**Предложения в аналитическую записку и практические рекомендации по результатам обобщения материалов о хищениях денежных средств с использованием компьютерной техники, кредитных карточек и подложных платежных документов.**

Анализ деятельности аппаратов БЭП СКМ за 2001–2002 г.г. и криминогенной ситуации с противоправным использованием компьютерной техники показывает, что преступления в сфере компьютерной информации приобретают все более организованный, групповой и транснациональный характер. Сегодня преступник, используя персональный компьютер и телекоммуникационную, сеть может совершить хищение десятков миллионов долларов, не выходя из офиса банка или квартиры, либо используя компьютерную систему, находящуюся на территории другого государства.

С увеличением числа компьютеров количество преступлений с их использованием стремительно растет. Если за 1997 год было выявлено лишь 30 преступлений, предусмотренных ст. ст. 272-274 УК РФ, в 2000 году – 800, за весь 2001 год – 1650, то лишь за первое полугодие 2002 годы выявлено свыше 800 преступлений.

Правоохранительные органы Российской Федерации активно участвуют в международном сотрудничестве по борьбе с компьютерными преступлениями экономической направленности. В соответствии с последними соглашениями государств «восьмерки», подписанными в США, в каждой из ее стран созданы национальные координирующие центры (в Германии это БКА, в США – ФБР, в России - на базе МВД). Основной задачей центров является выполнение совместных мероприятий по срочному перехвату электронных данных и взаимный обмен этой информацией. Кроме того, еще с 2000 года между странами – членами СНГ действует «Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации», что, в частности, позволило в 2001-2002 г.г. выявить и расследовать ряд хищений валютыс использованием компьютерной техники в сумме свыше 97 млн. долларов США.

**1. Характеристика преступлений в сфере компьютерной информации. Хищения денежных средств с использованием компьютерной техники.**

Зачастую компьютерное преступление предполагает атаку на компьютер, как объект несанкционированного, противоправного доступа. Практика органов внутренних дел показывает, что в основном это связано с получением компьютерной информации, либо с использованием системы компьютеров для хищений товаров и услуг. Статистика ГИЦ МВД РФ о выявлении преступлений экономической направленности за 2001-2002 г.г. свидетельствует, чтобольшинство преступлений этого вида связано с несанкционированным доступом к компьютерным системам.

Как правило компьютерная техника используется для получения преступником несанкционированного доступа к компьютерной системе предприятия (фирмы), чтобы воспользоваться предоставляемыми ею услугами бесплатно, либо получать денежные средства за эти услуги через других лиц. Например, в Москве в 2001-2002 г.г. группы преступников использовали свою компьютерную технику, чтобы проникать в международную коммутационную систему, в т.ч. в фирменные АТС с выходом на городскую и междугородную сеть, для того, чтобы незаконно воспользоваться услугами по предоставлению международной телефонной связи. Такого рода преступления, с ущербом в сотни тысяч рублей, выявлялись неоднократно УБЭП СКМ ГУВД г. Москвы. В большинстве случаев лицами, совершающими указанные преступления, являлись иностранные Вьетнама и Китая, в т.ч. проживающие в столице без регистрации.

**2. Противоправное завладение компьютерными информационными ресурсами для совершения иных преступлений.**

2.1. Объектом компьютерного преступления зачастую являлась секретная информация, хранящаяся на жестких дисках компьютеров МВД, ФСНП, ГТК, ФСБ РФ и других правоохранительных, либо фискальных органов. Эта информация является очень привлекательным объектом для преступников в отношении которых ведется расследование по уголовным делам, в т.ч. членов организованных преступных групп.

2.2. Бизнес-фирмы являются мишенью для овладения их секретами, хранящимися в ведомственных компьютерах. Интерес проявлялся, прежде всего к экономически важной информации. Так, в 2002 г. в Поволжском регионе возбуждено уголовное дело в отношении троих преступников, которые с помощью компьютера получили программный продукт, информацию о счетах клиентуры фирмы, их компьютерные данные и сами организовали фирму по электронному обслуживанию, чем нанесли собственнику суммарный ущерб в 152 000 рублей.

2.3. В другом, аналогичном случае, компьютерный взломщик похитил производственную информацию, являющуюся также собственностью фирмы, на сумму свыше 1 млн. долларов США, для создания частной телефонной фирмы.

2.4. В третьем случае преступник получил доступ к системе бронирования номеров в гостинице VIP-класса в г. Москве с целью получения номеров кредитных карточек иностранцев, их последующей подделки и хищения денежных средств.

**3. Компьютерная техника как орудие мошенников.**

3.1. Наиболее часто мошенничества с использованием компьютерного обмена в режиме онлайн (реального времени**)** включали в себя мошенничества с предоплатой поставки товаров от вымышленных фирм. Поддавшись на рекламу в средствах массовой информации или Интернет-магазинах и низкие (относительно) цены, пострадавшие переводили деньги и только после этого обнаруживали, что товаров нет, либо они низкого качества и бракованные. Удобной средой для мошенничества стало использование сетевой торговли в Интернете. Нередко предложения для оплаты направлялись без разбора **сотням участников** интернет-общения по электронным почтовым адресам.

3.2. Выявлены факты, когда преступники использовали компьютеры для того, чтобы совершать крупные денежные хищения. Например, создание финансовых пирамид, псевдоперевод «крупных партий товаров», взлом сети и реальное перечисление многомиллионных сумм **с** банковских счетов с последующей «обналичкой» и хищением денег.

3.3. В России широкое распространение получают мошеннические действия с использованием компьютерной техники для создания азартных игр, лотерей, спортивных тотализаторов и онлайновых казино. Для мошенников здесь имеются самые широкие возможности. При этом для расчетов используются кредитные карточки, что только способствует расширению системы компьютерных хищений: от отказа выплаты выигрыша, до всевозможных «лохотронных разводок» игроков на крупные суммы.

3.4.Особо необходимо отметить, что сегодня электронная компьютерная почта используются организованными преступными сообществами для координации или планирования опасных преступлений любого вида (вымогательство, угрозы совершения терракта и т.п.).

1. **Повреждение компьютеров и компьютерных сетей.**

4.1. Как правило, преступления подобного рода совершались бывшими, по их мнению, несправедливо уволенными сотрудниками фирм, коммерческих банков, которые таким образом пытались отомстить. Они предпринимали попытки внести в компьютеры вирус, изменить каким-либо образом информацию (файлы), иные компьютерные данные, являющиеся важными для банка (фирмы). Несанкционированный доступ такого рода иногда наносил ущерб в сотнитысяч рублей.

4.2. При этом можно выделить два основных типа компьютерных повреждений на расстоянии: в первом случае с несанкционированным проникновением преступник использует пробелы в системе безопасности банка (фирмы) в качестве средства доступа к коммерческой информации. В этом случае он похищает ее или уничтожает. Во втором случае преступник, даже не имея доступа, повреждает (уничтожает) компьютерную систему путем засылки огромных объемов электронной информации. В третьих, это обычное блокирование телефонных линий банка (компании), либо использование низкоуровневых протоколов передачи данных, что также приводит систему в непригодное состояние.

**5. Основные итоги работы органов внутренних дел по выявлению преступлений с использованием компьютерной техники.**

Анализ результатовработы органов внутренних за 9 месяцев 2002 года, а также аналогичного периода прошлого года (АППГ) позволяет сделать вывод, что положение дел с выявлением и расследованием хищений денежных средств с использованием компьютерной техники, кредитных карт и платежных документов в течение последних лет довольно стабильно, а результаты работы по линии БЭП улучшились.

Так, за первое полугодие 2002 года подразделениями СКМ выявлено 805 преступлений, совершенных в сфере компьютерной информации, т.е. преступлений, предусмотренных статьями главы 28 УК РФ или 0,32 % от общего количества преступлений экономической направленности, выявленных ОВД. В то же время за 1 полугодие 2001 г. было выявлено 445 фактов, т.е. в этом году налицо рост на 45,7 % по сравнению с АППГ.

В числе преступлений: нарушение правил эксплуатации компьютеров, систем или их сетей (ст. 274 УК РФ), создание, использование и распространение вредоносных компьютерных программ, заведомо проводящих к несанкционированному уничтожению, блокированию, модификации и копированию, использование вредоносных программ (ст. 273 УК РФ). Таких преступлений выявлено свыше ста. Кроме того были выявлены хищения, совершенные с использованием компьютерных технологий, организованными группами в особо крупном размере.

Можно привести пример типичного хищения денежных средств с использованием компьютерной техники, выявленного в сентябре 2002 года, когда компьютерным взломщиком - программистом Центрального банка Туркмении А. Какаевым в целях хищения было переведено 20 млн. долларов США в московский АКБ «Русский депозитный банк».

Преступник воспользовался тем, что имел непосредственный доступ к банковской компьютерной системе международных платежей«Свифт».В целях хищения А. Какаев взломал банковские коды и введя четыре электронные подписи руководителей банка РТ, в течение 2002 г. неоднократно переводил крупные суммы инвалюты на заранее открытые в зарубежных банках счета, в том числе в Россию, на общую сумму 40 млн. долларов США.

Подобным способом им было переведено 1 млн. 250 тыс. долларов США в отделение банка «НSBS» в Гонконге; свыше 18,7 млн. долларов США в «Парексбанк» в г. Риге (Латвия). Рекордная для этого уголовного дела сумма - 20,0 млн. долларов из «Русского депозитного банка» была в тот же день (3.09.2002 г.) переведена на расчетный счет клиента этого банка – фирмы «Сванситигруппбанк». Обращает внимание, что А. Какаев совершил хищение в составе хорошо организованной преступной группировки. В частности ее члены осуществили получение не только кодированных, электронных подписей руководства Центробанка Туркмении, но и организовали сопровождение валютных трансакций всеми необходимыми сопроводительными электронными документами.

Вся валюта похищена после обналичивания через подставных лиц в иностранных банках. О хорошем владении компьютерными технологиями и тщательной подготовке преступления свидетельствует то, что о факте перевода 20 млн. долларов США в Россию руководством АКБ «Русский депозитный банк» было своевременно сообщено Комитету по финансовому мониторингу РФ, однако специалисты финансовой разведки посчитали эту операцию вне подозрений.

За 8 месяцев т.г. было выявлено уже 920 преступлений данной категории (1,1% от общего количества преступлений экономической направленности, выявленных СКМ), в том числе шесть преступлений, совершенных группами или преступными сообществами. От общего числа уголовных дел по ст. ст. 273, 274 УК РФ за первое полугодие в суд было направлено 55 дел или 15,6% от числа оконченных производством. За АППГ направлено 459 дел или 68,6% .

В 2002 году наибольшее число преступлений экономической направленности, совершенных с использованием компьютерной техники, было связано с неправомерным доступом к охраняемой законом компьютерной информации, то есть информации на магнитных носителях, серверах и т.д. Подобные деяния зачастую влекли уничтожение, блокирование, модификацию, либо негласное противоправное копирование ее в корыстных целях.

Таких преступлений было совершено 87,5% от общего числа выявленных подразделениями криминальной милиции (за АППГ – 70,4%). В частности, оперативными сотрудниками БЭП СКМ было изъято контрафактной продукции, в т.ч. различного типа магнитных носителей с программным компьютерным обеспечением на сумму 418,6 млн. рублей (в 2001 году – 167,4 млн. рублей).

Только за 3 квартал 2002 года 9 отделом УБЭП СКМ ГУВД г. Москвы в столице выявлено семь подпольных цехов по выпуску контрафактных компьютерных дисков с программным продуктом. Лишь в одном случае, в ноябре с.г. в цехе на Пятницком шоссе, замаскированном под магазин по торговле видеокассетами было изъято 10 000 контрафактных CD-rom. Поставка дисков шла из Украины и стран Юго-Восточной Азии. Их упаковку и поставку в 10 торговых точек г. Москвы осуществляли трое наемных рабочих из Украины.

По 570 уголовным делам указанной категории (81,3%) лица, их совершившие, были установлены. По одному делу по ст. 272 УК РФ ущерб, причиненный потерпевшим владельцам компьютерной информации, превысил крупный размер (свыше 50 000 рублей).

Так, по материалам УБЭП СКМ ГУВДСамарскойобласти в апреле 2002 года прокуратурой Октябрьского района г. Самары было возбуждено уголовное дело по признакам ч. 2 ст. 272 УК РФ за неправомерный доступ к компьютерной информации, совершенный группой лиц, по предварительному сговору, которые имели доступ к внутрифирменной системе компьютеров.

Предварительной проверкой, проведенной закрытым акционерным обществом «Институт информации» Самарского регионального центра правовой охраны программ для ЭВМ, баз данных и топологий интегральных микросхем, было установлено, что бывшие сотрудники ООО «Бюро электронной почтовой доставки» М, Б и К похитили и незаконно используют в коммерческих целях компьютерную базу данных ООО. Похитители нарушили тем самым не только авторское право, но и право собственности двух фирм: «Бюро электронной доставки» и ТОО «Деловые партнеры «Компрэл», базы данных которых были с 25.05.1998 года официально зарегистрированы в Роспатенте Российской Федерации.

Указанными лицами с помощью дискет типа «Verbatim Detal Laif Plus», была похищена база данных клиентуры для рассылки корреспонденции и сведения о доставочных ведомостях. Ранее обвиняемые работали в указанных фирмах программистом, менеджером и главным бухгалтером соответственно, имея доступ к базам данных. Фактами противоправного использования компьютерных данных причинен материальный ущерб ООО «Бюро электронной доставки» на сумму свыше 660 тыс. рублей, а ТОО «Компрэл» – около 880 тыс. рублей.

За истекший период 2002 года в 296 случаях или 49,9% от числа оконченных производством по ст. 272 УК РФ уголовные дела были направлены в суд. Из направленных дел в 8,4% случаях (2001 – 7,9%) преступления были совершены в составе групп, в том числе организованными группами было совершено четыре преступления (за 8 мес. т.г. – шесть преступлений).

По экономическим преступлениям с использованием компьютерной техники выявлено 179 лиц из них 163 человека (91,0%) совершившие неправомерный доступ к компьютерной информации. При этом 32 человека (19,6%) было привлечено к уголовной ответственности реально (за АППГ – 37) из них четыре человека совершили это преступление в группе. Почти все проходившие по указанным уголовным делам в качестве обвиняемых являлись служащими, в том числе трое - работниками кредитно-финансовой и банковской систем, а 22 (68,7%) сотрудники частных фирм, либо частные предприниматели.

**6. Хищения денежных средств с использованием кредитных карт и иных расчетных документов.**

Из анализа криминогенной ситуации видно, что преступность в сфере использования пластиковых кредитных карт растет параллельно с развитием процессинговых и банковских систем. Одним из показателей уровня преступности является отношение потерь к объему финансового оборота в этой сфере. В 2002 году в России этот уровень вплотную приблизился к 0,9-1,0%. Банковские и расчетные системы вынуждены постоянно совершенствовать и внедрять новейшие технологии защиты. Однако разрозненные шаги, в т.ч. без участия специалистов ФАПСИ, МВД, других правоохранительных органов России не могут привести к желаемому результату.

В текущем и 2003 году перед аппаратами БЭП СКМ стоит задача решить эти проблемы комплексно, во взаимодействии с эмитентами карт, на уровне современной компьютерной техники. Поскольку в результате преступлений, совершаемых с использованием кредитных и дебетовых пластиковых карточек, причиняется значительный ущерб не только субъектам предпринимательской и финансовой деятельности (расчетным системам, банкам, гостиницам, объектам торговли и другим участникам сделок), но и экономике России в целом.

Необходимо иметь в виду опыт Германии, Франции и Великобритании где такие мошенничества приводят к хищению ежегодно сотен миллионов евро и фунтов стерлингов. Так крупнейшая международная процессинговая система «VISA» (годовой объем 300 млн. операций) терпит за счет несанкционированного использования ее кредитных карт и дорожных чеков убытки в пределах 2 - 3-х млрд. долларов (в 2001-2002 г.г. около 1,8 - 2,0% годового оборота).

Только крупнейшие торговые фирмы США оценивали стоимость злоупотреблений с кредитными карточками в миллиард долларов ежегодно, а по оценкам 2002 года до 2,4 миллиарда долларов. Уже с середины 90-х годов недобросовестное использование пластиковых карточек только в торговле, гостиничном и туристическом сервисе влекло за собой ежегодный ущерб свыше полумиллиарда долларов, не учитывая мошенничеств, связанных с использованием банкоматов.

Ущерб от злоупотреблений с кредитными картами несут и российские банки. Только в системах КБ Альфабанк и Интуркредит ежегодно признаются недействительными более 90 тыс. сделок. Ущерб составляет около 3,5 млн.долларов. Практика аппаратов БЭП ГУВД г. Москвы показывает, что подобное млн. мошенническое завладение чужим имуществом происходит от 50 до 100 раз в неделю. По сведениям оперативного характера ГУБЭП МВД РФ в течение 2002 года только в Москве ежемесячно подделывается до нескольких сотен единиц кредитных карт международных процессинговых систем MasterCard, Visa, Амerican Express, Diner & Club и некоторых банков - эмитентов. По оценкам консалтинговой корпорации «Europay» в 2002 году, в целом по странам Европейского союза, финансовый ущерб от мошеннических операций с поддельными картами и подложными платежными документами превысит 2 млрд. евро.

Приказом МВД РФ № 730-1997 г. борьба с тяжкими преступлениями в кредитно-финансовой системе определена как приоритетное направление деятельности подразделений БЭП. Вместе с тем, отмеченные аспекты преступлений экономической направленности с использованием кредитных карт, иных подложных платежных документов, деятельность по их выявлению, раскрытию и предупреждению являются недостаточно изученными, имеется еще недостаточное количество методических рекомендаций, чем и обусловлена подготовка данных предложений.

**7. Основные способы совершения мошенничества при расчетах кредитными картами и иными платежными документами.**

В настоящее время преступления, связанные с кредитными картами условно можно разделить на три группы: незаконное использование поддельных кредитных карточек; мошенническое использование платежных квитанций и поддельных кредитных карточек. В первую группу входят преступления, при совершении которых злоумышленники не подвергают платежное средство (кредитные карточки) каким-либо изменениям и фальсификациям.

Среди преступлений этой группы можно выделить следующие разновидности: использование или попытка использования карточки на чужое имя; противоправное использование карточки ее законным держателем. К этой же разновидности относятся факты использования потерянной карточки ее законным владельцем. Распространены случаи, когда преступники похищают и пользуются ими как законные держатели. Где это необходимо, применяется код доступа к счету владельца, а также похищенные паспорта.

Кражи карт могут быть совершены при пересылке карточек компанией их владельцам по почте. В этом случае имеется большая вероятность для злоупотреблений, т.к. ни отправитель, ни получатель не знают о пропаже кредитных карточек. Кражи совершаются также у законных владельцев как на территории страны, так и за рубежом карманными ворами, лицами из числа обслуживающего персонала гостиниц и других категорий.

Потерянные или украденные карточки в дальнейшем используются для получения товаров и услуг в предприятиях, осуществляющих расчеты по кредитным карточкам, лично, через подставных лиц, либо в сговоре с работниками гостиниц и торговых предприятий. При этом подделывается подпись владельца карточки на счетах, либо изготавливаются и предъявляются фальшивые паспорта на имя владельца карточки. Выявлен ряд фактов, когда после покупки дорогостоящего изделия карточка подбрасывалась сотрудницами гостиниц законному владельцу. Кроме того теперь и в России кредитные (дебетовые) карточки широко используются для получения наличных денег в банкоматах, естественно при условии знания личного кода держателя кредитной карточки.

7.1. Хищение денежных средств с использованием кредитных карточек ее законным владельцемсовершается двумя путями: в первом случае владелец, зная о наличии на своем счете определенной суммы валютных средств, путем злоупотребления доверием получает значительно большую сумму, превышающую лимиты кредитования. Так, в 2001 году турист - гражданин Германии К, имея на личном счете менее 4,0 тыс. долларов США, в результате технической ошибки обслуживающего персонала похитил в российском банке по кредитной карточке около 96 тыс. долларов США.

Этому хищению способствовало то, что согласно банковских правил, существующих в Германии, клиент может снимать деньги по кредитным карточкам выше установленного лимита с последующим внесением этой суммы на счет в банке. Однако данный гражданин получил крупные суммы (суммарно около 96 тыс. долларов США), которые по всем стандартам существенно выше норм выдачи наличных по кредитным картам. Поэтому, если бы банк получил запросы о полной сумме, в авторизации было бы отказано вследствие превышения суммы лимита кредитования, установленного владельцу карточки.

7.2. Зарегистрирован и такой способ незаконного использования кредитных карточек, при котором иностранец вступает в сговор с гражданином России и передает ему добровольно в пользование кредитную карточку. Срок использования оговорен заранее, в основном он совпадает со временем пребывания интуриста на территории страны. Обычно владелец кредитной карточки после выезда из России заявляет об ее утрате. Процесс ее использования гражданином России предполагает либо подделку документов, удостоверяющих его личность, либо предварительную подпись иностранцем копий счетов.

7.3. К этой группе злоупотреблений тесно примыкают хищения денежных средств, связанные с мошенническим использованием счетов (слипов). При этом возможны следующие варианты:

- с забытых в ресторанах, гостиницах и т.п. карт работниками предприятий снимаются слипы, в которых подделывается подпись и в дальнейшем они используются для незаконного получения товаров и услуг на своем предприятии; изготовленные аналогичным образом чеки сбываются иным лицам, которые предъявляют их в другие предприятия;

- с кредитной карточкой без ведома ее владельца снимается не один экземпляр оттисков (слипов), а несколько, по которым незаконно получаются товары и услуги. Такие действия совершаются, как правило, в ресторанах.

- используются полностью и частично подделанные кредитные карты. В этой группе можно выделить пластиковые карты, в которые внесены подлоги, переделанные кредитные карточки, а также полностью поддельные кредитные карточки. При этом использование кредитных карточек, в которые внесены подлоги, несколько проще.

7.4. В 2001-2002 г.г. в России выявлены факты относительно нового способа мошеннического хищения денежных средств и товаров посредством краж (либоввоза импортных)импринтеров (прокатных устройств), при помощи которых изготавливаются поддельные слипы, предъявляемые в дальнейшем для отоваривания.

7.5.Другую разновидность образуют преступления, при совершении которых у законных владельцев похищаются эти платежные средства и в их реквизиты (номер, имя и фамилия владельца, его подпись, цифровой код на магнитной полосе) вносятся новые данные. Они берутся с контрактов между фирмами, со счетов, копировальной бумаги от счетов и т.п. Изменения в кредитные карточки вносят также путем срезания букв и цифр, впечатанных в плоскость карточки и приклеивания других. Кроме того, преступники имеют машинки с набором букв и цифр, с помощью которых они вдавливают их в пластмассу.

7.6.Способ использования полностью подделанных кредитных карточек сложнее. Поскольку подделка дорога, эту форму используют организованные группировки. Одной из форм подделки является применение чистой пластмассы установленных форм и размеров, ввозимых, как правило из-за рубежа - т.н. «White Plastic Crime» - «Белый пластик». В этом случае на этот пластик наносятся действительные данные (магнитная полоса, номер карточки, срок действия, фамилия и т.д.). Полностью поддельные кредитные карточки изготовляются сегодня не только за рубежом, но и в России и странах ближнего зарубежья. В частности в 2002 году были выявлены факты массового ввоза в Россию заготовок пластиковых карточек для их дальнейшей подделки из Украины.

7.7. В 2002 году выявлены факты, когда в магазинах или ресторанах продавцы и официанты, используя мини-устройство, носимое ими на поясе, либо пользуясь нетрезвым состоянием клиента, прокатывают с кредитной карточки счета нужное количество раз, а клиент расписывается только на одном счете. Если сумма небольшая, то в кассу вкладываются деньги, а счет с подписью изымается. Далее счет используется для более точного воспроизведения подписи законного держателя кредитной карточки на других счетах, прокатанных без ведома владельца.

7.8. Сходный способ применяется при предъявлении похищенной кредитной карточки, когда кассир совместно с соучастниками на импринторе магазина прокатывает большое количество счетов, которые затем используются для изъятия товаров или валюты, как в этом магазине, так и в других по сговору с их работниками.

# Так, например, мошенническим использованием кредитных карт, в течение 2002 года, крупное хищение денежных средств совершила сотрудница московского «Академхимбанка», которая списывала тысячи рублей со счетов клиентуры с помощью пластиковых карт. Как установлено ОБЭП УВД Западного округа г. Москвы, 24-летняя кассирша Ф. более двух лет была занята выдачей наличных денег в обменном пункте, расположенном в гостинице «Салют».

# Периодически она умышленно отключала автоматику и прокатывая кредитные карты через оборудование, выписывала чеки вручную. Кроме того она могла вносить данные кредиток в компьютер также вручную. По инструкции в этих случаях она записывала информацию о клиентах в специальный регистрационный журнал, предназначенный лишь для служебного использования. Этим Ф. и решила воспользоваться для хищения денежных средств.

Как правило, в качестве потенциальных жертв она использовала иностранных туристов и бизнесменов. От их имени Ф. неоднократно снимала со счетов банка крупные суммы. Деньги после снятия с депонентов мошенница похищала. Только в течение последних нескольких месяцев 2002 года мошенница успела похитить более 83 000 руб. Только с помощью службы собственной безопасности банка сотрудникам ОБЭП удалось задокументировать факты неоднократных хищений с использованием компьютера и кредитных карт.

7.9. По степени организованности и механизму совершения указанные преступления можно классифицировать на преступления, совершенные одиночками и неорганизованными преступными группам, либо совершаемые организованными группами. Первая группа преступлений может быть систематизирована по такому признаку как национальность. Здесь можно выделить два направления - преступления, совершенные российскими гражданами и иностранцами.

Преступления, совершаемые российскими гражданами, можно охарактеризовать как непрофессиональные. Эти лица, в основном, действуют по схемам: кража карточки с последующей перепродажей, либо ее «прокатка» с последующим присвоением товаров (услуг). Подделка подписей, документов осуществляется ими примитивно.

Преступления, совершаемые иностранными гражданами, можно разделить на два вида: первые совершают иностранцы - бывшие граждане России. Выехав за рубеж и освоив систему расчетов кредитными карточками, они выявляют в ней уязвимые места (сейчас более характерные для России). По новому месту жительства за границей они делали заявление о потере карточки, а приехав в Россию, предъявляли ее для оплаты. Нередко они использовали украденные карты. Следует отметить, что процент таких преступлений небольшой.

Граждане других национальностей (вьетнамцы, китайцы) образующие организованные, но относительно небольшие группы состоят из лиц, получивших незаконным образом кредитные карты. В дальнейшем такие лица также стремятся вовлечь в свою преступную деятельность работников гостиниц или торговли. Применяемые для этого способы различны: от угрозы применения насилия к кассирам или их родственникам, до использования корыстной заинтересованности. Количественный состав таких групп два-четыре человека. Порой группы состоят только из работников торговых предприятий. Такими группами совершается наибольшее число преступлений (до 40,0 %.).

Наоборот участники ОПГ, как правило, отличаются хорошим знанием системы расчетов и обслуживания по кредитным картам, высоким профессионализмом совершения преступлений. Здесь также наблюдается распределение ролей и обязанностей: одни специализируются на краже карточек, другие на подделке, сбыте, снятии денег и т.д.

Организационные формы объединения лиц, совершающих хищения денежных средств и иные преступления экономической направленности с использованием поддельных карт и иных подложных документов, условно можно классифицировать на два направления:

- российские организованные преступные группировки и организации;

- международные организованные группы.

Среди последних, кроме распределения ролей и обязанностей, распределены также и места совершения определенных действий. Например, кража или подделка карточек совершается в Германии или на Украине, а предъявление к оплате производится в России, либо наоборот.

8. Хищение денежных средств с использованием подложных платежных документов или изготовлением и сбытом ценных бумаг.

За 1 полугодие 2002 года подразделениями ОВД было выявлено свыше 11 тыс. преступлений, связанных с изготовлением или сбытом поддельных денег или ценных бумаг (ст. 186 УК РФ). За АППГ – 5,9 тыс. При этом сотрудниками аппаратов БЭП СКМ выявлено более 6,5 тыс. преступлений (59,3%), сотрудниками уголовного розыска 200 фактов (1,8%), РУБОП, УОП, ООП и ОРО – 129 (1,1%).

За тот же период выявлено 124 факта хищений денежных средств путем подделки ценных бумаг, в том числе 26 фактов (20,9%) путем подделки различных ценных бумаг государственных предприятий, отделений Сбербанка России и 98 фактов (79,0%) подделки ценных бумаг (векселей, чеков, акций и облигаций), а также подложных расчетных документов других субъектов финансово-хозяйственной и предпринимательской деятельности.

В результате оперативно-розыскных мероприятий и следственных действий из обращения было изъято 26 ценных бумаг государственных предприятий на сумму свыше 40,4 млн. рублей, а также 116 ценных бумаг и расчетных документов иных предприятий на сумму более 53,6 млн. рублей. От общего числа выявленных фактов хищений денежных средств с использованием подложных платежных документов и ценных бумаг (государственных и иных предприятий) 11 фактов подделки (8,8%) было совершено мошенническим способом (дорисовкой цифр, наклейкой нулей и т.п.) на общую сумму 4,5 млн. рублей. За АППГ 2001 года – 8 преступлений на сумму 14,8 млн. рублей.

Наибольшее количество преступлений экономической направленности, связанных с изготовлением поддельных кредитных либо расчетных карт и иных платежных документов, не являющихся ценными бумагами, в том числе, совершенных неоднократно или организованными группами, выявлено аппаратами БЭП ГУВД г. Москвы. Однако по итогам 9 месяцев 2002 года результаты этой работы снизились на 66,3%, выявлено 54 факта против 160 за аналогичный период 2001 года. Вместе с тем практически все преступления текущего года относятся к тяжким и особо тяжким.

И наоборот существенный рост экономических преступлений связан с финансово-кредитной системой г. Москвы. В этой сфере в результате активизации оперативно-розыскных мероприятий выявлено свыше 6,7 тыс. фактов против 4,5 тыс. фактов за АППГ 2001 года (рост на 48,0%). Причем на 79,1% увеличилось количество хищений денежных средств в крупных и особо крупных размерах или 2,4 тыс. против 1,3 тыс. за 9 мес. 2001 года.

По всем выявленным преступлениям было возбуждено и направлено в суды 20 уголовных дел (16,1%), а 64 уголовных дела (51,6%) было приостановлено в связи с неустановлением, либо нерозыском лиц, совершивших изготовление и сбыт ценных бумаг, хищение денежных средств с использованием подложных платежных документов.

**9. Основные негативные факторы влияющие на криминогенную обстановку в сфере использования компьютерной техники и кредитных карт, в т.ч. недостатки в деятельности ОВД:**

- несовершенство общероссийского законодательного и нормативно-правового регулирования использования компьютерной техники, передовых компьютерных технологий и информационного обмена в деятельности правоохранительных органов;

- противоправная разведывательнаядеятельность организованных преступных группировок, сообществ и организаций, непосредственно направленная не только на совершение преступлений с применением компьютерных технологий, но и на сбор сведений по раскрытию методов работы и планов деятельности органов внутренних дел Российской Федерации;

- имеющиеся нарушения инструкций МВД России и установленного регламента сбора, обработки, хранения и передачи секретной и служебной информации, которая содержится в ведомственных АБД и компьютерной информации, использующейся для раскрытия преступлений экономической направленности;

- отсутствие до сего времени единых методик и методологии хранения и обработки оперативно-розыскной информации в компьютерных сетях ФСБ, МВД, ФСНП, ФПС РФ и др. федеральных правоохранительных органов, не позволяет организовать на надлежащем уровне обмен справочными, статистическими и криминалистическими данными о подготавливаемых и совершаемых преступлениях, в т.ч. экономической направленности;

- задержка передачи, искажение*,* а нередко и сокрытие оперативной информации, а также преднамеренные действия, либо грубые ошибки оперативных сотрудников и техперсонала с компьютерной техникой, приводят не только к несанкционированному доступу к ней криминальных элементов из числа ОПГ, но и прямому сращиванию с преступной средой;

Кроме того к основным факторам, негативно влияющим на выявление и расследования уголовных дел о хищениях денежных средств, мошенничества с кредитными картами и иными платежными документами можно отнести следующие:

- несмотря на то, что с созданием в ГУВД Москвы и на местах подразделений по борьбе с хищениями, совершаемыми с помощью электронных средств доступа, создана система подразделений ОВД, специализирующихся на борьбе с этими преступлениями, не решен ряд отраслевых проблем. Нет централизованного учета поддельных кредитных карт и иных подложных платежных средств; оперработники слабо владеют особенностями оборота карт и методиками выявления мошенничеств, особенно совершаемыми международными ОПГ;

- несвоевременное получение от представительств международных расчетных систем и банков-эмитентов кредитных карточек заявлений об их противоправном использовании, причинении материального ущерба, а также информации об их законных держателях;

- задержка информации об их возможной причастности к мошенническому использованию кредитных (дебетовых карт), иных расчетных операциях с картами и иными расчетными документами на территории России, промедление с предоставлениемсотрудникам подразделений БЭП СКМ и СК образцов почерка и подписи держателей (для проведения сравнительных исследований);

- при проведении почерковедческих и технических экспертиз постоянно возникают существенные сложности для экспертов, т.к. в распоряжении следствия в основном остаютсявторые и третьиэкземпляры слипов кредитных карт, которые оформляются через копировальную бумагу; кроме того, сравнительному исследованию приходится подвергать копии сотен слипов*,* что значительно затягивает расследование;

- практически во всех региональных подразделениях МВД-ГУВД-УВД возникает необходимость проведения безотлагательных выемок документов в коммерческих банках, однако известно, что последнее представляет известные трудности с учетом соблюдения требований ст.26 Закона РФ «О банках и банковской деятельности» (о банковской тайне);

- часть похищаемых денежных средств перечисляются на корреспондентские счета в зарубежных банках, либо открытых в филиалах российских коммерческих банках, а согласно ст. 26 вышеуказанного закона наложение ареста на такие счета может быть проведено только по решению суда;

## В целом анализ динамики развития и проблем кредитно-финансовой системы за ряд последних лет показывают, что даже к концу 2002 года в Российской Федерации все еще есть регионы, где не только нет возможности выбирать банк, обслуживающий клиентуру с применением кредитных карт, но и сложно вообще найти какую-либо банковскую структуру для финансового обслуживания, что влечет различные злоупотребления. Причем до сего времени имеются разногласия о том, какое количество банков оптимально для российской экономики.

**10. Предложения в аналитическую записку и практические рекомендации о мерах совершенствования деятельности ОВД.**

10.1. Поскольку одной из задач МВД РФ является защита предпринимательской деятельности, необходимо активизировать деловое сотрудничество с провайдерским бизнесом, банками-эмитентами, с созданными ими службами безопасности, ЧОПами, которые в чем-то дублируют правоохранительную деятельность. Службе БЭП СКМ необходимо продолжить постоянное и конструктивное взаимодействие с ними, задействовать их в плане обеспечения компьютерной безопасности, использования банками и потребителями расчетных документов.

10.2. В этой связи, при проведении «круглых столов» с участием представителей фирм-провайдеров, банков и сети интернет-торговли рекомендовать конкретные меры повышения безопасности. Совместно с СБ этих систем внедрять передовые методики контроля за работой кассиров, выполнения ими должностных инструкций о порядке приёма кредитных (дебетовых) карт и дорожных чеков к оплате, что одновременно повысит уровень взаимодействия с сотрудниками БЭП СКМ МВД,ГУВД,УВД, горрайорганов.

10.3. При этом МВД РФ, совместно с СБ международных и российских расчетных систем и банков необходимо повысить уровень координирующих и контрольных функций, постоянное внедрение новых технологий, в целях защиты кредитных (дебетовых) карт от мошеннических подделок, превентивные меры по выявлению незаконных операций по хищению денежных средств на ранних стадиях.

10.4. В частности, в процессе рабочего взаимодействия, рекомендовать специалистам СБ ведущих процессинговых (расчетных) систем и Банка России усилитьштрафныесанкции к банкам, скрывающим случаи преступлений с кредитными карточками, а службам безопасности банков усилить охрану пунктов обслуживания платежных пунктов, в т.ч. банкоматов.

10.5. В системах, где оборот карточек весьма высок (по российским меркам), рекомендовать повсеместное внедрение самообучающихся компьютерных программ для выявления мошеннических подделок кредитных карт на стадии контакта с импринтером или банкоматом. На наш взгляд, несмотря на высокую стоимость, услуга несомненно прогрессивна и рентабельна.

10.6. Имеющийся опыт показал, что совершенствование нормативной базы однозначно ведет к снижению уровня хищений и мошенничества. В этой связи представляется необходимым МВД РФ внести предложения о дополнении не только уже принятых законов, но всего блока нормативных актов, регулирующих оборот в России кредитных (дебетовых) карточек, дорожных чеков, иных платежных документов. При этом важно ускорить присоединение к общеевропейскому законодательству по предотвращению мошеннического использования кредитных карт.

10.7. В целях усиления борьбы с хищениями денежных средств мошенническим использованием кредитных карточек необходимо разработать и внестина утверждение Банком России «Положение об обязательном обучении специалистов банков-эмитентов и процессинговых систем». Имеется в виду систематическое обучение продавцов, кассиров, других операторов правилам приема кредитных карт, предупреждению и выявлению мошеннических действий с ними.

10.8. Для дальнейшего повышения безопасности применения кредитных карточек коммерческими банками, внести предложения в Банк России по результатам работы ОВД за 2002 год. В тех же целях, во взаимодействии с ГИЦ МВД РФ, разработать и внедрить форму оперативного учёта сделок с кредитными картами и иными платежными документами, признанных недействительными.

## 10.9. Кроме того, по итогам работы за 2002 год представляется целесообразным ГУБЭП СКМ МВД РФ, совместно с АРБ и Банком России рассмотреть ситуацию, сложившуюся в сфере компьютерной информации, а также использования кредитных карт. Предложить ряд конкретных мер нормативно-правового и законодательного характера, не только по совершенствованию контроля, но и упрощению порядка регистрации филиальной сети коммерческих банков.

10.10. В контексте мер улучшения учетно-регистрационной дисциплины в ОВД, для совершенствования практики выявления рассмотренных преступлений аппаратами БЭП СКМ, по всем нераскрытым фактам противоправного использования кредитных карт, хищений денежных средств путем подделки иных платежных документов, либо неправомерного доступа к компьютерной информации, ввести вместо дел оперучета – карты-накопители.

##### НИЛ-2 Центра № 2 ВНИИ МВД РФ