- 7) стандартизация программных средств ПК. Исходя из последнего пункта и практических исследований специалистов, занимающихся вопросами антивирусной безопасности компьютерных систем, нетрудно заметить, что, например, вирусы для MS DOS и PC DOS активно используют именно этот принцип — стандартную систему прерываний, общепринятую маркировку исполняемых файлов и единую структуру организации хранения данных в ПК. Конструкторские изменения в архитектуре строения любого из этих компьютеров, как показывает практика, делают систему нестандартной и, следовательно, недоступной для алгоритмов вируса, который не может заданно функционировать в измененной программной среде.

Указанные выше уникальные, на наш взгляд, возможности персональных компьютеров в конечном итоге обусловили их повышенную подверженность различного рода компьютерным посягательствам, одним из которых является компьютерный вирус.

По оценкам многих специалистов, от решения проблем борьбы с этим видом компьютерного преступления зависит не только надежность и бесперебойность функционирования компьютерных информационных систем (в т. ч. и органов внутренних дел), но и вообще сам факт и возможность их существования [101; 99, с. 45]. Подобная опасность многократно возрастает в условиях все большего функционирования и распространенности компьютерных сетей, когда пути и возможности распространения вирусных “эпидемий” практически неконтролируемы.

Мы считаем, что в данном случае гораздо проще и экономически выгоднее защититься от “заболевания”, чем его “лечить”. Здесь, помимо организационно-правового “иммунитета”, необходимо активно использовать и специальные программные антивирусные средства защиты, разрабатываемые в настоящее время у нас в стране лишь на уровне отдельных, достаточно талантливых и предприимчивых специалистов, представляющих собой научный костяк новой отечественной отрасли информационной технологии, которая получила название Компьютерная вирусология [5; 6]. Такое самодеятельное начало в этом направлении нельзя считать нормальным,

т. к. общее положение дел в борьбе с компьютерной преступностью должно обязательно вестись на государственном уровне, а не на уровне отдельных коммерческих организаций и частных лиц. Последнее предполагает собой разработку государственной программы действий, направленных на защиту и охраноспособность информационных ресурсов в плане предупреждения компьютерных преступлений, включающей в себя такие обязательные разделы, как разработка и принятие соответствующих госстандартов, общих требований безопасности функционирования компьютерных информационных систем и сетей, средств связи и т. д. и т. п.

В настоящее время разрабатываемые отечественные и зарубежные программные антивирусные средства позволяют с определенным успехом опознать зараженные и незараженные программные средства и их компоненты, а также проконтролировать доступ к вычислительным ресурсам (данным, программам, оборудованию и т. д.). Для этих целей используются различные программные методы, позволяющие значительно расширить возможности обеспечения безопасности машинной информации и зависящие от специфики объекта охраны (типа и конфигурации системы и сети, их программного и аппаратного обеспечения (реализации), адресности защищаемого информационного ресурса, специфики формы его представления и т. д.).

Существующие антивирусные программные пакеты позволяют уже сейчас обнаруживать и уничтожать известные и неизвестные, постоянно появляющиеся модификации и оригиналы новых типов вирусов; “лечить” любые программные средства. По оценкам специалистов, эффективность использования данных программных средств позволяет обнаруживать до 90% новых вирусов с неизвестным рабочим алгоритмом строения. Особенную популярность среди пользователей ЭВМ завоевали отечественные антивирусные программные средства защиты, такие, как: детектор-полифаг ANTIAPЕ, разработанный ВВ. Богдановым; фаги AIDSTEST — ДН. Лозинского; VR, AN, -V — ЕВ. Касперского; SHERIFF — ЮД. Фомина, а также ADinf, разработанный акционерным обществом “Диалог-Наука” (авторский коллектив:

В.С. Ладыгин, Д.Г. Зуев, Д.Ю. Мостовой). Помимо вышеперечисленного, считаем необходимым акцентировать внимание на следующем отечественном программном продукте. Летом 1994 г.

АО “Диалог-Наука” было создано принципиально новое антивирусное средство, которое получило название Doctor Web — “лечебная паутинка”. Основное ее предназначение — борьба со сложными самокодирующимися вирусами, подробно рассмотренными нами в третьей главе работы. По мнению специалистов, именно Doctor Web, начиная с версии 1.07, позволяет не только обезвреживать полиморфы типа OneHalf, но и восстанавливать зашифрованные вирусом участки памяти компьютерной системы (винчестера), если само тело вируса еще не удалено с нее [41]. Среди зарубежных аналогичных средств нами отмечаются Anti-Virus 2.0 фирмы Central Point Software Inc., DiskLock 2.0 компании Fifth Generation Systems для автономных ПК и VIRSCAN — пакет программных антивирусных средств фирмы McAfee Associates, в состав которого входят специальные программы: CLEAN для восстановления “зараженных” программных средств, VCOPI для проверки “зараженности” копируемой машинной информации, SENTRY — средство автоматического контроля изменений программных кодов начала программ, FSP — средство проверки контрольных сумм файлов, LOOK.COMD — средство проверки командно-запускных файлов на соответствие с их резервной копией и т. д. [39; 42, с. 269-272].

По оценкам специалистов, существует уже достаточное количество различных антивирусных программных средств, позволяющих надежно защитить средства компьютерной техники от компьютерного вируса. Надежность этих средств составляет 97%. Особенной эффективностью отличаются следующие антивирусные программные средства защиты: резидентные программы-сторожа (“dog”), программы-полифаги, фаги, детекторы, ревизоры, программы-мониторы — “детекторы лжи” (Disk Monitor, VirBlk, Vaccine, ANTI14US, FSP, программы-мони-тор-D). Последние перехватывают запросы операционной системы ЭВМ на “опасные” с их точки зрения действия программ защиты и представляют собой программные средства автоматического контроля за программами защиты (“служба внутренней безопасности” программных средств защиты компьютерных систем) [39, с. 149]. Программы мониторинга сопоставляют результаты наблюдений за поведением системы с характеристиками, которые представляются критическими, например, когда:

— нарушение какого-либо стандартного условия сводит на нет целесообразность выполнения определенной функции;

— некоторый возможный эффект, вытекающий из алгоритма действий, нарушает какое-то ограничение, предусмотренное данным алгоритмом.

Для борьбы с компьютерными вирусами разработаны даже специальные методики, позволяющие пользователю своевременно обнаружить его появление в информационных ресурсах и даже успешно “вылечить” их, не обладая специальными навыками и познаниями в этой области [42, с. 261, 277-278].

Но тем не менее, всегда остаются те самые 3%, которыми и пользуются преступники для совершения компьютерных преступлений, ибо не существует абсолютно надежных средств защиты компьютерной техники от различного рода преступных посягательств. Заметим также, что в случае полного рассекречивания своей информационной системы из компаний средних размеров 20% просуществуют всего несколько часов, 48% — несколько дней, а оставшиеся 32% — от нескольких часов до нескольких дней, при этом 33% банков просуществуют несколько часов, 50% — несколько дней и 17% — от нескольких часов до нескольких дней [2, с. 198]. Поэтому наиболее эффективным, на наш взгляд, направлением в предупреждении подобных посягательств является комплексное использование различных мер предупреждения компьютерных преступлений: организационных, аппаратных и программных. Например, для уменьшения опасности вирусных посягательств на СКТ, по мнению специалистов, необходимо предпринять следующие комплексные организационно-технические меры, которые могут быть сокращены или расширены по своему содержанию, исходя из каждой конкретной ситуации.

1. Информировать всех сотрудников учреждения, организации, использующих СКТ, об опасности и возможном ущербе в случае совершения вирусного посягательства.

2. Не осуществлять неофициальные связи с другими организациями, связанные с обменом программных средств. Запретить сотрудникам приносить на рабочее место программные средства (ПС) “со стороны” для работы с ними на СКТ, находящихся в учреждении, организации по месту работы сотрудника. В крайнем случае для этих целей может быть создано специальное автономное рабочее место для тестирования таких ПС на предмет установления наличия или отсутствия в них средств вирусного характера. Должны использоваться только официально распространяемые ПС, содержащиеся на аттестированных и опломбированных носителях машинной информации.

3. Запретить сотрудникам использовать и хранить на носителях и в памяти ЭВМ компьютерные игры, являющиеся источником повышенной опасности для безопасности компьютерных систем. Если такое запрещение не может быть обеспечено; то создать специальное игровое место или общий игровой файл, постоянно контролируемый сотрудниками службы компьютерной безопасности и имеющий “иммунные” средства антивирусной защиты.

4. Предостеречь сотрудников организации от использования ПС и носителей машинной информации, имеющих происхождение из учебных заведений различного уровня и профиля. Тем более ставящих целью их использование в компьютерных системах организации, например, для выполнения работы частного-личного характера в свободное от основной работы время. В крайнем случае производить такую работу на изолированных ЭВМ или с соблюдением определенных мер антивирусной безопасности и с особым контролем.

5. Если в процессе работы возникнет необходимость в использовании сторонних информационных компьютерных сетей, то для этих целей необходимо в обязательном порядке выделить специальное стендовое оборудование с обязательной его изоляцией от остальных СКТ (рабочей станции от локальной сети или периферии). Все файлы, поступающие из внешней компьютерной сети, должны обязательно проверяться (тестироваться).

6. Создать архив копий ПС, используемых в непосредственной работе организации (обязательно должны храниться копии операционных систем, используемых системных ПС, необходимых для восстановления нормального режима работы компьютерных систем, например PCTOOLS, UNERASE и т. п.) с одновременным исключением несанкционированного доступа к этому архиву.

7. Регулярно просматривать хранимые в компьютерной системе ПС, создавать новые их архивные копии, архивные копии файлов с обновляемой информацией и, где это возможно, использовать

защиту типа “только чтение” для предупреждения несанкционированных манипуляций с ценными данными.

8. Периодически (а в организациях, имеющих ярко выраженную денежно-финансовую и кредитную функцию, — к концу каждого рабочего дня) проводить ревизионную проверку контрольных сумм файлов, путем их сличения с эталоном, иногда хранящимся в зашифрованном либо архивированном виде с защитой “только чтение”.

9. Использовать для нужд электронной почты отдельный стендовый компьютер или ввести специальный отчет. Запретить использование ПС, полученных по внешним каналам связи с помощью электронной почты и не прошедших специального тестирования.

10. Контролировать ведение журналов операторов ЭВМ (работы ЭВМ). В случае отсутствия соответствующей записи при наличии работающего сотрудника принимать дисциплинарные меры воздействия.

11. Установить системы защиты информации на особо важных ЭВМ. Заактивировать на них специальные комплексные антивирусные ПС в обязательном порядке.

12. Периодически пересматривать и обновлять ПС и всю систему антивирусной защиты и правила обеспечения компьютерной безопасности.

13. Постоянно контролировать исполнение установленных правил обеспечения безопасности СКТ и применять меры дисциплинарного воздействия к лицам, сознательно или неоднократно нарушавшим их [42, с. 273-276].

Подчеркнем, что хорошо защищенные СКТ менее всего подвержены риску стать предметом преступного посягательства, нежели те из них, которые вообще не имеют никаких средств защиты. Анализ же последних показывает, что они обеспечивают в настоящее время выполнение следующих функций:

1) идентификация защищаемых ресурсов, т. е. присвоение защищаемым ресурсам идентификаторов — уникальных признаков, по которым в дальнейшем осуществляется процесс их аутентификации;

2) аутентификация защищаемых ресурсов, т. е. установление их подлинности на основе сравнения с эталонными идентификаторами;

3) разграничение доступа пользователей к информационным ресурсам;

4) разграничение доступа пользователей по операциям над ресурсами, защищаемыми с помощью программных средств;

5) администрирование'

— определение прав доступа к защищаемым ресурсам;

— обработка и ведение регистрационных журналов;

— установка/снятие системы защиты с ЭВМ;

6) регистрация событий:

— входа пользователя в систему;

— выхода пользователя из системы;

— нарушения прав доступа к защищаемым ресурсам;

7) реакция на факты неустановления подлинности и нарушения прав доступа (инициализация ответных мер системы защиты);

8) контроль целостности и работоспособности систем защиты;

9) обеспечение безопасности информации при проведении регламентных и ремонтно-профилактических работ;

10) обеспечение безопасности информации в аварийных ситуациях [89, с. 15].

Общепризнано мнение о том, что профилактика любого, в том числе и компьютерного, преступления должна носить комплексный характер и относиться к компетенции государственных органов, а не различных коммерческих охранных структур, что имеет пока место в нашей стране. Этому учит нас и опыт зарубежных государств, где уже с 60-х гг. (с момента совершения первого компьютерного преступления) стали серьезно заниматься этими проблемами на государственном уровне. В частности, помимо основных правовых актов, о которых мы говорили ранее, были предприняты и другие законодательные мероприятия, направленные на обеспечение общей безопасности информационных ресурсов и возлагающие ответственность за их сохранность на несколько федеральных ведомств. Например, в США в 1965 г. был принят соответствующий Brooks Act [71, с. 254].

В настоящее время в зарубежных странах уже действует развитая система обеспечения компьютерной безопасности, осуществляемая государственными силами и средствами, включающая в себя законодательные, организационные и технические мероприятия, проводимые по единому комплексному плану и направленные на предупреждение компьютерных преступлений. Так, например, 14 мая 1991 г. вышла в свет директива Совета Европейского сообщества стран — участниц ЕЭС “О юридической защите компьютерных программ”, которая обязала законодательные органы стран — членов общего рынка в срок до 1 января 1993 г. ввести основные положения, указанные в ней, в свои национальные законодательства [58]. По поводу сущности этого нам приходится только сожалеть, применительно к отечественному положению дел, несмотря на всю актуальность и злободневность существующих проблем. Реальная ситуация по этому вопросу такова, что в настоящее время она находится лишь на первоначальном этапе, в состоянии разрозненных теоретических и практических разработок, осмысления специалистами различных наук и областей специальных познаний. Наиболее серьезным, по нашему мнению, в этом направлении является научное исследование, проведенное Черкасовым В.Н., в котором он впервые предложил и обосновал собственную модель системы мер борьбы с компьютерной преступностью (99, с. 30). На наш взгляд, ее можно использовать как базовую для построения общей целостной государственной системы мер борьбы, расширяя предложенные автором узкие рамки понятия этого социального явления с уровня борьбы с экономической преступностью до их истинных специфических размеров, вытекающих из определения понятия сущности компьютерного преступления, предложенного нами в данной работе. С позиций законодательства, стержневой основой в этом направлении, по нашему мнению, может стать Указ Президента Российской Федерации “О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации”, направленный на усиление борьбы с организованной преступностью и повышение защищенности информационно-телекоммуникационных систем органов государственной власти, российских кредитно-финансовых структур, предприятий и организаций [93]. Данным Указом, в частности, регламентируются следующие основные положения, имеющие непосредственное отношение к рассматриваемым нами проблемам, а именно:

— Программе создания и развития информационно-телекоммуникационной системы России придан статус президентской программы;

— запрещено использование государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата Федерального агентства правительственной связи и информации (ФАПСИ) при Президенте Российской Федерации;

— запрещено размещение государственных заказов на предприятиях, в организациях, использующих указанные выше технические и шифровальные средства, не имеющие сертификата ФАПСИ;

— Центральному банку России (ЦБР) совместно с ФАПСИ предложено принять необходимые меры в отношении российских коммерческих банков, уклоняющихся от обязательного использования имеющих сертификат ФАПСИ защищенных технических средств хранения, обработки и передачи информации при их информационном взаимодействии с подразделениями ЦБР;

— запретить деятельность физических и юридических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных и защищенных средств, а также предоставлением услуг в этой области без лицензии ФАПСИ;

— запретить ввоз на территорию России нелицензированных шифровальных средств и защищенной техники иностранного производства;

— правоохранительным органам России совместно с ФАПСИ осуществлять выявление юридических и физических лиц, нарушающих требования настоящего Указа;

— создать Федеральный центр защиты экономической информации при ФАПСИ, возложив на него разработку и реализацию комплексных программ обеспечения безопасности экономической информации российских кредитно-финансовых и других экономически значимых структур страны.

Первым официальным документом по выполнению данного Указа можно считать Постановление правительства Российской Федерации № 608 от 26 июня 1995 г. "О сертификации средств защиты информации" (Положение), которое обязывает соответствующие министерства и ведомства разработать и ввести в действие собственные Положения, определяющие системы сертификации, перечни средств защиты информации, подлежащие лицензированию в конкретной системе сертификации, порядок производства средств, порядок оплаты услуг по их разработке, установке и эксплуатации и т. д. и т. п. [72].

В заключение отметим, что, по-видимому, актуальность и значимость проблем, касающихся научных разработок в области компьютерной безопасности, будет возрастать в ближайшее время пропорционально процессу увеличения количества и качества совершаемых компьютерных преступлений. В конечном итоге это приведет к образованию новой подотрасли информационной индустрии — индустрии средств безопасности компьютерных систем и технологий.

Глава 5

Практика раскрытия и расследования компьютерных преступлений

Применение системы правовых и организационно-технических мер предупреждения компьютерных преступлений, несомненно, является одним из ведущих направлений в борьбе с компьютерными преступлениями. Однако хорошо известно, что одними мерами предупреждения (сдерживания) не всегда удается предотвратить преступное посягательство. Тем более, что, по единому мнению ведущих специалистов, занимающихся вопросами обеспечения безопасности компьютерных систем и электронного оборудования, в мире не существует абсолютно надежных электронных систем, гарантирующих своим пользователям полную конфиденциальность и сохранность машинной информации, циркулирующей в них [25, п. 21-22]. В связи с этим возникает необходимость заниматься не только вопросами защиты средств компьютерной техники (СКТ), но и решать вопросы расследования компьютерных преступлений. Указанная необходимость возникает в том случае, когда принятые меры предупреждения исчерпаны и не смогли в полной степени предотвратить наступление противоправного события.

На основании вышеизложенного нам представляется возможным выделить следующие основные криминалистические проблемы, возникающие в настоящее время перед правоохранительными органами при расследовании компьютерных преступлений и характеризующие одновременно специфику этого процесса, а именно:

- 1) сложность в установлении факта совершения компьютерного преступления и решении вопроса о возбуждении уголовного дела;
- 2) сложность в подготовке и проведении отдельных следственных действий;
- 3) особенности выбора и назначения необходимых судебных экспертиз;
- 4) целесообразность использования средств компьютерной техники в расследовании преступлений рассматриваемой категории;
- 5) отсутствие методики расследования компьютерных преступлений.

По оценкам отечественных и зарубежных исследователей, решение проблем раскрытия и расследования преступлений данного вида представляет собой задачу на несколько порядков более сложную, чем, скажем, задачи, сопряженные с их предупреждением. Видимо, поэтому уровень латентности компьютерных преступлений, в немалой степени зависящий и от этих обстоятельств, определяется в настоящее время в 90%. А из оставшихся 10% выявленных компьютерных преступлений раскрывается только 1%. Такое положение дел можно проиллюстрировать и конкретными статистическими данными. Например, в Великобритании из 270 установленных преступлений, совершенных с использованием средств компьютерной техники за последние 5 лет, были расследованы только 6; в ФРГ в 1987 г. было выявлено 2777 случаев аналогичных преступлений, из них расследовано только 170, тогда как остальные 2607 уголовных дел были прекращены по различным основаниям; во Франции в том же году было зарегистрировано 70 преступлений, а расследовано — 10 уголовных дел; в США в период с 1978 по 1986 г. правоохранительными органами было расследовано всего 200 преступлений, по которым к уголовной ответственности было привлечено лишь 6 чел. [32, с. 39; 81, с. 9]. При этом, по оценкам тех же специалистов, только 10% раскрытых компьютерных преступлений могут быть своевременно обнаружены с помощью систематических ревизионных проверок, тогда как 90% из них выявляются только благодаря случайностям [4, с. 38]. Приведенные данные красноречиво свидетельствуют об уровне сложности осуществления процессов расследования преступлений рассматриваемой категории.

Проведенный нами анализ отечественных уголовных дел, имевшихся в нашем распоряжении, в целом подтверждает вышеизложенное.

Относительная новизна возникших проблем, стремительное наращивание процессов компьютеризации российского общества, по нашему мнению, застали врасплох правоохранительные органы, оказавшиеся неготовыми к адекватному противостоянию и активной борьбе с этим новым социальным явлением. Считаем, что данная тенденция усугубляется еще и под воздействием ряда объективных и субъективных факторов, подробно рассмотренных нами в первой главе настоящей работы. Отчасти это подтверждается и данными проведенного нами исследования. Так, например, 76% опрошенных респондентов, составляющих исследуемую группу в лице начальников городских

И районных управлений (отделов) внутренних дел, считают что во вверенных им подразделениях нет в настоящее время сотрудников, способных заниматься вопросами раскрытия компьютерных преступлений. Аналогичной точки зрения придерживаются и респонденты из группы начальников следственных подразделений органов внутренних дел.

Оставляет желать лучшего и положение с отечественными научными разработками этих проблем, особенно в области криминалистической науки (отсутствие соответствующих методик). Остается нерешенным также и ряд основных организационных аспектов проблемы, связанных, например, с координацией усилий различных государственных органов, подготовкой соответствующих специалистов и т. д. Отечественное положение дел в этих направлениях, как показывает анализ литературных источников, резко контрастирует с зарубежным, где в последние годы им уделяется все более повышенное и пристальное внимание со стороны государственных органов. Так, в ФРГ, например, в учебных заведениях системы МВД в курс “Экономические преступления” введен специальный раздел, касающийся вопросов раскрытия и расследования преступлений, связанных с автоматической обработкой информации в компьютерных системах, а в Академии ФБР США в г. Квонтико (штат Вирджиния) с 1976 г. для слушателей читается специальный трехнедельный учебный курс по теме “Техника расследования преступлений, связанных с использованием

компьютеров". Помимо этого, в каждом низовом структурном подразделении ФБР имеется штатный специалист в этой области и с 1982 г. функционирует специальное подразделение численностью 500 чел. Аналогичная ситуация и в других зарубежных странах: в Канаде — функционирует группа специалистов уголовной полиции, занимающихся расследованием этой категории уголовных дел в масштабе всей страны, в Швеции — штатная численность специального подразделения составляет 150 сотрудников и т. д.

Нам представляется возможным привести и следующий факт по существу рассматриваемого вопроса. Как отмечалось на совещании по вопросам компьютерной преступности, проходившем в мае 1986 г. в Высшей полицейской академии ФРГ, в котором приняли участие 60 представителей органов уголовной полиции и прокуратуры западноевропейских государств, необходимо проводить систематическую специальную подготовку сотрудников уголовной полиции и органов юстиции в целях повышения их квалификации в области автоматической обработки информации, что является обязательным условием для оперативного и эффективного расследования компьютерных преступлений [88, с. 36].

По нашему мнению, давно назрела необходимость создания подобных подразделений в России в системе правоохранительных органов и принятия аналогичных мер с учетом богатого зарубежного опыта. Отсутствие последних, по оценкам некоторых отечественных специалистов, уже привело к тому, что компьютерная преступность выпала из сферы контроля правоохранительных органов и грозит к 2000 г. перерасти в серьезную государственную проблему, как это уже было ранее в зарубежных странах. Тенденция отечественного негативного варианта развития в этом направлении научно обоснована и подтверждена соответствующими математическими расчетами в работе Черкасова В.Н. "Теория и практика решения организационно-методических проблем борьбы с экономической преступностью в условиях применения компьютерных технологий". В ней, в частности, автор приходит к выводу о том, что опасность преступлений, связанных с использованием ЭВМ, возрастает быстрыми темпами и их количество удвоится к 2000 г. в России по сравнению с ситуацией, сложившейся на начало 90-х гг. [99, с. 26].

На основе анализа специальной литературы и публикаций в периодической печати, нормативных актов, следственной практики, информации оперативно-розыскного характера, а также опросов специалистов, нами со всей определенностью делается вывод о том, что в настоящее время вопросами борьбы с компьютерной преступностью на государственном уровне практически никто не занимается, им не уделяется должного внимания, вследствие чего правоохранительные органы лишены возможности полнокровной борьбы с этим социально опасным явлением.

Общее положение дел таково, что расследование компьютерных преступлений ведется лишь сотрудниками отделов по борьбе с экономической преступностью, не имеющих соответствующей специализации и необходимых познаний в области компьютерной техники и, как правило, связанных исключительно с хищениями (покушениями на хищение) денежных средств в крупных и особо крупных размерах, что составляет лишь незначительную часть противоправных деяний, относимых нами к категории компьютерных преступлений.

Как показывает практика, следователи, производящие расследование этой части компьютерных преступлений, сталкиваются со многими, подчас неразрешимыми трудностями, среди которых нам представляется возможным выделить следующие:

- сложность квалификации преступных деяний;
- сложность в проведении различных следственных действий из-за несовершенства действующего уголовно-процессуального законодательства;
- сложность в назначении программно-технической экспертизы средств компьютерной техники и в формулировке вопросов, выносимых на рассмотрение эксперта;
- отсутствие по некоторым вопросам соответствующих специалистов, необходимых для привлечения в ходе следствия;
- отсутствие элементарных познаний в области компьютерной техники и т. д.

Нами особо выделяются факторы, оказывающие негативное влияние на процесс расследования компьютерных преступлений и требующие своего скорейшего решения:

- 1) несовершенство уголовно-процессуального законодательства;
- 2) крайне слабая нормативная база, призванная регламентировать правовой статус и специфические особенности информационных ресурсов;
- 3) отсутствие методик расследования преступлений указанного вида;
- 4) отсутствие обобщений следственной и судебной практики;
- 5) отсутствие базового экспертно-криминалистического центра по производству необходимых экспертиз средств компьютерной техники;
- 6) отсутствие методик проведения криминалистических (программно-технических) экспертиз СКТ;
- 7) отсутствие учебно-методических центров для подготовки соответствующих специалистов для нужд правоохранительных органов;
- 8) крайне низкая оснащенность подразделений правоохранительных органов средствами компьютерной техники и региональная разобщенность при решении этих вопросов, вызванная нескоординированностью действий.

В результате совокупного взаимодействия указанных выше факторов на практике сложилась ситуация, которая существенно затрудняет возможность своевременного обнаружения преступления и полного сбора доказательств на первоначальном этапе работы по делу.

Как видно из приведенных выше статистических данных, одной из особенностей компьютерных преступлений является то, что большинство из них остаются латентными.

Анализ специальной литературы показывает, что существует много косвенных признаков, указывающих на подготовку либо совершение компьютерного преступления. К ним относятся:

- хищение носителей информации;
- ненормальный интерес некоторых лиц к содержимому мусорных емкостей (корзин, баков и т. д.);
- совершение необоснованных манипуляций с ценными данными (например, частый перевод денежных средств с одного счета на другой, наличие у одного лица нескольких счетов, проведение операций с данными, не подтвержденными соответствующими бумажными документами, либо с задержкой такого подтверждения последними и т. д.);
- нарушение заданного (нормального) режима функционирования компьютерных систем либо иных СКТ;
- проявления вирусного характера;
- необоснованная потеря значительных массивов данных;
- показания средств защиты компьютерной техники;
- необоснованное нахождение в помещениях организации посторонних лиц, включая неплановый технический осмотр помещений, оборудования, различных средств и систем жизнеобеспечения представителями обслуживающих и контролирующих организаций (электрик, сантехник, радиотелемастер, связист, инспектор госпожнадзора, энергонадзора, вневедомственной охраны, санэпидстанции, системотехник, программист, электронщик и т. д.);

— нарушение правил ведения журналов рабочего времени компьютерных систем (журналов ЭВМ) или их полное отсутствие (например, исправление в них записей, “подчистки” и “подтирки”, отсутствие некоторых записей или их фальсификация);

— необоснованные манипуляции с данными: производится перезапись (тиражирование, копирование), замена, изменение, либо стирание без серьезных на то причин, либо данные не обновляются своевременно по мере их поступления (накопления);

— на ключевых документах появляются поддельные подписи либо подпись отсутствует вообще;

— появляются подложные либо фальсифицированные документы или бланки строгой отчетности;

— некоторые сотрудники организации без видимых на то оснований начинают работать сверхурочно, проявлять повышенный интерес к сведениям, не относящимся к их непосредственной деятельности (функциональным обязанностям), либо посещать другие подразделения и службы организации;

— сотрудники возражают либо высказывают открытое недовольство по поводу осуществления контроля за их деятельностью;

— у некоторых сотрудников, непосредственно связанных с компьютерной техникой, появляется ненормальная реакция на рутинную работу;

— становятся многочисленными жалобы клиентов;

— производится передача информации лицам, не имеющим к ней доступа;

— у некоторых сотрудников проявляется небрежность при работе со средствами компьютерной техники.

<• При этом одной из главных проблем при расследовании данного вида преступных посягательств, по нашему мнению, является установление самого факта совершения преступления. Особенность заключается в том, что для того, чтобы с полным основанием утверждать, что преступление с использованием СКТ было совершено, необходимо доказать тот факт, что лицом были осуществлены определенные неправомерные действия. Одновременно с этим должно быть установлено и доказано следующее обстоятельство: имел или не имел место факт несанкционированного доступа к средствам компьютерной техники либо попытка получения такого доступа. Например, необходимо доказать, что доступ был несанкционированным с целью совершения преступления. Тогда установлению и доказыванию подлежит тот факт, что действительно были совершены несанкционированные манипуляции со средствами компьютерной техники, например с программным обеспечением, и что эти манипуляции были недозволенными, а лицо, совершавшее их, знало об этом и совершало их с целью осуществления преступного умысла.

Нами выделяются следующие основные обстоятельства, подлежащие обязательному установлению и доказыванию по делам рассматриваемой категории, а именно:

1) имело ли место преступление (либо это правонарушение иного рода);

2) каков объект преступного посягательства (данное обстоятельство имеет решающее значение для применения следователем той или иной методики расследования конкретного преступления или их совокупности);

3) каков предмет преступного посягательства;

4) каков способ совершения преступления;

5) место, время (период) и обстоятельства совершения преступления;

- 6) размер и вид ущерба, причиненного пострадавшему;
- 7) кто совершил преступление;
- 8) если преступление совершено группой лиц, то каковы состав группы и роль каждого участника;
- 9) какие обстоятельства способствовали совершению преступления.

Для наглядности обратимся к отечественной практике раскрытия и расследования компьютерных преступлений (по материалам МВД СССР и МВД России).

На протяжении многих лет наиболее распространенным видом компьютерного преступления являются хищения, совершаемые с использованием средств компьютерной техники, как правило, бухгалтерами-расчетчиками в сговоре с кассирами-раздатчиками либо другими должностными лицами путем ввода в компьютерную систему данных с фиктивных первичных бухгалтерских документов и последующего получения ничем не подтвержденных распечаток денежных сумм, подлежащих выплате через кассу. Заметим, что подобные действия стали возможными по причине отсутствия контроля со стороны соответствующих должностных лиц и ревизионных органов за достоверностью процесса вводимой в ЭВМ информации и данных, незащищенности программного обеспечения от несанкционированного ввода и вывода фальсифицированных данных, применяемых, например, для начисления заработной платы, пособий, других выплат, а также неполной автоматизации расчетов с клиентами из-за несовершенства компьютерных систем и программного обеспечения.

Так, в 1985 г. на Л-ом судостроительном заводе была разоблачена преступная группа численностью свыше 70 чел., в которую входили работники расчетного бюро центральной бухгалтерии завода, должностные и материально-ответственные лица почти всех структурных подразделений предприятия во главе с начальником бюро расчетов Б., ранее судимой за хищение. Указанным выше способом в течение 1981-1985 гг. преступниками было похищено и присвоено более 200 тыс. руб. Расследование показало, что преступники путем внесения фиктивных данных в табуляграммы незаконно завышали фактический размер средств к выплате, числящихся на субсчете балансового счета 70 ("Расчеты по оплате труда"), на котором учитывались все внеплановые выплаты, выдаваемые рабочим и служащим завода в установленном порядке (внеплановые авансы, пособия по временной нетрудоспособности, премии и т. д.). Излишки начисленных средств относились на затраты производства. Параллельно осуществлялся ввод в ЭВМ фиктивных (свободных на данный момент) табельных номеров с указанием вымышленных фамилий их владельцев. В результате чего из вычислительного центра, обслуживающего бухгалтерию, в подразделения завода поступали распечатки о начислениях заработной платы, служившие основанием для выплаты денег через кассу. Начисленные на подставных лиц деньги изымались по подложным доверенностям либо по сговору с кассиром-раздатчиком. В отдельных случаях в платежных ведомостях вместо вымышленных лиц указывались работники данного подразделения, отсутствовавшие на момент выплаты (отпуск, болезнь, командировка). При этом излишне начисленные суммы либо не отражались в их лицевых счетах, либо проходили по шифру "долг за работающим". В дальнейшем эта сумма переводилась на лицевой счет уволенного сотрудника и "погашалась" фиктивным начислением дополнительной выплаты в размере, равном "долгу".

Кроме того, бухгалтеры-расчетчики присваивали деньги путем их перечисления в сберкассу на свой расчетный счет. В этих случаях в ЭВМ осуществлялся ввод фиктивного табельного номера с указанием фамилии преступника и номера его расчетного счета в сберкассе.

До 1988 г. были разоблачены преступные группы, действовавшие аналогичными способами и совершившие хищения в крупных и особо крупных размерах на заводах П-го и "К. С." г. Горького (Н. Новгород), "Р-во" г. Ленинграда (Санкт-Петербурга) и ряде других.

Впоследствии вся фиктивная информация в памяти ЭВМ уничтожалась путем корректировки как ошибочно введенная.

Не менее "искусной" оказалась бухгалтер-расчетчик завода "К. Л." Ворошиловградской области Ш., которая вводила в ЭВМ фиктивную информацию о включении в платежные ведомости на выплату

отпускных денег работникам завода, не находившимся в действительности в отпуске. Одновременно с этим она производила корректировку данных по подоходному налогу как возврат излишне удержанного на сумму, выданную из кассы по платежной ведомости. В корректировке указывались: фиктивный табельный номер и номера тех цехов, где отражался “долг по зарплате”. Затем эти корректировки Ш. сдавала для автоматической компьютерной обработки. После этой операции преступница их уничтожала, одновременно делая исправления и в других учетных документах. Таким образом в сводках удержаний впоследствии отражались реальные суммы. В платежную ведомость на выплату зарплаты суммы корректировок подоходного налога — как “к выдаче на руки” — не поступали, а суммы, выплаченные из кассы как “долг по зарплате”, в распечатке долгов не отражались. Отметим, что характерной особенностью этой категории хищений является то, что они совершаются, как правило, одним человеком. А это создает определенные трудности в своевременном их выявлении и требует более квалифицированной организации расследования преступления.

Для этих целей, в частности, специалистами предлагаются определенные направления и способы организации проверок законности ведения кассовых операций в условиях компьютерной обработки первичных данных бухгалтерского учета, которые хорошо известны сотрудникам отделов по борьбе с экономическими преступлениями.

Рассмотрим еще одну типичную следственную ситуацию по делам о компьютерных преступлениях, проиллюстрировав ее на примере одного из первых уголовных дел данной категории, расследованного Следственным управлением ГУВД г. Москвы (использованы материалы следственной практики, обобщенные Летниковым В.А., Худяковым А.А. и Гавриловым В.С.).

Из материалов доследственной проверки усматривалось, что житель г. Москвы Б. с целью хищения валютных средств вступил в сговор с начальником отдела автоматизации неторговых операций вычислительного центра бывшего В-банка СССР Е. Осуществляя преступные намерения, Б. подделал шесть паспортов граждан и справки ряда внешнеэкономических организаций и объединений, на основании которых открыл во В-банке шесть текущих счетов, внося на каждый из них по 50 долл. США. Е. изменил программное обеспечение, использовавшееся при осуществлении банковских операций, в результате чего на открытые Б. расчетные счета было переведено в совокупности более 125 тыс. долл. По поддельным паспортам Б. получил со счетов валюту и присвоил ее.

В процессе расследования преступления следователю пришлось проводить исследование и устанавливать фактические данные на основе специальных познаний в области информатики и средств компьютерной техники. Для этих целей им были привлечены следующие специалисты: программисты, системные аналитики (“системщики”), лица, сведущие в информатике, операторы ЭВМ, инженеры по средствам связи и телекоммуникационному оборудованию, инженеры по обслуживанию компьютерной техники, по обеспечению безопасности компьютерных систем, по ведению банковского учета с использованием средств компьютерной техники, документообороту, организации бухгалтерского учета и отчетности в системе В-банка.

Имеющие значение для дела сведения выяснялись в ходе допросов лиц, проводивших ведомственную ревизию по выявленным фактам хищений денежных средств и обладавших специальными познаниями в области документального бухгалтерского учета и компьютерного аудита, а также допросов работников подразделений В-банка по месту совершения хищений о специфических особенностях бухгалтерского учета, связанного с использованием ЭВМ.

Одновременно исследовались истребованные из В-банка нормативные акты и документы, регламентирующие его операционную деятельность, порядок ведения бухгалтерского учета, в том числе с применением ЭВМ, внутрибанковского контроля и отчетности. Особое внимание обращалось на анализ положений должностных инструкций лиц, обслуживающих компьютерную технику, документов, содержащих перечень и характер задач комплексного программного обеспечения компьютерных систем и технических указаний по ведению автоматизированного документального учета с их применением. Тщательно и всесторонне изучались технические средства, использовавшиеся для автоматизации банковских операций.

Полученные в ходе допросов и анализа документальные данные позволили наметить комплекс неотложных следственных действий, обязательных, на наш взгляд, для первоначального этапа расследования преступлений подобного вида.

Во-первых, это проведение обыска в служебном помещении по месту работы подозреваемого в совершении компьютерного преступления. Обыск был проведен в данном случае у подозреваемого сотрудника вычислительного центра в присутствии понятых, обладавших специальными познаниями в области СКТ и технологии. Целью обыска являлось обнаружение и изъятие физических (материальных) носителей машинной информации, представленных в данном случае в виде: магнитных лент ЭВМ в бобинах и кассетах (магнитные носители), графических (знакосинтезированных) распечаток — листингов, выполненных с использованием печатающих СКТ (принтеров) на бумажном носителе, содержащих данные, относящиеся к банковским операциям подразделений В-банка по месту совершения преступлений, и других документов, имеющих или возможно имеющие отношение к несанкционированному изменению программного обеспечения или носящих иные следы с целью хищения денежных средств. При этом следователем было принято во внимание следующее обстоятельство: по установленному в вычислительном центре (ВЦ) порядку магнитные носители с первоначальными записями хранились лишь в течение строго определенного времени (в рассматриваемом случае — 2 недели), после чего они повторно использовались для записи на них очередных данных и информации с одновременным стиранием (уничтожением) ранее записанной на них предыдущей информации.

Изъятые в процессе обыска и приобщенные к делу в качестве вещественных доказательств предметы были отправлены на экспертное исследование технической экспертизой программных средств компьютерной техники.

Кроме вышеперечисленного, был также изъят журнал сбойных ситуаций ВЦ, ведущийся как в подразделениях банка по месту совершения преступлений, так и в обслуживающем данное подразделение отделе ВЦ.

Отметим, что, помимо этого, в некоторых отдельных случаях имеющие значение для дела сведения могут быть получены и в результате исследования:

- журналов рабочего времени компьютерных систем (журналов ЭВМ);
- “прошитых” микросхем постоянного запоминающего устройства (ПЗУ) и микропроцессора компьютерной техники или их схемного соединения;
- распечаток информации оперативного запоминающего устройства (ОЗУ) — оперативной памяти ЭВМ и пошаговых действий последней;
- всего программного обеспечения ЭВМ;
- средств защиты и контроля компьютерных систем, регистрирующих пользователей, моменты включения (активации) компьютерной системы либо подключения к ней абонентов с определенным индексом или без такового;
- данных журнала о передаче смен операторами ЭВМ;
- контрольных чисел файлов;
- протоколов вечернего решения, представляющих собой копию действий оператора компьютерной системы, отображенную на бумажном носителе информации в ходе вечерней обработки информации, которая проводится по истечении каждого операционного дня, и хранящуюся определенное время, после чего она уничтожается на основании и в порядке, предусмотренном ведомственными инструкциями [86].

Во-вторых, это истребование и анализ технических указаний по обработке ежедневной бухгалтерской информации, осуществляемой с использованием СКТ с перечнем выходящих форм, например листингов. Как правило, в них имеются статистические сведения и данные контроля достоверности банковской информации, содержащейся или находящиеся в компьютерной системе. В рассматриваемом нами примере выходные формы также были изъяты в ходе проведения обыска и подвергнуты экспертному исследованию. Одновременно с этим

производились допросы лиц из числа инженеров-программистов, занимавшихся разработкой программного обеспечения и его сопровождением (отладкой и обслуживанием), и специалистов-электронщиков отдела технического обеспечения ВЦ, занимающихся эксплуатацией и ремонтом СКТ. Отметим, что при расследовании данного уголовного дела наибольшие трудности возникли у следователя в процессе назначения экспертизы. В результате чего им было принято наиболее правильное решение о назначении комплексной судебно-бухгалтерской и программно-технической экспертизы. Это потребовало тщательного подбора соответствующих специалистов, сведущих в этих областях. В связи с чем в состав экспертной комиссии были приглашены квалифицированные сотрудники соответствующих подразделений В-банка и его ВЦ, Главного ВЦ Центрального банка России, а также ВЦ одной из воинских частей, специализирующиеся на научных исследованиях в сфере программного обеспечения и защиты компьютерных систем.

Для проверки правильности документального бухгалтерского учета был привлечен ревизор Главного контрольно-ревизионного управления (КРУ) Управления Центрального банка России.

Участие в экспертном исследовании сотрудников отдела компьютерного аудита, а также специалистов ВЦ В-банка в области решения банковских задач было продиктовано необходимостью полного и тщательного исследования материалов операционной работы банка с учетом ее специфики в результате использования СКТ. бухгалтерского учета и отчетности, могли способствовать и способствовали образованию ущерба.

Заметим, что проведение указанных выше исследований при активном участии следователя и умелое использование им совокупности добытых по делу доказательств позволили обеспечить достаточные основания для привлечения преступников Б. и Е. к уголовной ответственности за хищение государственных денежных средств в особо крупных размерах. Помимо этого, действия Б., связанные с подделкой паспортов и справок, были дополнительно квалифицированы по ч. 1 ст. 196 Уголовного кодекса РСФСР.

Как показывает анализ следственной практики по делам рассматриваемой категории, существует постоянная необходимость использования в процессе расследования специальных познаний в области новых информационных технологий. Данные познания необходимы как для получения доказательств, так и для процессуального оформления документов, подготовленных средствами компьютерной техники, которые впоследствии могут играть роль доказательств. По нашему мнению, все это должно оформляться как заключение эксперта. Данный вид криминалистических экспертиз появился в России с начала 90-х гг. и получил рабочее название "программно-техническая экспертиза". В настоящее время с помощью таких экспертиз могут решаться следующие задачи (здесь и далее по тексту работы используются материалы обобщения практики подготовки и назначения программно-технических экспертиз, подготовленные Катковым С.А., Собециким И.В. и Федоровым А.Л.).

1. Воспроизведение и распечатка всей или части (по определенным темам, ключевым словам и т. п.) информации, содержащейся на физических носителях СКТ, в том числе находящейся в нетекстовой форме (в сложных форматах языков программирования), например в форме электронных таблиц, баз данных, WINDOWS и т. д.
2. Восстановление информации, ранее содержавшейся на физических носителях СКТ и впоследствии стертой (уничтоженной) или измененной (модифицированной) по различным причинам.
3. Установление времени ввода, изменения, уничтожения, либо копирования той или иной информации (документов, файлов, программ и т. д.).
4. Расшифровка закодированной информации, подбор Паролей и раскрытие защиты СКТ.
5. Установление авторства, места (средства) подготовки и способа изготовления документов (файлов, программ).
6. Выяснение возможных каналов утечки информации из компьютерной сети и помещений.

7. Выяснение технического состояния, исправности СКТ, процента их износа, оценки их стоимости, а также адаптации СКТ под конкретного пользователя.

8. Установление уровня профессиональной подготовки отдельных лиц, проходящих по делу, в области программирования и в качестве пользователя.

Исходя из указанных выше задач, следователь может поставить на разрешение эксперта следующие основные вопросы:

1. Какая информация содержится на физических носителях СКТ, представленных на исследование?

2. Раскодировать информацию, записанную в сложных форматах.

3. Какие текстовые документы (файлы) по интересующей теме находятся на представленных физических носителях СКТ?

4. Какие текстовые документы (файлы) по интересующей следствии теме были стерты (уничтожены), скопированы, изменены (модифицированы). Каковы их имена, размер, даты создания (уничтожения, изменения)?

5. Как изменялось содержание обнаруженных документов (файлов) на представленных на исследование физических носителях информации (указать параметры предыдущего вопроса)?

6. Получить скрытую информацию, касающуюся проходящих по делу лиц (физических и юридических).

7. Подготовлены ли представленные на исследование документы (файлы) на представленной на исследование технике?

8. Дать заключение об исправности (проценте износа, оценки стоимости и т. п.) СКТ, представленных на исследование.

9. Исследовать представленные СКТ на предмет наличия в них изменений вирусного характера либо иных, влияющих на алгоритм (параметры) нормального функционирования СКТ (заданных изготовителем), либо на конечные результаты работы конкретного программного продукта. В положительном случае определить механизм внесения таких изменений, место, время, характер и их последствия.

Указанный выше список вопросов, естественно, не является исчерпывающим и может быть расширен, исходя из обстоятельств конкретного уголовного дела. При этом в затруднительных случаях при постановке вопросов следует консультироваться у самого эксперта.

В настоящее время программно-технические экспертизы выполняются только в ИЦ ГУВД Московской области. Специалистами указанного учреждения в 1994 г. были разработаны и апробированы на практике некоторые основные аспекты методики подготовки и назначения рассматриваемых экспертиз.

Анализ литературных источников свидетельствует о том, что отечественными учеными достаточно активно ведутся разработки следующих методик экспертного исследования в этой области. Так, под руководством Е. Белоглазова разрабатывается методика идентификации пользователя ЭВМ при отработке следственной версии о том, что определенное лицо произвело какие-либо манипуляции с машинной информацией. Суждение относительно принципиальной возможности такого отождествления основано на том, что комплекс периодов времени нажатия на различные клавиши клавиатуры терминала можно рассматривать как своеобразный таймерный "почерк" по аналогии с "почерком" работы радиотелеграфиста в режиме передачи на ключе радиопередатчика. При условии его фиксации с использованием средств компьютерной техники он может способствовать, по утверждению автора, определению классификационной группы, к которой относится искомый пользователь-оператор, а в некоторых благоприятных случаях и

индивидуализировать его, поскольку скорость работы пользователя на клавиатуре обусловлена степенью выработанности у него соответствующих навыков.

Отрицательным моментом этой идеи, на наш взгляд, является то, что существует немало факторов, способных осложнить проведение исследования и исказить его результаты, например стресс, опьянение оператора, попытки симитировать навыки работы другого лица, ограничение зрительного контроля и т. д. Тем не менее, благодаря подобному исследованию, можно будет исключить из числа причастных к проверяемым операциям всех законных пользователей системы или сети, что должно означать установление несанкционированного доступа к информационной системе подозреваемого. После установления “почерка”, он может быть зафиксирован на физическом носителе в качестве следов преступления [86, с. 38].

По мнению ряда специалистов, давно назрела необходимость в разработке следующих методик экспертного исследования:

1) установления соответствия определенной компьютерной системы или сети стандарту и проверки ее работы с помощью специальных тестов;

2) исследования вещественных доказательств, предусматривающего:

— фиксацию источника, вида, способа ввода, вывода данных и их обработку;

— выявление изменений и дополнений в программных средствах;

— восстановление поврежденных или уничтоженных файлов;

— восстановление поврежденных магнитных и иных носителей машинной информации;

— определение давности исполнения отдельных фрагментов программных средств;

3) идентификации автора программного средства, его назначения (вирусного или иного), установления факта его интерпретации и пределов дозволенной компиляции.

В этом направлении определенным научным интересом, с нашей точки зрения, представляются разработки А. Комиссарова, основанные на использовании в качестве общего идентификационного признака степень выработанности у автора программного средства профессиональных навыков, а в качестве частных признаков — используемых в автороведческой экспертизе синтаксических, лексических особенностей письменной речи, топографических признаков и т. д. [86, с. 38].

Очень часто в процессе расследования компьютерного преступления возникает необходимость в установлении этапов обработки бухгалтерских данных с использованием ЭВМ, на которых вносились те или иные изменения, признаков интеллектуального подлога в первичных и сводных бухгалтерских документах, составленных на ЭВМ, в установлении фактов уменьшения облагаемой налогом прибыли, выявления причастных к совершению компьютерного преступления счетных работников путем исследования носителей оперативной информации, а также лиц, введших соответствующие данные в ЭВМ, и т. д. По нашему мнению, для этих целей возможно использовать уже существующие методики производства судебно-бухгалтерских экспертиз, позволяющие при проведении исследований установить, насколько соблюдены те или иные требования положений о документах и документообороте в бухгалтерском учете при оформлении различных хозяйственных и иных операций первичными документами и отображении их в регистрах бухгалтерского учета и отчетности, в том числе выраженных в форме, зафиксированной на машинном носителе и машинограмме, созданных средствами компьютерной техники. В случаях выявления нарушения этих нормативных документов эксперт-бухгалтер может установить их причины (не сделаны ли они с целью совершения преступления: злоупотребления, сокрытия недостачи материальных ценностей, уменьшения их размера и т. д.) одновременно формулируя вывод о том, насколько нарушения положений повлияли на состояние бухгалтерского учета и выполнение функций лицами, ответственными за это в управлении хозяйственной или иной деятельностью. При этом возможно установление лиц, ответственных за созданные или допущенные нарушения правил составления первичных документов и учетных регистров [9, с. 107]. Как показывает анализ следственной практики, основной проблемой при выявлении и

расследовании преступлений рассматриваемой категории является отсутствие у сотрудников минимально необходимых специальных познаний в этой области. Большая сложность возникает в вопросах терминологии, определения понятия составных частей компьютерной системы и сетей, правильного понимания общего режима их функционирования в различных технологических процессах. Все это приводит к тому, что многие нормативные документы, регламентирующие правовой режим функционирования средств компьютерной техники, остаются неизвестными и соответственно не учитываются в процессе проведения оперативно-розыскных мероприятий и следственных действий, что в конечном итоге значительно затрудняет выявление преступлений, сказывается на полном и объективном расследовании уголовных дел данной категории. Особенно много ошибок возникает при производстве следственных действий, которые, как правило, проводятся без участия соответствующего специалиста и без учета специфики расследуемого преступления.

Так, например, при осмотре места происшествия изымаются не все средства компьютерной техники (СКТ), несущие в себе следы преступной деятельности и имеющие важное значение для следствия, а те из них, которые изымаются, не могут впоследствии играть роль доказательств (в соответствии со ст.ст. 69 и 83 УПК — см.: 91), т. к. их изъятие в подавляющем большинстве случаев производится с нарушением установленного порядка и правил, учитывающих специфику предмета, в результате чего теряется их процессуальное значение. Поэтому в процессе расследования компьютерных преступлений при производстве практически любых следственных действий считаем необходимым в обязательном порядке привлекать соответствующего специалиста (специалистов).

Помимо этого, следователю необходимо знать, что существует много особенностей, которые должны учитываться при производстве отдельных следственных действий. Приведем примеры некоторых из них.

Если следователь располагает информацией, что на объекте обыска находятся СКТ, расшифровка данных с которых может дать доказательства по делу, он должен заранее подготовиться к их изъятию. Необходимо участие в ходе обыска как минимум двух специалистов по компьютерной технике: программиста (системного аналитика) и связиста.

По прибытии на место обыска следует сразу же принять меры к обеспечению сохранности СКТ и имеющихся на них данных и ценной информации. Для этого необходимо:

- 1) не разрешать кому бы то ни было из лиц, работающих на объекте обыска или находящихся здесь по другим причинам (персоналу), прикасаться к СКТ с любой целью;
- 2) не разрешать кому бы то ни было из персонала выключать электроснабжение объекта;
- 3) в случае если на момент начала обыска электроснабжение объекта выключено, то до его восстановления следует отключить от электросети всю компьютерную технику, находящуюся на объекте;
- 4) самому не производить никаких манипуляций со средствами компьютерной техники, если результат этих манипуляций заранее неизвестен;
- 5) при наличии в помещении, где находятся СКТ, опасных веществ, материалов и/или оборудования (взрывчатых, токсических, едких, легковоспламеняющихся, магнитных и электромагнитных и т. п.) удалить их в другое помещение;
- 6) при невозможности удаления опасных материалов из помещения, а также при настойчивых попытках персонала получить доступ к СКТ принять меры для удаления персонала в другое помещение.

После принятия указанных выше неотложных мер можно приступать к непосредственному обыску помещения и изъятию СКТ. При этом следует принять во внимание следующие неблагоприятные факторы:

— возможные попытки со стороны персонала повредить СКТ с целью уничтожения информации и ценных данных;

— возможное наличие на СКТ специальных средств защиты от несанкционированного доступа, которые, не получив в установленное время специальный код, автоматически уничтожат всю информацию;

— возможное наличие на СКТ иных средств защиты от несанкционированного доступа;

— постоянное совершенствование СКТ, следствием чего может быть наличие на объекте программно-технических средств, незнакомых следователю.

В целях недопущения вредных последствий перечисленных факторов следователь может придерживаться следующих рекомендаций:

1. Перед выключением питания по возможности корректно закрыть все используемые программы, а в сомнительных случаях просто отключить компьютер (в некоторых случаях некорректное отключение компьютера — путем перезагрузки или выключения питания без предварительного выхода из программы и записи информации на постоянный носитель — приводит к потере информации в оперативной памяти и даже к стиранию информационных ресурсов на данном компьютере).
2. При наличии средств защиты СКТ от несанкционированного доступа принять меры к установлению ключей доступа (паролей, алгоритмов и т. д.).
3. Корректно выключить питание всех СКТ, находящихся на объекте (в помещении).
4. Не пытаться на месте просматривать информацию, содержащуюся на СКТ.
5. В затруднительных случаях не обращаться за консультацией (помощью) к персоналу, а вызывать специалиста, не заинтересованного в исходе дела.
6. Следует изъять все СКТ, обнаруженные на объекте.
7. При обыске не подносить ближе 1 м к СКТ металлоискатели и другие источники магнитного поля, в т. ч. сильные осветительные приборы и некоторую спецаппаратуру.
8. Поскольку многие, особенно неквалифицированные, пользователи записывают процедуру входа-выхода, работы с компьютерной системой, а также пароли доступа на отдельных бумажных листках, следует изъять также все записи, относящиеся к работе СКТ.
9. Так как многие коммерческие и государственные структуры прибегают к услугам штатных и временно работающих специалистов по обслуживанию СКТ, следует записать паспортные данные у всех лиц, находящихся на объекте, независимо от их объяснений цели пребывания на объекте.

При изъятии средств компьютерной техники необходимо обеспечить строгое соблюдение требований действующего уголовно-процессуального законодательства. Для этого необходимо акцентировать внимание понятых на всех производимых действиях и их результатах, давая им при необходимости пояснения, поскольку многим участникам следственного действия могут быть непонятны производимые манипуляции. Кроме того, следует опечатывать СКТ так, чтобы исключить возможность работы с ними, разуклоптовки и физического повреждения основных рабочих компонентов в отсутствие владельца или эксперта. При опечатывании компьютерных устройств следует наложить один лист бумаги на разъем электропитания, расположенный на задней панели, второй — на переднюю панель сверху с захлестом на верхнюю панель и закрепить их края густым клеем. На листах бумаги должны быть подписи следователя, понятых и представителя персонала. При изъятии магнитного носителя машинной информации нужно помнить, что они должны перемещаться в пространстве и храниться только в специальных опломбированных и экранированных контейнерах или в стандартных дискетных или иных алюминиевых футлярах заводского изготовления, исключающих разрушающее воздействие различных электромагнитных и магнитных полей и “наводок”, направленных излучений. Для

опечатавания магнитных носителей лучше всего упаковать их в пакет из обычной фольги (возможно от оберток плиточного шоколада) и опечатать их обычным способом. Недопустимо приклеивать что-либо непосредственно к физическим носителям информации, пропускать через них бечеву, пробивать стиплером, наносить подписи или маркировки (пометки), пластилиновые (сургучные) печати и т. д.

В случае когда необходимо сослаться непосредственно на определенный физический носитель, следует указать в протоколе его серийный (заводской) номер, тип, название (если есть) или провести его точное описание (размеры, цвет, класс, надписи, физические повреждения). При отсутствии четких внешних признаков физический носитель запечатывается в отдельную коробку (ящик, конверт), о чем обязательно делается отметка в протоколе проведения следственного действия.

В случае невозможности изъятия и приобщения к делу в качестве вещественного доказательства средства компьютерной техники (например, если компьютер является сервером или рабочей станцией компьютерной сети) в обязательном порядке после его осмотра необходимо блокировать не только соответствующее помещение, но и отключать источники энергоснабжения аппаратуры или в крайнем случае создать условия лишь для приема информации с одновременным опломбированием всех необходимых узлов, деталей, частей и механизмов компьютерной системы.

Если же возникла необходимость изъятия информации из оперативной памяти компьютера (непосредственно из оперативного запоминающего устройства — ОЗУ), то сделать это возможно только путем копирования соответствующей машинной информации на физический носитель с использованием стандартных паспортизированных программных средств с соответствующим документальным приложением и в порядке, установленном следующими нормативными документами: Государственный стандарт (ГОСТ) № 6104-84 от 01.07.87 “УСД. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения” и Постановление Госстандарта № 2781 от 24.09.86 “Методические указания по внедрению и применению ГОСТ 6104-84” [18; 73]. Только с использованием указанных нормативных документов машинная информация будет относиться к разряду “документированной информации”, как требует того закон [31]. В данном случае необходимо установить и зафиксировать в протоколе проведения следственного действия следующее:

— программу, исполняемую компьютером на момент проведения следственного действия или последнюю исполненную им. Для этого необходимо детально изучить и описать изображение, существующее на экране дисплея компьютера, все функционирующие при этом периферийные устройства и результат их деятельности. Необходимо знать, что многие сервисные программные средства позволяют определить и просмотреть наименование всех ранее вызывавшихся программ и последнюю исполненную. Например, с использованием NORTON COMMANDER последняя исполнявшаяся программа определяется по положению курсора (выделенной световой полосой);

— результат действия обнаруженной программы;

— все манипуляции со средствами компьютерной техники (включая нажатия на клавиши клавиатуры), произведенные в процессе проведения следственного действия, и их результат (например, при копировании программ и файлов, определении их атрибутов, времени и даты создания и записи, а также при включении и выключении аппаратуры, порядка отсоединения ее частей).

Изъятие аппаратуры СКТ производится только в выключенном состоянии. При этом должны быть выполнены и отражены в протоколе следующие действия:

— установлено включенное оборудование и зафиксирован порядок его отключения;

— описано точное местонахождение изымаемых предметов и их расположение относительно друг друга и окружающих предметов (с приложением необходимых схем и планов);

— точно описан порядок соединения между собой всех устройств с указанием особенностей соединения (цвет, количество, размеры, характерные индивидуальные признаки соединительных проводов, кабелей, шлейфов, разъемов, штеккеров и их спецификация);

— определено отсутствие либо наличие используемого для нужд СКТ канала (каналов) связи и телекоммуникаций. В последнем установлены тип связи, используемая аппаратура, абонентский номер, позывной либо рабочая частота;

— разъединены с соблюдением всех необходимых мер предосторожности аппаратные части (устройства) с одновременным опломбированием их технических входов и выходов [52, с. 241-243].

Как показывает практика, при изъятии средств компьютерной техники у следователя могут возникать конфликты с персоналом. При их разрешении дополнительно к вышеизложенным правилам желательно руководствоваться следующими рекомендациями:

1) недопустимо производить изъятие в несколько приемов, даже если следователь не располагает необходимым транспортом. В этом случае нужно сделать несколько рейсов с объекта до места хранения изъятых материалов;

2) изъятые материалы не могут быть оставлены на ответственное хранение на самом объекте или в другом месте, где к ним могут иметь доступ посторонние лица;

3) недопустимо оставление на объекте части средств компьютерной техники по мотивам ее “абсолютной необходимости” для деятельности данной фирмы (организации). Желание персонала сохранить от изъятия определенные СКТ обычно указывает на наличие на них важной для следствия информации;

4) следует изымать все СКТ, находящиеся в помещении объекта, независимо от их юридической принадлежности;

5) если персонал настаивает на отражении в протоколе следственного действия конкретных качеств изымаемых СКТ (марка, быстродействие, марка процессора, объем памяти и т. д.), то эти сведения могут быть записаны лишь как отдельные заявления.

Обратим особое внимание на то, что при производстве любых следственных действий, касающихся непосредственно компьютерных систем и средств их защиты, необходимо перед их началом в обязательном порядке получать и анализировать информацию, касающуюся их периферийной принадлежности, уровня соподчиненности и используемых при этом телекоммуникационных средств во избежание: их разрушения либо нарушения заданного технологического ритма и режима функционирования; причинения крупного материального ущерба; уничтожения вещественных доказательств, следов и документов.

Отметим также, что при расследовании компьютерных преступлений зачастую трудно бывает установить как объективную, так и субъективную сторону преступления. Сложность для следствия здесь заключается в том, что очень часто преступник не может в полной мере представить себе последствия своей деятельности. Такая неопределенность часто возникает, например, при попытках несанкционированного доступа в компьютерные сети. Преступник не всегда правильно представляет себе ценность копируемой, уничтожаемой или искажаемой информации, а тем более дальнейшие последствия, к которым могут привести его действия. Специфичность СКТ такова, что одни и те же действия приводят к разным последствиям при различных (и часто совершенно неизвестных преступнику) состояниях вычислительной системы, ее загрузки, степени надежности и защищенности, связи с другими системами. Все это в конечном итоге приводит к сложности не только в установлении причинно-следственных связей, но и в определении всех последствий преступления, не говоря уж об отличии умысла от неосторожности.

Как отмечают зарубежные специалисты, затрудняет процесс расследования компьютерных преступлений такое обстоятельство, как сокрытие преступником следов своей деятельности, например путем стирания данных или путем введения в компьютерную систему потерпевшей стороны вредоносных программ типа “логическая бомба”, “троянский конь”, компьютерный вирус и т. п. Непросто также установить причинно-следственную связь между фактом совершения преступления и подозреваемым, особенно в случае наличия значительного числа пользователей компьютерной системы [79, с. 8].

Помимо вышеуказанного, существующая в настоящее время в России инфраструктура связи и телекоммуникаций, по нашему мнению, не обеспечивает пользователя достаточно адекватной защитой от попыток получения несанкционированного доступа к СКТ, равно как и не дает возможности к установлению личности преступника, пользующегося этой связью.

Таким образом, работа по раскрытию и расследованию компьютерных преступлений обладает целым рядом особенностей и требует специальной подготовки сотрудников правоохранительных органов.

Как свидетельствует зарубежный опыт и показывает отечественная практика, прежде всего сам следователь должен обладать определенными познаниями и навыками в этой области (знать терминологию, составные части компьютерной системы и сетей, общий режим их функционирования, основные нормативные документы, регламентирующие этот режим, правовые акты, определяющие статус машинной информации и иных информационных ресурсов, обладать навыками пользователя ЭВМ и т. д.), поскольку без этого невозможно полное и объективное расследование уголовных дел данной категории. Это подтверждают и данные проведенного нами исследования. Так, на вопрос «Нужны ли следователю, ведущему подобные уголовные дела, специальные познания в этой области?» 65% респондентов ответили «Да», а 46% из них подчеркнули «Обязательно», тогда как «Нет» ответили всего 2% опрошенных. Между тем реальное положение дел таково, что на практике лишь 15% следователей (из числа опрошенных) имеют эти познания и используют их непосредственно для своей работы, 37% — их не имеют вообще, а 48% — имеют лишь частичные познания в этой области. Нетрудно подсчитать, что общий процент следователей, совершенно не обладающих данными познаниями, составляет 85% ! Одновременно с этим респондентами отмечалась необходимость в получении подобных знаний: на вопрос «Требуется ли обучение сотрудников органов внутренних дел для работы на компьютере в качестве пользователя?» ответили «Да» 78%, из них «Обязательно» — 28%.

Дальнейшее исследование показало, что подобная ситуация, характеризующая обозначенную выше проблему, сложившаяся на начало сентября 1994 г. в органах внутренних дел (на момент проведения исследования), обусловлена, по нашему мнению, значительным некомплектом подразделений ОВД средствами компьютерной техники. По данным проведенного нами исследования видно, что в среднем активно использовалось в масштабе городского (районного) управления (отдела) ОВД лишь 4 ед. указанной техники при общем недостатке соответствующих программных средств, отсутствии специалистов и необходимых знаний у сотрудников ОВД и их начальников.

Известно, что расследование преступлений как специальный вид юридической деятельности предполагает планирование, организацию и проведение определенной совокупности действий и образующих их операций, успешная реализация которых в конечном итоге должна привести к достижению желаемых результатов — выявлению события преступления и лица (лиц), его совершившего.

В ходе многовековой практики расследования преступлений определился круг таких действий и их направленность, целевые функции, что позволяет говорить об их определенной типизации, в частности применительно к расследованию конкретных видов преступлений. Кроме того, глубокий анализ следственной практики показал, что, хотя к началу расследования любого преступления могут сложиться различные следственные ситуации, все их многообразие тоже можно подразделить на несколько наиболее характерных групп, или, иными словами, типизировать, выделить типичные следственные ситуации.

В свою очередь конкретная следственная ситуация обуславливает основные направления расследования, в частности те следственные версии, которые она порождает и проверка которых требует проведения сугубо определенных следственных или оперативно-розыскных действий, что опять-таки приводит к типизации операций по выявлению, исследованию и использованию разнообразной криминалистической информации, которую можно обрабатывать с использованием соответствующих орудий — компьютерной техники.

Все это и позволяет считать, что наиболее перспективным направлением совершенствования организации работы следователя является использование персональных компьютеров и других средств компьютерной техники в процессе предварительного расследования компьютерных

преступлений. Подобное утверждение подтверждается и данными зарубежной специальной литературы.

Как показывает практика, обработка всей имеющейся информации и документов по расследуемому уголовному делу с использованием персональных компьютеров позволяет значительно сократить сроки предварительного расследования, уменьшить временные затраты на оформление и составление необходимых материалов и документов, а значит, больше внимания уделить тактике расследования преступления и в конечном итоге более полно и объективно провести расследование с одновременной его оптимизацией.

Исследованию данной проблемы было уделено достаточно много внимания со стороны широкого круга исследователей, среди которых можно выделить: Баранова А.К., Белякова К.И., Бобрынина Н.Б., Карпычева В.Ю., Кузьмина А.П., Минаева В.А., Полежаева А.П., Попова Ю.В., Смирнова Д.И., Цымбалюка В.И., Черкасова В.Н., Швеца Н.Я. и др.

Как отмечается авторами, наиболее эффективным средством при расследовании уголовных дел с большим объемом информации, текстовых и числовых данных является использование персонального компьютера. Последний позволяет следователю в максимально сжатые сроки своевременно сопоставлять между собой различные документы, находить в них взаимные противоречия, устанавливать отклонения от стандартного образца, а также определять множества числовых показателей по большому количеству документальных форм, производить другие действия, связанные с хранением, поиском, обработкой накапливаемой оперативной информации значительного объема и содержания и имеющей важное значение для следствия. Помимо этого, возникает постоянная необходимость в корректировке и анализе текстовой информации, потребность поиска в материалах уголовного дела различных причинно-следственных связей, в подготовке многих процессуальных и непроцессуальных документов. Этому есть и практическое подтверждение. Например, исходя из факта конкретного уголовного дела, впервые расследованного с использованием персонального компьютера работниками следственной части ГСУ МВД РСФСР в 1990 г. Об эффективности его применения в расследовании говорят следующие цифры:

— всего по делу проходил 31 обвиняемый;

— было исследовано 24 эпизода хищений государственного имущества, 11 эпизодов краж личного имущества граждан и 21 эпизод иных преступлений, совершенных обвиняемыми, в том числе: подделка документов, незаконное хранение и ношение холодного и огнестрельного оружия и боеприпасов и т. д.;

— на 21 обвиняемого дело было направлено в суд, причем окончательная распечатка всех постановлений заняла всего один рабочий день, хотя объем лишь одного постановления составлял порядка 10-15 страниц машинописного текста;

— печатание обвинительного заключения объемом в 200 машинописных страниц заняло всего 6 рабочих часов.

Отметим, что в условиях роста преступности, снижения уровня раскрываемое преступлений, повышения требований к доказыванию вины обвиняемых, о которых нами говорилось в первой главе настоящей работы, решение задач, стоящих перед правоохранительными органами, уже невозможно только экстенсивным путем, только путем наращивания сил и средств. Усложнение процесса расследования предъявляет совершенно иные, гораздо более высокие требования к мыслительной деятельности следователя. Данный вид деятельности, в свою очередь, требует высочайшей квалификации, большого опыта работы, глубоких знаний из самых различных отраслей науки. Помочь в этом следователю, по нашему мнению, может только активное использование им в работе средств компьютерной техники, и в частности персонального компьютера. Последний потому и называется персональным, что ориентирован на разработку и решение различного рода задач, поставленных пользователем без участия каких-либо посредников — специалистов.

Для нормального и эффективного функционирования любой компьютерной системы, как известно, необходимо соответствующее программное обеспечение, и в частности то, которое

непосредственно участвует в информационном технологическом процессе расследования преступления, подчиняющегося, как правило, определенной стандартной процедуре [43].

Исходя из вышесказанного, в настоящее время можно отчетливо выделить два основных направления в разработке программного обеспечения для нужд органов внутренних дел. Рассмотрим их детальнее. (Здесь и далее по тексту используются материалы обобщения практики применения средств компьютерной техники в деятельности ОВД России, подготовленные авторами: Щербининым А.И., Игнатовым Л.Н., Зайченко В.С., Мاستинским Я.М., Николаевым В.Н., Котовым И.А., Михайловым М.Ю.)

1. Программы (комплексы) расследования уголовных дел, позволяющие следователю оформлять процессуальные и непроцессуальные документы, осуществлять визуальный анализ материалов уголовного дела и характеризующиеся следующим набором обрабатываемой информации:

- фиксируемой следователем в процессуальных документах (протоколах, постановлениях и т. д.);
- истребованной следователем по запросам (справки, характеризующий материал и т. д.);
- получаемой при анализе процессуальных документов (формула обвинения, обвинительное заключение, постановление о прекращении уголовного дела и т. д.).

Отсюда следует и перечень автоматизируемых функций:

- заполнение процессуальных документов;
 - составление формулы обвинения;
 - оформление характеризующего материала;
 - составление материалов профилактических мероприятий;
 - систематизация материалов уголовного дела;
 - поиск необходимых сведений в имеющихся материалах уголовного дела (фамилии, имена, клички, даты, суммы, эпизоды, протоколы, постановления и другие реквизиты);
 - составление обвинительного заключения или другого необходимого документа;
 - подготовка справочных материалов для направления в суд.
2. Программы обработки сопутствующей информации (не использованной в материалах конкретного уголовного дела) и дополнительного анализа материалов уголовного дела для основных видов расследуемых преступлений, где под сопутствующей информацией понимаются сведения, являющиеся рабочим материалом следователя (по типу "записной книжки") и не оформленные в процессуальных документах, приобщенных к уголовному делу.

Данные программы позволяют следователю обрабатывать следующие категории информации:

- сведения о лицах, данные о которых имеются в деле;
- связи лиц, проходящих по делу;
- сведения о вещественных доказательствах (как появились в деле, их описание, денежная оценка, место хранения и т. д.);
- данные об эпизодах преступлений (описание эпизодов, место, время, участники, способ совершения, наличие вещественных доказательств и т. д.).

Автоматизации подлежат следующие функции: ввод, хранение и обработка (поиск и вывод) информации следующего содержания:

- о лицах, сведения о которых имеются в деле;
- о связях лиц, проходящих по делу;
- о вещественных доказательствах;
- об эпизодах преступлений.

При этом нами особо выделяется следующее обстоятельство:

удельный вес перечисленных выше факторов может существенно изменяться каждым конкретным пользователем в зависимости от количественных и качественных характеристик расследуемого уголовного дела, например от количества эпизодов, участников следственного процесса, вида и состава преступлений.

Как видно из вышеприведенного, основные требования, предъявляемые к программному обеспечению персональных компьютеров, достаточно просты и сводятся к одному понятию: использовать компьютерные системы только в качестве обычной электронной пишущей машинки и автоматизированного банка данных, с чем, естественно, нельзя согласиться. Проведя анализ наиболее распространенных программных средств, используемых в настоящее время в органах внутренних дел, нами было установлено, что все они в основном направлены на решение тех же задач, которые требуют для этих целей чрезвычайно малых вычислительных ресурсов имеющейся на вооружении компьютерной техники, используя при этом ее мощности неэффективно. К ним, в частности, можно отнести следующие программные средства:

- 1) текстовые редакторы “Фотон” и “Лексикон”;
- 2) система анализа и учета уголовных дел в интерактивной среде “Мастер” (САУД-М);
- 3) гипертекстовая система “Интелтекст”, созданная на базе системы “БАГИС” и применяемая только высококвалифицированным пользователем;
- 4) автоматизированная система “АРСЕНАЛ”, функционирующая на основе начальных версий программного средства “Флинт”;
- 5) автоматизированные информационно-поисковые системы (АИПС): “Опознание”, “Спрут”, “Кондор”, “Сейф”, “Дакто-эксперт”, “Папилон”, “Портрет”, “Квадрат” и др.;
- 6) диалоговый конструктор “БИНАР-3” (ДК БИНАР). На последнем программном продукте стоит остановиться более подробно, т. к., по нашему мнению, он в настоящее время наиболее эффективен по сравнению с другими в плане его применения в процессе расследования компьютерных преступлений, связанных с хищением денежных средств в банковских, финансовых и коммерческих структурах, характерной особенностью которых является наличие нескольких десятков и сотен участников процесса, большого числа эпизодов, учетно-бухгалтерских и иных документов.

Программное средство диалоговый конструктор “БИНАР-3” предназначен для решения информационно-справочных и информационно-логических задач на совокупности взаимосвязанных объектов учета (ОУ), задач информационной поддержки принятия решений, задач синтеза новой информации на основе построения цепочек связей и задач идентификации ОУ. ДК БИНАР работает в операционной системе Novell Net Ware (версии не ниже 2.2), предназначенной для работы в сетевом режиме с распределенными базами данных (БД) с отношениями вида M; N, обеспечивающими работу следственной бригады, каждый сотрудник которой вводит информацию и необходимые связи в БД независимо от работы других членов бригады. Причем данной информацией могут воспользоваться только лица, непосредственно работающие по данному уголовному делу. Это достигается с помощью программных средств защиты от несанкционированного доступа, примененных в системе.

ДК БИНАР позволяет хранить и обрабатывать формализованные символьные данные и текстовые фрагменты с подключением (свободной интеграцией) любого текстового редактора (по желанию пользователя); обладает хорошо развитыми средствами настройки БД.

База данных может произвольно изменяться и расширяться пользователем в пределах 32 различных ОУ, что вполне перекрывает практические потребности следствия. Объем записей (количество реализации) по каждому объекту учета практически неограничен — до 1 млн. символов. При этом количество характеристик (реквизитов) одного ОУ — не менее 150 единиц.

На верхнем уровне управления ходом расследования преступления ДК БИНАР может быть получена обобщенная информация об объектах преступления и связях, выявленных в ходе анализа накопленной в БД информации. Однако для подготовки текстовых документов возможности БИНАРА ограничены из-за пакетного режима их обработки, а необходимость специальных познаний в области функций программирования системы Clipper, как и сама сложность системы в целом, резко снижает ее эффективность при расследовании уголовных дел средней и малой сложности и объема.

Вышеизложенное свидетельствует о том, что специфические условия, в которых осуществляется процесс раскрытия и расследования преступлений, в том числе и компьютерных, обуславливает существенные изменения в организации решения задач с использованием компьютерной техники. Отсутствие на любой стадии предварительного следствия, вплоть до его окончания, достаточно полных и достоверных данных об обстоятельствах, подлежащих обязательному установлению и составляющих, в силу уголовно-процессуального закона, предмет доказывания, требует новых, более гибких подходов при использовании персональных компьютеров в ходе расследования преступлений. Решение задач следствия уже не может быть обычным запуском готового программного продукта, а представляет собой сложную цепь их модификаций и интеграции, связанных с осмыслением задачи в самом процессе расследования, включением в нее дополнительных входных данных, корректировку ранее введенных, что часто приводит к значительным изменениям всей первоначальной структуры логики программного обеспечения. Подчеркнем, что здесь в первую очередь важна не работа по готовому алгоритму, заданному разработчиком программного средства, а динамическое развитие логики самой задачи, требующей своего разрешения в процессе расследования определенной категории уголовных дел, реализуемое в процессе диалога следователя-пользователя с ЭВМ.

По мнению ряда специалистов, например Баранова А.К., Цветкова С.И., подобных результатов можно достичь лишь при создании и использовании в деятельности органов внутренних дел компьютеризированных систем искусственного интеллекта (экспертных систем), представляющих собой автоматизированные информационные системы, которые на основе своих внутренних ресурсов могут приспосабливаться к возникающей внешней ситуации, определять взаимосвязь между различными факторами, характеризующими эту ситуацию, их место и роль в окружающей системе информационной среде и на основе обработки введенной на первоначальном этапе и вводимой пользователем по запросам системы в процессе ее работы информации и данных вырабатывать набор возможных решений поставленной задачи (задач), снабженных интеллектуальным интерфейсом, позволяющим пользователю обращаться к данным на естественном или профессионально-ориентированном языке.

Как свидетельствует анализ специальной литературы, используемые и разрабатываемые в настоящее время в органах внутренних дел программные средства уже сейчас позволяют формулировать рекомендации в сложных ситуациях, возникающих в процессе расследования преступления. Однако эффективность их использования ограничивается огромным объемом информации и данных о криминалистических, уголовно-правовых и уголовно-процессуальных знаниях, нуждающихся в формализации и введении в память указанных систем. С другой стороны, опыт использования таких систем свидетельствует о том, что значительный объем подобной информации о знаниях является универсальным и может быть использован при расследовании различных категорий преступлений, обуславливая в конечном итоге необходимость создания новых информационных систем, основанных не на данных, а на знаниях, на использовании объективно ориентированного подхода и методах обработки информации в любой форме ее представления (в т. ч. и графической).

По нашему мнению, последнее возможно лишь посредством использования новых информационных технологий, составной частью которых является нетрадиционный (поп von Neumann) подход к организации и управлению информационными ресурсами в компьютерных

системах, выраженный в принципе управления потоками данных (знаний) в отличие от управления потоками команд. В данном случае основными орудиями производства информационного продукта являются персональные компьютеры

V и VI поколений (fifth-and sixth-generation computers), характеризующиеся:

- отсутствием использования принципа последовательной передачи управления (счетчиком команд);
- отсутствием реализации концепции переменной (идентификатора);
- использованием в качестве элементной базы сверхбольших интегральных микросхем (СБИС) либо трансфазорных или органических (био-) элементов;
- использованием новых конструкторских решений в архитектуре строения вычислительной среды для реализации принципов искусственного интеллекта;
- возможностью полноценного использования систем виртуальной реальности.

В качестве примера можно привести опыт использования потоковых и редуцированных компьютеров для решения задач правоохранительных органов в зарубежных странах: ФРГ, США, Канаде, Англии, Японии [57, с. 84; 100]. Из указанных литературных источников видно, что ведущие подразделения правоохранительных органов зарубежных стран с начала 90-х гг. начали активно оснащаться указанными компьютерами с соответствующим программным обеспечением, стоимость которого достигает 40 тыс. долл. США (например, программные пакеты проведения автоматической ревизии машинной информации и тестирующих проверок компьютерных систем с целью установления и фиксации фактов потерь финансовых средств). В настоящее время в полиции зарубежных государств широкое распространение получили портативные персональные компьютеры типа Toshiba-5200, ThinkPad, Latitude и Laptop в блокнотном (notebook) и субблокнотном (весом менее 1,5 кг - subnotebook) исполнении.

Основными фирмами-производителями являются: IBM, Compaq, NEC, Del, Toshiba, Motorola, Fujitsu, Olivetti, Vobis Microcomputers, а также фирма Apple, производящая компьютеры типа Macintosh на платформе ОС, совместимой с IBM PC с использованием процессора PowerPC нового поколения [59].

Как показывает анализ специальной литературы, в последние годы исследование проблем искусственного интеллекта становится одним из ведущих направлений в отечественной науке, охватывая при этом самые различные отрасли знаний. Общенаучные основы данной проблемы исследуются в рамках разнообразных междисциплинарных теорий. Тем не менее, объективно оценивая сложившуюся неблагоприятную общественно-политическую и экономическую ситуацию в России (о чем подробно говорилось в первом параграфе первой главы настоящей работы), считаем, что пока рано конкретно вести речь о создании интегрированных сложных экспертных систем (искусственного интеллекта) для нужд органов внутренних дел. Это обусловлено как значительными ресурсными затратами, так и общей профессиональной неподготовленностью сотрудников в этой области знания. Поэтому в настоящее время, с нашей точки зрения, целесообразнее всего говорить, учитывая современное состояние дел и существующую материально-техническую базу органов внутренних дел, о разработке и использовании новых программных средств принятия тактических решений, например следователем в процессе расследования конкретного уголовного дела по типу автоматизированного рабочего места (АРМ).

Особенно перспективным, на наш взгляд, направлением в этом является использование для этих целей программного комплекса FLINT (Formal Language of INteractive Talk), позволяющего пользователю, имеющему минимальные познания, самому создавать необходимые базы данных (БД) и работать с ними без помощи специалистов. Использование FLINT облегчает проектирование на персональных IBM-совместимых компьютерах типа IBM PC/XT/AT автоматизированных рабочих мест как универсального, так и специального назначения и ориентированных на обработку документальной информации анкетного (вопрос-ответ) вида с формированием БД по типу картотеки [96]. Рассмотрим его более подробно.

Практически для любого объекта инструментальное средство (ИС) FLINT позволяет легко и быстро создавать интегрированные БД, функционирующие как в автономном, так и в сетевом режимах, поддерживая их работоспособность за счет более 200 специальных функций, воплощенных в ИС.

Программы FLINT написаны на языке Clipper (Nantucket Corp.) ver. 5.01. Структура информационных файлов (DBF) соответствует стандартному формату AshtonTate для БД реляционного типа, а структура индексных файлов (NTX) при этом соответствует самому формату Clipper. ИС FLINT функционирует в среде операционной системы MS DOS версий 3.30 и выше, которые позволяют пользователю работать в сети через NET BIOS, либо любую другую сетевую среду, разработанную по стандартам DOS, хотя заметим, что основной средой, гарантирующей качественную работу FLINT, является NetWare ver. 2.1 и выше.

В системе предусмотрен и такой немаловажный, по нашему мнению, функциональный блок, как ведение паролей пользователей (программный модуль fl4.exe), предназначенный для разграничения и предотвращения несанкционированного доступа к информации [96, с. 7].

В заключение отметим, что, как видно из вышеприведенного, в настоящее время имеется немало возможностей, способствующих раскрытию компьютерных преступлений. Однако их эффективность зависит от ряда рассмотренных нами объективных и субъективных обстоятельств, из которых на первое место выступает, по нашему мнению, создание в системе правоохранительных органов России общего организационно-методического центра, координирующего всю работу в этом направлении, наделенного соответствующими полномочиями и способного по своему профессиональному составу заниматься всем спектром поднятых нами проблем.

Литература

1. Айламазян А.К, Стась Е.В. Информатика и теория развития. М.: Наука, 1989. С.126.
2. Батурин Ю.М. Проблемы компьютерного права. М.: Юрид. лит., 1991. С. 271.
3. Батурин Ю.М. Право и политика в компьютерном круге. М.: Юрид. лит., 1987. С. 134.
4. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. М.: Юрид. лит., 1991. С. 158.
5. Безруков Н.Н. Введение в компьютерную вирусологию. Общие принципы функционирования, классификация и каталог наиболее распространенных вирусов в MS DOS. Киев: Укр. сов. энцикл., 1989. С. 196.
6. Безруков Н.Н. Компьютерная вирусология: Справочное руководство. Киев: Укр. сов. энцикл., 1991. С. 157.
7. Белкин Р.С., Лузгин И.М. Криминалистика: Учебное пособие. М.: Юрид. лит., 1978. С. 310.
8. Белов В.Н. Правонарушения, связанные с использованием ЭВМ // В кн.: Проблемы совершенствования советского законодательства. Труды ВНИИСЭ. Вып. 5. М., 1976. С. 176-185.
9. Белуха Н.Т. Судебно-бухгалтерская экспертиза. М.: Дело, 1993. С. 270.
10. Борковский А.Б. Англо-русский словарь по программированию и информатике (с толкованиями). М.: Международ. шк. переводчиков, 1992. С. 332.
11. Борьба с компьютерной преступностью в США // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1986. № 4. С. 4-8.
12. Вакурин А.В. О некоторых тенденциях развития криминогенных факторов в финансово-кредитной сфере // В сб.: Актуальные проблемы борьбы с коррупцией и организованной преступностью в сфере экономики. М.: МИ МВД России, 1995. С. 3-9.

13. Виноградов Г.П. Организованная преступность в Тверской области // В сб.; Проблемы борьбы с организованной преступностью. М.: МИ МВД России, 1996. С. 18-23.
14. Вопросы защиты информации // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1987. № 10. С. 9-11. 173
15. Временные санитарные нормы и правила для работников вычислительных центров № 4559-88. М.: Наука, 1988.
16. Выступление Министра внутренних дел Российской Федерации “Об экстренных мерах по усилению борьбы с преступностью и личной безопасности граждан Российской Федерации” на заседании Государственной Думы от 16.11.94 г. // Щит и меч, 1994, № 44.
17. Глистин В.К. Проблемы уголовно-правовой охраны общественных отношений: объект и квалификация преступлений. Л.: ЛГУ, 1979. С. 125.
18. Государственный стандарт (ГОСТ) № 6104-84 от 01.07.87 “УСД. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения”. Постан. Госстандарта № 3549 от 9.10.84. // Бюллет. норм. актов мин. и ведомств СССР. М., 1987.
19. Государственный стандарт (ГОСТ) № 28147-89 “Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования // Бюллет. норм. акт. мин. и ведомств СССР. М., 1989.
20. Гражданский кодекс Российской Федерации (ч. 1 и ч. 2). Волгоград: ВЮИ МВД России, 1995.
21. Гудков П.Б. Компьютерные преступления в сфере экономики // В сб.: Актуальные проблемы борьбы с коррупцией и организованной преступностью в сфере экономики. М.: МИ МВД России, 1995. С. 136-145.
22. Давыдов Э.Г. Исследование операций. М.: Высш. школа, 1990. С. 323.
23. Двойной удар ! // МН Коллекция, 1995. № 2.
24. Довгаль С.И., Литвинов Б.Ю., Сбитнев А.И. Локальные сети и компьютерные вирусы // В кн.: Персональные ЭВМ. Киев, 1993. С. 242-245.
25. Доклад генерального секретаря Организации Объединенных Наций “Воздействие организованной преступной деятельности на общество в целом” // В мат. Комиссии ООН по предупреждению преступности и уголовному правосудию. Вена, 13-23 апр., E/CN. 15/1993/3.
26. Есипов В.М., Пешков А.И. Криминализация внешнеэкономической деятельности // В сб.: Проблемы борьбы с организованной преступностью. М.: МИ МВД России, 1996. С. 79-83.
27. Закон Российской Федерации “О правовой охране программ для электронно-вычислительных машин и баз данных” // Ведом. Верх. Сов. РФ, № 42, 22 окт., 1992, ст. 2325.
28. Закон Российской Федерации “О правовой охране топологий интегральных микросхем” // Ведом. Верх. Сов. РФ, № 42, 22 окт., 1992, ст. 2328.
29. Закон Российской Федерации “О государственной тайне” // Рос. газета, 1993, 21 сент.
30. Закон Российской Федерации “О связи” // Собр. Закон. РФ, № 8, 20 фев., 1995, ст. 600.
31. Закон Российской Федерации “Об информации, информатизации и защите информации” // Собр. Закон. РФ, № 8, 20 фев., 1995, ст. 609.

32. Законодательные меры по борьбе с компьютерной преступностью // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1988. № 10. С. 36-45.
33. Законодательство в борьбе с компьютерными преступлениями // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1989. № 8. С. 23-28
34. Защита информации в базах данных // Иностран. печать о тех. оснащении полиции кап. государств. М.: ВИНТИ, 1992. № 2. С. 15-35.
35. Зуйков Г.Г. Криминалистическое учение о способе совершения преступления; Диссертация на соиск. уч. степени д.ю.н. М.: Академия МВД СССР, 1970. С. 720.
36. Какоткин А. Российские хакеры считают, что Левина подставили // Известия, 1995. № 176. С. 5.
37. Карась И.З. Вопросы правового обеспечения информатики // Микропроцессорные средства и системы, 1986. № 1. С. 3-17.
38. Карась И.З. Экономический и правовой режим информационных ресурсов // В кн.: Право и информатика. М.: МГУ, 1990. С.40-59.
39. Касперский Е. Компьютерные вирусы в MS-DOS. М.: "ЭДЭЛЬ" — "Ренессанс", 1992. С. 174.
40. Кашеев В.И. Специальная техника контроля и защиты информации // Системы безопасности. М.: "Гротек", 1995. № 1. С. 51-73.
41. Кириченко А. Вирусы научились размножаться по своим законам // МН Коллекция, 1995. № 2.
42. Козлов С.Б., Иванов Е.В. Предпринимательство и безопасность. М.: Универсум, 1991. С. 480.
43. Колдин В.Я., Полевой Н.С. Информационные процессы и структуры в криминалистике: Учебное пособие. М.: МГУ, 1985. С. 132.
44. Компьютерная "фомка" // Комсомольская правда, 1994. № 82.
45. Компьютерная преступность в Великобритании // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1990. № 8. С. 14-15.
46. Компьютерная преступность в США // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1990. № 9. С. 3-5; 1987. № 9. С. 3-5,
47. Компьютерная преступность в ФРГ // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1987. № 6. С. 10-13.
48. Компьютерная преступность в Швейцарии: формы проявления и характеристика преступников // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1987. № 9. С.5-10.
49. Компьютерные преступления в Великобритании // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1988. № 3. С. 18-20.
50. Компьютерные преступления и методы борьбы с ними // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1985. № 1. С. 3-7.
51. Компьютерные преступления и обеспечение безопасности ЭВМ // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1983. № 6. С. 3-6.
52. Компьютерные технологии в юридической деятельности: Учебное и практическое пособие Под ред. Полевого Н.С. М.: БЕК, 1994. С. 301.

53. Коржанский Н.И. Объект и предмет уголовно-правовой охраны. М.: Академия МВД СССР, 1980. С. 248.
54. Косоплечев Н.П., Григорян В.А., Федулов И.В. Система мер предупреждения преступности. М.: ВНИИ укрепления законности и правопорядка, 1988. С.128.
55. Кравченко В. Как защитить телефон от подслушивания // ,МН Коллекция, 1995. № 2.
56. Лучин И.Н., Желдаков А.А., Кузнецов Н.А. Взламывание парольной защиты методом интеллектуального перебора // Информатизация правоохранительных систем. М.: Академия МВД России, 1996. С. 287-288.
57. Меры по защите от экономических преступлений // Борьба с преступностью за рубежом. М.: ВИНТИ, 1991. № 1 С. 51-53.
58. Меры по защите программного обеспечения в странах ЕЭС // Борьба с преступностью за рубежом. М.: ВИНТИ, 1992. № 8. С. 18-19.
59. Мир в ожидании Apple-совместимых ПК // Business MN, 1994. № 41.
60. Мосесов А., Блинов Ф. Понедельник. День тяжелый // Неделя,1994.№ 48.
61. Мошенники “засветились” на дисплее // Комсомольская правда,1994.№ 74.
62. Мячев А.А., Степанов В.Н., Щербо В.К. Интерфейсы систем обработки данных: Справочник / Под ред. А.А. Мячева. М.: Радио и связь, 1989. С. 245.
63. Некоторые аспекты компьютерной преступности // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1990. № 6. С. 12-13.
64. Некоторые правовые аспекты защиты и использования сведений, накапливаемых в информационных системах // Борьба с преступностью за рубежом. М.: ВИНТИ, 1990. № 7. С. 63-64; 1992. № 6. С. 13-14.
65. Овчинский В.С. Стратегия борьбы с мафией. М.: “СИМС”, 1993. С. 158.
66. О законе против “хэккеров” // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1990. № 7. С. 62-63.
67. Пантелеев И.Ф., Селиванов Н.А. Криминалистика: Учебник. М.: Юрид. лит., 1993. С. 591.
68. Першиков В.И., Савинков В.М. Толковый словарь по информатике. М.: Фин. и стат., 1991. С. 536.
69. Подпольная банковская система // Борьба с преступностью за рубежом. М.: ВИНТИ, 1992. № 8. С. 3-9.
70. Полевой Н.С. Криминалистическая кибернетика: Теория и практика математизации и автоматизации информационных процессов и систем в криминалистике: Учебное пособие. М.: МГУ, 1989. С. 324.
71. Полевой Н.С. и др. Правовая информатика и кибернетика: Учебник. М.: Юрид. лит., 1993. С. 527.
72. Постановление Правительства Российской Федерации, № 608 от 26.06.95 “О сертификации средств защиты информации” (Положение) // Собр. Закон. РФ № , июля, 1995, ст. .
73. Постановление Госстандарта № 2781 от 24.09.86 “Методические указания по внедрению и применению ГОСТ 6104-84” // Бюллет. норм акт. мин. и ведомств СССР. М., 1987. № 7.

74. Предотвращение компьютерных преступлений // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1986. № 4. С.5-9.
75. Преступления против офисов // Борьба с преступностью за рубежом. М.: ВИНТИ, 1991, № 10. С. 16-18.
76. Преступность в кредитно-финансовой сфере ФРГ // Борьба с преступностью за рубежом. М.: ВИНТИ, 1992. № 7. С. 8-10.
77. Применение интеллектуальных карточек для шифрования данных и формирования электронных подписей // Иностран. печать о тех. оснащении полиции кап. государств. М.: ВИНТИ, 1991. № 12. С. 33-37.
78. Проблемы безопасности ЭВМ // Иностран. печать о тех. оснащении полиции кап. государств. М.: ВИНТИ, 1990. № 11. С. 90—101.
79. Проблемы борьбы с компьютерной преступностью // Борьба с преступностью за рубежом. М.: ВИНТИ, 1992. № 4. С. 3-10.
80. Различные аспекты компьютерной преступности // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1987. № 3. С. 16-19.
81. Расследование в Великобритании преступлений, совершаемых с использованием компьютеров // Борьба с преступностью за рубежом. М.: ВИНТИ, 1993. № 8. С. 9-13.
82. Расширение масштабов компьютерной преступности // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1986. № 10. С. 9-11.
83. Румянцев А. Банкоматный вор работал под колпаком // Известия, 1995. № 235. С. 5
84. Рыжков А.А. Вопросы защиты информации от ее негласного снятия по виброакустическому каналу // В сб.: Информатизация правоохранительных систем. М.: Академия МВД России, 1996. С. 315-317.
85. Савельева И.В. Правовая охрана программного обеспечения ЭВМ // В кн.: Право и информатика. М.: МГУ, 1990. С. 9-24.
86. Селиванов Н.А. Проблемы борьбы с компьютерной преступностью // Законность, 1993. № 8. С. 36-40.
87. Симаков В.В., Балакирев С.В. Многоканальный цифровой комплекс регистрации и обработки аудиоинформации // В сб.: Информатизация правоохранительных систем. М.: Академия МВД России, 1996. С. 76-78.
88. Совещание по вопросам компьютерной преступности // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1986. № 11. С. 36-40.
89. Спесивцев А.В., Вегнер В.А., Крутяков А.О., Серегин В.В., Сидоров В.А. Защита информации в персональных ЭВМ. М.: Радио и связь, 1992. С. 188.
90. Стоит ли злоупотреблять разговорами // МН Коллекция, 1994. дек.
91. Уголовно-процессуальный кодекс РСФСР (с измен. и доп. по состоянию на 01.02.95 г. М.: Контракт, 1995. С. 219.
92. Уголовный кодекс Российской Федерации // Рос. газета, 1996. № 118, 25 июня.

93. Указ Президента Российской Федерации № 334 от 03.04.95 г. “О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации” // Собр. Закон. РФ, № 15, 10 апреля, 1995. ст. 1285.
94. Федоров В. Компьютерные преступления: выявление, расследование и профилактика // Законность, 1994. № 6. С.44-47.
95. Фигурнов В.Э. IBM PC для пользователя. М.: фин. и стат., 1994. С. 250.
96. Формальный язык интерактивного общения (FLINT). М.: “ТАИС”, 1993. С. 205.
97. Хананашвили М.М. Информационные неврозы. М.: Медицина, 1986. С. 290.
98. Цуприков С. Новый этап автоматизации банков Московского региона // ComputerWorld, М., 1993. № 28.
99. Черкасов В.Н. Теория и практика решения организационно-методических проблем борьбы с экономической преступностью в условиях применения компьютерных технологий. М., 1994.
100. Черкасов В.Н. О понятии “компьютерная преступность” // Проблемы компьютерной преступности. Минск: НИИПКК СЭ, 1992. С. 26-34.
101. Чугуев А.Д., Захарин С.И. Вирусный бизнес криминальной среды как социальная база для развития преступной деятельности по созданию вирусов // В сб.: Подготовка специалистов в условиях изменяющейся структуры преступности и обновляющегося законодательства России. Волгоград: ВСШ МВД РФ, 1994. С.169-171.
102. Шальнев А. Наша мафия — самая компьютеризированная в мире // Известия, 1995. 15 фев.
103. Шаповалов А. ФБР вызывали? // Рос. газета, 1995. 29 апр.
104. Шрейдер Ю.А. Социальные аспекты информатики // НТИ, сер. 2. М.: Наука, 1989. № 1. С. 3-14.
105. Экономическая преступность в ФРГ и Швейцарии // Проблемы преступности в капиталистических странах. М.: ВИНТИ, 1987. № 4. С. 3-10.
106. Яблоков Н.П., Колдин В.Я. Криминалистика: Учебник. М.: МГУ, 1990,