МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВОЛГОГРАДСКАЯ АКАДЕМИЯ

В. Б. ВЕХОВ

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ПЛАСТИКОВЫХ КАРТ И ИХ РЕКВИЗИТОВ

Монография

Волгоград 2004

ББК 67.629.41
В 39

Одобрено
редакционно-издательским советом
Волгоградской академии МВД России

Вехов В. Б.

В 39 Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов: Монография. – Волгоград: ВА МВД России, 2004. – 280 с., 500 экз.

ISBN 5-7899-0300-2

Эта книга – одна из первых работ, посвященных исследованию актуальных научно-практических проблем расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов.

В издании комплексно рассматриваются: понятие и криминалистическая характеристика данных преступных посягательств; признаки различных способов их совершения; типичные следы и методы их выявления; обстоятельства, подлежащие установлению и доказыванию; типичные следственные ситуации и действия сотрудников органов предварительного расследования на первоначальном этапе. Даны практические рекомендации по организации расследования преступлений выделенной категории, методике и тактике производства отдельных следственных действий, взаимодействию следователей с органами дознания и специалистами.

Книга предназначается для студентов, аспирантов и преподавателей юридических образовательных учреждений, а также практических работников правоохранительных органов.

ББК 67.629.41

Р е ц е н з е н т ы : *В. В. Попова, В. М. Решетников*

ISBN 5-7899-0300-2

О Г Л А В Л Е Н И Е

Введение …….. 5

Глава 1. **КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ПЛАСТИКОВЫХ КАРТ И ИХ РЕКВИЗИТОВ**…… 8

§ 1. Понятие криминалистической характеристики преступлений, совершенных с использованием пластиковых карт и их реквизитов..…..……..…….. 8

§ 2. Содержание и основные элементы криминалистической характеристики преступлений, совершенных с использованием пластиковых карт и их реквизитов..…… 23
2.1. Понятие пластиковой карты как предмета и орудия совершения преступления……..…… 23
2.2. Криминалистическая классификация пластиковых карт…. 43
2.3. Сведения о некоторых типичных обстоятельствах совершения преступления и личности преступника…….. 76

§ 3. Способы преступлений, основанные на использовании технологий пластиковых карт, и типичные следы их применения…… 91
3.1. Использование подлинных карт ……92
3.2. Использование конфиденциальной информации о реквизитах подлинных карт и их держателях……..109
3.3. Использование поддельных карт…….. 147
3.4. Использование несовершенства программно-аппаратного обеспечения технологии обращения пластиковых карт……..…… 159

Глава 2. **ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ПЛАСТИКОВЫХ КАРТ И ИХ РЕКВИЗИТОВ, НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ**..…… 163

§ 1. Общие вопросы организации первоначального этапа расследования ……..…….. 163

§ 2. Программы действий следователя на первоначальном этапе расследования. Обстоятельства, подлежащие установлению…….. 181

Глава 3. **ОСОБЕННОСТИ ТАКТИКИ ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ**…… 205

§ 1. Особенности тактики осмотра места происшествия…..…….. 205

§ 2. Особенности тактики осмотра пластиковой карты..…….. 213

§ 3. Особенности тактики осмотра документов, подтверждающих законность проведения операции и право пользования пластиковой картой…….. 221

§ 4. Особенности тактики осмотра документа на машинном носителе (электронного документа)…..……..…….. 223

§ 5. Особенности тактики осмотра машинограммы…….. 229

§ 6. Особенности тактики осмотра электронного терминала..…..… 232

§ 7. Особенности тактики обыска и выемки ……..…… 239

§ 8. Особенности тактики допроса ..…….. 244

§ 9. Особенности тактики подготовки и назначения судебных экспертиз..……256

Литература……..……263

Приложения

1. Криминалистическая классификация пластиковых карт…… 272
2. Словарь жаргонных слов и выражений..……..……..273

ВВЕДЕНИЕ

В настоящее время не вызывает сомнений тот факт, что пластиковые карты стали все активнее вытеснять из гражданского и служебного оборота обычные бумажные документы, начиная от удостоверений личности, пропусков, санкционирующих доступ на охраняемый объект либо в хранилище, и заканчивая реальными деньгами и документами, подтверждающими имущественные права. При этом известно, что для совершения большинства операций используются не сами карты, а лишь реквизиты, указанные на них и вводимые в компьютерное терминальное устройство. По действующему российскому законодательству, большинство этих реквизитов являются конфиденциальными, т. е. относятся к различного вида тайнам и иной охраняемой законом информации.

К сожалению, такое импульсивное внедрение в указанные чувствительные сферы экономики страны последних достижений научно-технического прогресса не было адекватно подкреплено соответствующей законодательной и иной нормативной базой. Являясь одним из прогрессивных и достаточно широко используемых средств организации безбумажных технологий, особенно в сфере денежного обращения при проведении расчетно-кассовых операций, оборот пластиковых карт в России остается не урегулированным на законодательном уровне. Подготовленный еще в августе 1997 г. проект Федерального закона «Об использовании платежных карт в Российской Федерации», так до сих пор и не рассмотрен Государственной Думой. Такое положение дел привело к серьезным негативным последствиям.

Анализ специальной литературы и материалов конкретных уголовных дел показывает, что в последние годы наблюдается заметное увеличение числа преступлений, связанных между собой одним общим криминалистическим признаком – все они были совершены с использованием пластиковых карт и их реквизитов. К ним можно отнести следующие составы: *кража* (ст. 158 УК РФ), *мошенничество* (ст. 159 УК РФ), *изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов* (ст. 187 УК РФ), *незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну* (ст. 183 УК РФ), *неправомерный доступ к компьютерной информации* (ст. 272 УК РФ), *нарушение правил эксплуатации*

ЭВМ, системы ЭВМ или их сети[1] (ст. 274 УК РФ), *лжепредпринимательство* (ст. 173 УК РФ), *легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем* (ст. 174 УК РФ), *легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления* (ст. 174.1 УК РФ). С помощью пластиковых карт, разработанных на их основе специальных технических средств и созданных поддельных документов преступникам во многом беспрепятственно удается проникать в охраняемые объекты и хранилища с целью хищения чужого имущества, мошенническим путем – без соответствующей оплаты пользоваться услугами электросвязи, железнодорожного транспорта и другими.

В наши дни говорить о серьезности проблемы борьбы с преступлениями в сфере высоких технологий, одним из видов которых являются рассматриваемые преступные деяния, нет никакого смысла. Актуальность этой темы очевидна. Столь же очевидно и то, что достигнутые на этом фронте отечественными правоохранительными органами успехи явно проигрывают по сравнению с неудачами. Например, официальная статистика свидетельствует о том, что количество таких преступлений увеличивается ежегодно в несколько раз, а наносимый ими материальный ущерб возрастает в арифметической прогрессии, по сравнению с хищениями, совершенными обычными (традиционными) способами. Так, по данным Главного информационного центра МВД России, в 1997 г. было зарегистрировано 53 преступления, ущерб от которых составил 1,6 млн рублей, в 1998 г. – 98 преступлений с общим ущербом в 88,2 млн рублей, в 1999 г. – 325 преступлений и 99,5 млн рублей

---

[1] Под **электронной вычислительной машиной** (**ЭВМ**) понимается программируемое электронное техническое устройство, состоящее из одного или нескольких взаимосвязанных центральных процессоров и периферийных устройств, управление которых осуществляется посредством программ, и предназначенное для автоматической обработки информации в процессе решения вычислительных и (или) информационных задач. **Система ЭВМ** – совокупность ЭВМ, программного обеспечения и периферийных устройств, предназначенных для организации и (или) осуществления информационного процесса. **Периферийные устройства** – технические устройства, обеспечивающие передачу данных и команд между оперативным или постоянным запоминающим устройством и пользователем относительно определенного центрального процессора (комплекс внешних устройств ЭВМ, не находящихся под непосредственным управлением центрального процессора). **Сеть ЭВМ** – две и более ЭВМ, объединенные между собой с помощью средств электросвязи.

ущерба, в 2000 г. – 467 преступлений и 155,8 млн рублей ущерба, в 2001 г. – 600 преступлений и 200 млн рублей ущерба[2].

Представляется, что одной из главных причин такого негативного положения дел является недостаточная обеспеченность оперативных, следственных и экспертных работников соответствующим научно обоснованным инструментарием, который необходим для качественного решения стоящих перед ними сложных задач, возникающих на стадиях возбуждения уголовных дел и предварительного расследования. В первую очередь это касается методики расследования преступлений выделенной категории, основные составляющие которой и раскрываются в настоящей монографии.

Автор надеется, что рассмотренные в работе понятия, характеристики, классификации, методы и рекомендации окажутся полезными не только для сотрудников правоохранительных органов, но и вызовут живой интерес у научных работников, разрабатывающих те или иные вопросы борьбы с преступлениями, совершенными с использованием пластиковых карт и их реквизитов, а также всех, кто изучает и преподает криминалистику.

[2] См.: *Анчабадзе Н.А.* Организационно-правовые и криминалистические вопросы предотвращения хищений, совершаемых в финансовой сфере с использованием пластиковых карточек, мошенническим путем. – Волгоград, 2002. – С. 5.

Глава 1

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ПЛАСТИКОВЫХ КАРТ И ИХ РЕКВИЗИТОВ

§ 1. ПОНЯТИЕ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ПЛАСТИКОВЫХ КАРТ И ИХ РЕКВИЗИТОВ

Известно, что криминалистическая характеристика обусловлена не общим понятием преступления, которое определяет уголовный закон, а представляет собой некую форму абстракции, основанную на результатах научного изучения и обобщения современной криминальной практики. Отражая типичные особенности разнообразных видов (групп) преступлений, она является обособленным продуктом научного анализа значительного и разнообразного эмпирического материала, результатом самостоятельного научного исследования, а также средством, способствующим решению прикладных задач следственно-оперативной практики. Практическое значение криминалистической характеристики заключается в том, что при наличии одних признаков (например, относящихся к следам орудий и инструментов) следователь может предположить наличие других (например, определенных профессиональных навыков у преступника) и провести в связи с этим необходимые следственные действия, ревизионные и иные мероприятия (например, по возмещению ущерба, причиненного преступлением, установлению и задержанию преступника)[3].

Вместе с тем криминалистическая характеристика – категория динамичная, изменяющаяся под воздействием совокупности объективных и субъективных факторов. Данное свойство отчетливо проявляется в видовой криминалистической характеристике, когда, например, под воздействием научно-технического прогресса изменяются способы преступления, орудия и предметы преступного посягательства, причины и условия, способствовавшие соверше-

[3] См.: *Ермолович В.Ф.* Криминалистическая характеристика преступлений / В.Ф. Ермолович. – Минск, 2001. – С. 245.

нию данной группы преступлений. В связи с чем меняются и видовые криминалистические характеристики. «Криминалистическая характеристика преступлений, – пишет И.Ф. Пантелеев, – не застывшая, неизменная совокупность определенных сведений о данной группе (виде) преступлений, а подвижная категория, отражающая криминалистически значимые особенности этих преступлений в определенный период времени»[4]. Нельзя не согласиться с утверждением о том, что криминалистическая характеристика будет выполнять свою роль лишь тогда, когда она будет не только реальной и достаточно полной, но и современной – отражающей последние изменения в криминальной практике, содержащей «свежие» результаты криминалистического анализа данной группы (вида) преступлений, совершенных в последний (анализируемый) период времени[5]. По этим обстоятельствам рассматриваемая дефиниция относится к тем проблемам криминалистической науки, которые в последние годы широко и очень активно изучаются и обсуждаются в литературе.

Анализ многочисленных научных работ по рассматриваемой проблематике показывает, что предлагаемые авторами определения понятия «криминалистическая характеристика преступлений» хотя и отличаются по существенным признакам, но не носят принципиального характера. Большинство ученых-криминалистов солидарны в том, что криминалистическая характеристика преступлений должна служить отправной точкой для формирования методики расследования преступлений. По этой причине в структуре частных методик ей отводится первое место, по сравнению с другими составляющими[6].

Комплексное исследование, проведенное Р.С. Белкиным, показало, что наряду с криминалистической характеристикой преступления в состав методики также входят: описание типичных следственных ситуаций и особенностей планирования действий

---

[4] Криминалистика: Учебник / Под ред. И.Ф. Пантелеева, Н.А. Селиванова. – М., 1993. – С. 26.

[5] См.: Там же. – С. 27.

[6] См., например: *Колесниченко А.Н.* Общие положения методики расследования отдельных видов преступлений. – Харьков, 1976. – С. 19-20; *Возгрин И.А.* Научные основы криминалистической методики расследования преступлений. Ч. 4. – СПб., 1993. – С. 21; Криминалистика: Учебник / Под ред. И.Ф. Герасимова, Л.Я. Драпкина. – М., 1994. – С. 328; Криминалистика / Под ред. проф. В.А. Образцова. – М., 1997. – С. 495-496; Криминалистика: Учебник / Под ред. Н.П. Яблокова. – 2-е изд., перераб. и доп. – М., 1999. – С. 491; *Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р.* Криминалистика: Учебник для вузов / Под ред. проф. Р.С. Белкина. – М., 2000. – С. 687.

следователя на первоначальном и последующем этапах расследования; изложение тактики первоначальных следственных действий и сопутствующих оперативно-разыскных мероприятий; описание типичного круга и особенностей последующих следственных действий в их сочетании с осуществляемыми на этом этапе расследования оперативно-разыскными мероприятиями[7]. Соглашаясь с автором в том, что под частной криминалистической методикой следует понимать «типизированную систему методических (научно-практических) рекомендаций по организации и осуществлению расследования и предотвращения отдельного вида преступлений»[8], отметим, что в настоящей работе в качестве «отдельного вида преступлений» выделяются преступные посягательства, совершенные с использованием пластиковых карт и их реквизитов.

С учетом методологических положений современной криминалистической науки, возможно заключить следующее. **Во-первых**, необходимо различать два вида криминалистической характеристики – общую и частную. **Во-вторых**, *под криминалистической характеристикой преступлений, совершенных с использованием пластиковых карт и их реквизитов, целесообразнее всего понимать систему криминалистически значимых сведений, полученных в результате специальных научных исследований, которая является основополагающим структурным элементом методики расследования этих преступлений и способствует их раскрытию, расследованию и предупреждению*.

Анализ многочисленных литературных источников показывает, что большинство исследователей к основным элементам криминалистической характеристики рода, вида или группы преступлений чаще всего относят следующие:

1) характеристика типичной исходной информации;

2) обобщенные данные о типичных способах подготовки, совершения и сокрытия преступлений;

3) типичные материальные следы преступления и вероятные места их нахождения (локализации);

4) криминалистически значимые сведения о типичных предметах преступного посягательства;

---

[7] Подробнее см.: *Белкин Р.С.* Курс советской криминалистики. Т. 3. – М., 1979. – С. 176-214; *Он же.* Курс криминалистики: В 3-х т. Т. 3: Криминалистические средства, приемы и рекомендации. – М., 1997. – С. 298-341.

[8] *Белкин Р.С.* Курс криминалистики: В 3-х т. Т. 3: Криминалистические средства, приемы и рекомендации. – С. 301.

5) криминалистически значимые сведения о личностных особенностях вероятных потерпевших;

6) криминалистически значимые сведения о личности вероятного преступника, типичных мотивах и целях преступления;

7) обобщенные данные о некоторых типичных обстоятельствах совершения преступления (месте, времени и обстановке);

8) данные о типичных обстоятельствах, способствовавших совершению преступления.

В связи с этим было бы логически правильно рассмотреть возможность включения в понятие криминалистической характеристики преступлений выделенного вида каждого из указанных элементов. Для достижения данной цели, как наиболее удачные, будут использоваться подход и методология, предложенные профессором Р.С. Белкиным[9].

При разработке частной криминалистической методики расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов, большое значение будет иметь исследование наиболее типичных источников, содержания и условий получения первоначальной криминалистически значимой информации о событии преступного деяния. Очевидно, что характер и полнота исходных данных, имеющихся в распоряжении оперативного сотрудника, дознавателя или следователя, учитываются ими при выдвижении версий, определяют последовательность и порядок проведения первоначальных следственных действий и оперативно-разыскных мероприятий, помогают сузить круг лиц, среди которых надлежит искать вероятного преступника. Поэтому описание типичной исходной информации является одним из начальных элементов криминалистической характеристики преступлений выделенного вида. Однако, и это следует подчеркнуть, исходные данные никоим образом нельзя отождествлять с понятием следственной ситуации, поскольку они дают представление лишь о некоторых ее компонентах. Следственная ситуация представляет собой сложную систему взаимодействий следователя и иных субъектов, участвующих в доказывании, действующих в конкретной обстановке, в которой происходит расследование, под воздействием объективных и субъективных факторов[10]. Правы те авторы, которые полагают, что криминалистическая характеристика является лишь вероятностной моделью происшедшего криминального события и только как таковая может быть использована в качестве основания

---

[9] См.: Там же. – С. 312-315.

[10] Подробнее об этом см.: *Белкин Р.С.* Очерки криминалистической тактики. – Волгоград, 1993. – С. 63-71.

для таких же вероятностных умозаключений – следственных версий[11]. Криминалистическая характеристика при этом играет роль своеобразной матрицы, которая «накладывается» на конкретный исследуемый в ходе раскрытия и расследования случай и позволяет с достаточной степенью достоверности построить его вероятностную модель. Именно с этих позиций и необходима характеристика типичной исходной информации.

Способы подготовки, совершения и сокрытия (маскировки) преступлений также имеют ярко выраженное криминалистическое значение. Существование определенных черт, характерных именно для данного конкретного вида преступлений, позволяет говорить о них как об основном элементе криминалистической характеристики, имеющем решающее значение для частной методики. Вместе с тем в науке в настоящее время все еще не существует какой-нибудь общей позиции в вопросе содержания данного понятия.

Изучением этой проблемы занимались многие исследователи. Среди научных работ особо выделяется диссертационное исследование на соискание ученой степени доктора юридических наук профессора Г.Г. Зуйкова по теме: «Криминалистическое учение о способе совершения преступления». В ней автор рассматривает **способ как систему действий** по подготовке, совершению и сокрытию преступления, детерминированных условиях внешней среды и психофизиологическими свойствами личности, могущих быть связанными с избирательным использованием соответствующих орудий или средств и условий места и времени[12]. Продолжая отстаивать свою точку зрения, в последующих работах он пишет: «Во взаимосвязанный комплекс действий преступника входят осуществляемые до завершения исполнения преступного замысла действия, направленные на подготовку к совершению преступления, на его сокрытие, а не только непосредственно на его совершение»[13].

И.А. Возгрин, в свою очередь, полагает, что способ совершения преступления стоит рассматривать в широком смысле этого понятия, включая в нее подготовку и сокрытие преступного посягательства, так как «это система взаимосвязанных и взаимообусловленных действий, с помощью которых преступник достигает своей

---

[11] См.: *Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р.* Криминалистика: Учебник для вузов / Под ред. проф. Р.С. Белкина. – М., 2000. – С. 688.

[12] См.: *Зуйков Г.Г.* Криминалистическое учение о способе совершения преступления: Автореф. дис. … д-ра юрид. наук. – М., 1970. – С. 10.

[13] *Зуйков Г.Г.* Способы сокрытия преступления и уклонения от ответственности // Способы сокрытия следов преступлений и криминалистические методы их установления: Сб. трудов. – М., 1984. – С. 21.

цели»[14]. Исследование способа совершения преступления как элемента криминалистической характеристики он видит в установлении наиболее распространенных видов орудий и средств, применяемых преступниками, выявлении типичных мест и определении характерного времени преступления, изучении обстоятельств, способствующих преступлению, и описании материальных и идеальных следов преступления или изучении его **типичной следовой картины**[15]. Изложенное положение принципиальных возражений не вызывает, хотя более точна в этом вопросе позиция Р.С. Белкина, который считает, что данные определения верны лишь для тех случаев, «когда подготовка, совершение и сокрытие преступления совершаются по заранее обдуманному единому замыслу, когда все эти действия действительно связаны между собой в единую систему и, еще не совершив преступление, субъект имеет четкую программу действий по его сокрытию»[16]. Естественно, такое бывает не всегда. Чаще всего, по его мнению, возможны два варианта:

1) *действия по совершению и сокрытию преступления могут быть разорваны по субъекту*, когда сокрытие преступления совершается не тем, кто его совершил, а другим лицом без ведома субъекта преступления, не предпринимавшего этих мер вообще для сокрытия своих преступных действий;

2) *действия по совершению и сокрытию преступления могут быть разорваны по замыслу*, когда цели сокрытия преступником первоначально не преследовались, а возникли уже после совершения преступления в связи с непредвиденными или изменившимися обстоятельствами[17].

Разделяя изложенную точку зрения, представляется более правильным считать, что способ сокрытия преступления может существовать самостоятельно как система действий по уничтожению, маскировке или фальсификации материальных следов преступления.

Из вышеуказанного следует, что структура способа совершения преступления является непостоянной категорией. В зависимости от своеобразия поведения преступника, ситуаций, возникающих до и после совершения преступления, и иных обстоятельств она может быть трех видов:

---

[14] *Возгрин И.А.* Научные основы криминалистической методики расследования преступлений. Ч. 4. – СПб., 1993. – С. 26.

[15] См.: Там же.

[16] *Белкин Р.С.* Курс криминалистики: В 3-х т. Т. 3: Криминалистические средства, приемы и рекомендации. – С. 313.

[17] См.: Там же.

1) трехзвенной – включать в себя поведение субъекта до, во время и после совершения преступления;

2) двухзвенной – содержать различные комбинации типичных действий преступника, наиболее ярко проявляющиеся в ходе подготовки и в момент совершения, в момент совершения и в ходе сокрытия либо только в ходе подготовки и сокрытия преступления;

3) однозвенной – характеризовать поведение субъекта лишь во время самого преступного акта[18].

С учетом отмеченных мнений, было бы вполне логично сделать вывод о некорректности выделения отдельными авторами в качестве самостоятельного элемента криминалистической характеристики совокупности сведений о типичных материальных следах преступления и вероятных местах их нахождения[19]. Подобное утверждение и позицию в этом вопросе можно пояснить тем, что описание способов подготовки, совершения и сокрытия преступления сводится не только к описанию действий или бездействия субъекта, с помощью которых достигается цель преступного посягательства, но и к описанию типичных последствий применения того или иного способа, типичных орудий и средств, оставляемых следов и мест, где эти следы вероятнее всего могут быть обнаружены. Иными словами, описание способов всегда идет через призму типичных материальных и идеальных следов и вероятных мест их нахождения (локализации), характерных для конкретного вида преступлений. «При разработке частных криминалистических методик идут именно этим путем: описывают, например, типичные способы хищений денег и тут же указывают, какие признаки позволяют судить об этих способах, то есть какие следы они оставляют... «Голое» описание способа совершения преступления не достигает цели, его надо производить либо от следов применения данного способа с тем, чтобы по ним раскрывать механизм преступления, либо к следам применения этого способа, чтобы, зная его, суметь обнаружить доказательства совершенного преступления и установить личность преступника»[20].

Вместе с тем, как всякий акт человеческого поведения, преступление в целом и способы его осуществления определяются взаимодействием многих причин и условий, оказывающих влияние как

---

[18] Идею такой классификации см.: Криминалистика: Учебник / Под ред. Н.П. Яблокова, В.Я. Колдина. – М., 1990. – С. 328.

[19] См., например: Криминалистика: Учебник / Под ред. И.Ф. Пантелеева, Н.А. Селиванова. – М., 1993. – С. 31.

[20] *Белкин Р.С.* Курс криминалистики: В 3-х т. Т. 3: Криминалистические средства, приемы и рекомендации. – С. 314.

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 и тем большей информацией будет располагать следователь для выдвижения следственных и разыскных версий. Применительно к рассматриваемой в настоящей работе проблеме наибольшую ценность будут представлять следы, указывающие на то, каким образом преступник попал на место преступления (получил доступ к предмету преступного посягательства), ушел с него, преодолел различного рода физические и интеллектуальные преграды, использовал свое служебное положение, выполнил намеченную преступную цель; какие знания, умения, навыки и физические усилия применил; пытался или не пытался скрыть следы совершенного деяния. В этом отношении особенно существенное значение будут иметь следы, свидетельствующие о характере связи преступника с предметом преступного посягательства.

Именно такого рода признаки, проявляющиеся вовне, и позволяют создать основу для наиболее быстрого распознавания в процессе первоначальных следственных действий того или иного характерного способа преступления даже по его отдельным признакам. Это дает возможность точнее определить направление и методы выявления остальных недостающих данных о предполагаемом способе и вероятном преступнике, который мог им воспользоваться, в целях быстрого раскрытия и расследования преступления. При этом, с криминалистической точки зрения, важно не только выявить все внешние проявления, но и установить, что в нем было заранее заготовлено преступником, а что явилось результатом приспособления к сложившейся на момент совершения преступного деяния внутренней и внешней обстановке[21]. Данное обстоятельство связано с тем, что сам факт и характер вносимых в заранее продуманный способ совершения преступления коррективов также содержит существенную информацию о степени осведомленности преступника в той обстановке, которая сложилась к моменту преступного деяния, а также о его привычках, навыках, наличии преступного опыта, некоторых физических, интеллектуальных, профессиональных и иных индивидуальных особенностях.

Одновременно с вышеуказанным стоит обратить внимание и на то, что способ совершения и сокрытия преступления относится как

---

[21] См.: *Белкин Р.С., Лузгин И.М.* Криминалистика: Учеб. пособие. – М., 1978. – С. 243.

к объективной стороне состава преступления (включается в его уголовно-правовую характеристику), так и к предмету доказывания, обладая при этом процессуальным содержанием. Как известно, способ совершения преступления является в ряде составов необходимым элементом объективной стороны преступления и входит в его уголовно-правовую характеристику. Иногда он также 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 указанной характеристике способ совершения преступления представлен в общем виде, например способ открытого или тайного хищения чужого имущества, проникновения в жилище, помещение или иное хранилище, и для нее безразличны приемы открытого или тайного хищения, конкретные способы проникновения в хранилище, используемые при этом технические средства, источник их получения и т. д. В этом случае имеет место уже криминалистическая характеристика способа совершения преступления.

Помимо указанного, с криминалистической точки зрения способ всегда конкретен и у него имеется немало таких граней, которые имеют важное следственно-оперативное значение. Среди них выделяются следующие: распространенность способа, конкретные приемы его применения, используемые при этом технические и иные средства, их конструктивные особенности; сведения о том, как подготавливалось преступление, каким образом проводились тренировки, как и где изготавливались или приспосабливались необходимые орудия и другие средства совершения преступления, каковы источники их получения, какие недостатки в учете их хранения облегчили доступ к ним преступных элементов, какие технологические процессы, оборудование, материалы и документы использовались для их изготовления, каким образом и с помощью каких методов они применялись при совершении и сокрытии преступления[22].

---

[22] Подробнее см.: Криминалистика: Учебник / Под ред. И.Ф. Пантелеева, Н.А. Селиванова. – М., 1993. – С. 33.

Сведения о типичных личностных особенностях вероятных преступников и потерпевших также могут иметь криминалистическое значение. Знание данного элемента криминалистической характеристики оперативным сотрудником, дознавателем или следователем позволяет, как уже отмечалось ранее, сузить круг лиц, среди которых может находиться преступник. Одновременно с этим такая характеристика позволяет выдвинуть версии о мотиве и цели преступления, способе его совершения и сокрытия, месте нахождения искомых объектов и других обстоятельствах преступного деяния. Впрочем, как и наоборот.

Исследования в области криминологии, юридической психологии и виктимологии показывают, что преступники и потерпевшие нередко обладают рядом психологических, физических, биологических и социальных черт, типичных для отдельных видов преступлений. Кроме того, между жертвой и субъектом преступления, предметом и преступником, как правило, существуют связи определенного характера. Выявление этих черт и связей в ходе раскрытия и расследования преступления позволяет уже по последствиям преступного деяния судить о личностных особенностях преступника и характере деятельности потерпевшего, что в конечном итоге оптимизирует работу органов предварительного расследования.

Известно, что ряд сведений о личности субъекта преступления остается за пределами криминологической характеристики. К ним, в частности, можно отнести так называемые «профессиональные» навыки преступников, проявляющиеся в определенных способах преступлений и отражающиеся в материальной обстановке места происшествия в виде определенного индивидуального «почерка». В свою очередь, на месте совершения преступления обнаруживаются и такие вещественные улики, которые проливают свет не только на «профессиональные» навыки преступника, но и на его личностные качества: осведомленность, интеллектуальность, образованность и другие. Совокупность таких сведений имеет большое разыскное значение[23]. Выявление всех возможных форм выражения личности, отраженных в первичной информации о событии преступления, в ходе его раскрытия и расследования, позволяет составить представление об общих, а затем и о частных (индивидуальных) особенностях преступника. Подобная информация, несомненно, должна быть выделена в качестве самостоятельного элемента криминалистической характеристики, в содержание

[23] См.: Там же. – С. 35-36.

которого также следует включить криминалистически значимые сведения о типичных мотивах и целях преступления, не выделяя их отдельно, обособленно, как это предлагает И.А. Возгрин[24].

Рассматривая архитектонику строения криминалистической характеристики преступлений, совершенных с использованием пластиковых карт и их реквизитов, нельзя оставить без внимания характеристику некоторых типичных обстоятельств, имеющих криминалистическое значение. По мнению ряда авторов (А.Н. Васильев, Р.С. Белкин, В.Г. Танасевич, И.А. Возгрин), сведения о месте, времени, типичных непосредственных предметах посягательства, особенностях технологий их оборота и условиях охраны должны включаться в качестве элемента криминалистической характеристики имущественных преступлений. «Таким образом, – писал И.А. Возгрин, – обстоятельства, подлежащие доказыванию при расследовании отдельных видов (групп) преступлений, имеют для частных криминалистических методик то же самое значение, что и остальные элементы криминалистических характеристик преступлений, и нет никаких оснований отрывать их друг от друга. Более того, и с этим стоит согласиться, в структуре частных методик расследования нет иного места для их описания, чем их криминалистические характеристики»[25]. Вместе с тем, в связи с новизной для отечественной криминалистической науки и практики исследуемых в настоящей работе типичных предметов и орудий преступлений – пластиковых карт и их реквизитов, возможно выделить описание их признаков в качестве самостоятельного элемента криминалистической характеристики.

Анализ литературы показывает, что в настоящее время в криминалистике разработано много различных частных методик расследования преступлений отдельных видов. Еще больше существует криминалистических характеристик одних и тех же групп преступлений. Они подразделяются на типовые (родовые), видовые и групповые, хотя отдельные стороны этого вопроса все еще дискутируются. С учетом предмета исследования настоящей работы представляется ***под видовой*** *криминалистической характеристикой понимать характеристику преступлений, совершенных с использованием пластиковых карт и их реквизитов*, а ***под групповой*** *– более мелкие их разновидности,* например: кража, совершенная с использованием пластиковой карты (электронного ключа); мошенничество, совершенное с использованием поддель-

[24] Подробнее см.: *Возгрин И.А.* Научные основы криминалистической методики расследования преступлений. Ч. 4. – СПб., 1993. – С. 25-27.

[25] *Возгрин И.А.* Указ. соч. – С. 27.

ной кредитной либо расчетной карты и документов, обеспечивающих ее применение; мошенничество, совершенное в компьютерной сети Интернет с использованием отдельных реквизитов банковской карты; изготовление или сбыт поддельных кредитных либо расчетных карт; легализация (отмывание) денежных средств или иного имущества, приобретенных незаконным путем, с использованием технологий банковских карт; незаконное или лжепредпринимательство в сфере оборота пластиковых карт; неправомерный доступ к компьютерной информации с использованием реквизитов пластиковых карт и другие. Естественно, данное положение не является бесспорным, однако оно допустимо, поскольку криминалистические характеристики представляют собой абстрактные научные категории, как было подчеркнуто ранее.

Подводя некоторую черту в исследовании выделенной дефиниции, можно отметить стремление одних авторов расширить круг элементов криминалистической характеристики, других, наоборот, – сузить его. Видимо, в этом вопросе представляется более правильным поддержать точку зрения тех ученых-криминалистов, которые считают, что дать исчерпывающий перечень элементов криминалистической характеристики преступлений не представляется возможным, ибо он так же изменчив, как изменчива сама криминальная практика, в связи с чем, по мере развития криминалистических знаний он, несомненно, будет дополняться и уточняться новыми сведениями[26]. Вместе с этим нельзя забывать, что у каждого вида преступлений должен быть установлен свой индивидуальный набор элементов криминалистической характеристики с определением их закономерных корреляционных связей и зависимостей. «Криминалистическая характеристика, как целое, как единый комплекс, приобретает практическое значение лишь в тех случаях, – как неоднократно писал Р.С. Белкин, – когда установлены корреляционные связи и зависимости между ее элементами, носящие закономерный характер и выраженные в количественных показателях». При этом, «данные об этих зависимостях могут служить основанием для построения типичных версий по конкретным делам»[27].

---

[26] См., например: Криминалистика: Учебник / Под ред. И.Ф. Герасимова, Л.Я. Драпкина. – М., 1994. – С. 330; Криминалистика: Учебник / Под ред. И.Ф. Пантелеева, Н.А. Селиванова. – М., 1993. – С. 31; *Возгрин И.А.* Указ. соч. – С. 27.

[27] *Белкин Р.С.* Курс криминалистики: В 3-х т. Т. 3: Криминалистические средства, приемы и рекомендации. – С. 316; см.: *Он же.* Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. – М., 2001. – С. 221-222.

Кратко рассмотрев общетеоретические вопросы и проанализировав суждения различных авторов относительно сущности и структуры криминалистической характеристики, ее роли в формировании частной методики расследования преступлений отдельных видов, перейдем к детальному исследованию структуры криминалистической характеристики преступлений, совершенных с использованием пластиковых карт и их реквизитов.

Анализ эмпирических источников показал, что в отличие от зарубежной юридической практики, имеющей на вооружении многочисленные работы, содержащие методические рекомендации по раскрытию, расследованию и предупреждению преступлений рассматриваемого вида, отечественная криминалистическая литература весьма скудна в освещении этих вопросов. Большая часть работ посвящена исследованию уголовно-правовых и криминологических характеристик преступлений, схожих по своим основным признакам с преступлениями выделенной категории, которые нашли свое отражение в трудах А.Н. Андреева, С.М. Астапкиной, А.Э. Жалинского, А.В. Козлова, Б.М. Леонтьева, Ю.И. Ляпунова, Е.Н. Максимовой, И.А. Наумова, А.С. Овчинского, М.Н. Панова, К.А. Смирнова, Н.И. Степанова, П.С. Яни и других. К различным аспектам раскрытия, расследования и предупреждения хищений, совершенных с использованием пластиковых карт, обращались С.В. Амплеев, Н.А. Анчабадзе, Д.К. Ахмадулин, В.Г. Баяхчев, В.Н. Довжук, А.М. Дьячков, С.Г. Евдокимов, С.Г. Еремин, Т.А. Казакбиев, И.И. Никитин, В.И. Отряхин, В.Ю. Рогозин, В.И. Рохлин, К.С. Скоромников, Н.Н. Сологуб, В.В. Улейчик, О.И. Цоколов, В.Н. Черкасов, Л.В. Шульга, Н.Г. Шурухнов и другие.

Судя по содержанию работ указанных авторов, одна из современных тенденций развития криминалистики по данному направлению состоит в некотором объединении различных категорий преступлений по двум основным признакам – по объекту (предмету) уголовно-правовой охраны и по орудию (средству) совершения преступления. Так, например, исследуя преступления в сфере экономики, как правило, рассматривают те из них, которые совершаются с использованием компьютерной информации либо ее носителей – пластиковых карт, а также иных средств электронно-вычислительной техники (далее – СВТ). В свою очередь, рассматривая преступления в сфере компьютерной информации, авторы невольно обращаются к исследованию преступлений в сфере экономики, поскольку в действительности типична совокупность их составов, нередко – идеальная. С криминалистических позиций объективно происходит условное объединение этих преступлений

в общие виды (группы). Причем анализ содержания литературы вопроса показывает следующую, представляющую научный интерес закономерность – одни составы преступлений (в нашем случае – хищения) являются основными, а другие (отмеченные во введении к настоящей работе) – факультативными. Не вдаваясь в полемику по поводу уголовно-правовой корректности данного положения, представляется, что оно вполне приемлемо и употребимо в силу относительной абстрактности рассматриваемой научной категории. Поэтому имеются основания полагать, что криминалистическая характеристика преступлений, совершенных с использованием пластиковых карт и их реквизитов, будет отличаться от других, уже известных криминалистической науке, и обладать определенной спецификой. С учетом имеющихся научных разработок попытаемся конкретизировать ее структуру и положить в основу соответствующей частной методики расследования.

В работах вышеперечисленных ученых-криминалистов приводятся различные точки зрения относительно сущности и структуры криминалистической характеристики преступлений различных видов, имеющих отношение к предмету настоящей работы. В связи с чем проанализируем отдельные из них.

Так, например, К.С. Скоромников выделяет следующие элементы криминалистической характеристики хищений денежных средств в банковских компьютерных системах и сетях, а именно: место и время совершения преступления; способ преступного посягательства; последствия преступления; объекты, поражаемые преступлениями; характеристика субъектов преступного посягательства; цели и мотивы совершения преступления; обстоятельства, способствовавшие совершению преступления[28]. По видимому, это положение приемлемо лишь в той части, в которой «последствия преступления и объекты, поражаемые преступлением», не выделяются в качестве самостоятельных элементов. В данном случае, видимо, правильнее говорить о типичных следах-отражениях применения тех или иных способов совершения преступления, рассматривая конкретные материальные объекты, «поражаемые» преступным деянием, именно в их контексте.

---

[28] См.: *Скоромников К.С.* Некоторые особенности расследования хищений денежных средств в банковских компьютерных системах и сетях // Расследование преступлений повышенной общественной опасности: Пособие для следователей / Под ред. проф. Н.А. Селиванова, канд. юрид. наук А.И. Дворкина. – М., 1998. – С. 386-401.

Оригинально, хотя и не бесспорно, суждение В.Ю. Рогозина. Он предлагает включить в состав криминалистической характеристики в качестве самостоятельного элемента, применительно к непосредственному предмету посягательства – компьютерной информации, типичные сведения о «внутренних» и «внешних» угрозах с одновременной дифференциацией субъектов преступления по тому же признаку. Если и допустимо так говорить, то лишь со значительной степенью условности и в аспекте других составляющих содержательную часть элементов криминалистической характеристики, а именно: обобщенных данных о личности вероятного преступника, типичных для данного вида преступлений; отдельных типичных обстоятельств совершения преступления, характеризующих особенности доступа к непосредственному предмету преступного посягательства (например, к чужому имуществу, кредитной или расчетной карте); орудий и средств преступления.

Учитывая вышеизложенное, возможно заключить, что **структура видовой криминалистической характеристики преступлений, совершенных с использованием пластиковых карт и их реквизитов, должна содержать следующие взаимосвязанные элементы:**

1. Характеристику типичной исходной криминалистически значимой информации, включая место и обстоятельства обнаружения преступления.

2. Систему данных о типичных способах подготовки, совершения и сокрытия преступлений в совокупности с типичными последствиями их применения.

3. Обобщенные данные о личности вероятных преступников и преступных групп.

4. Криминалистически значимые сведения о вероятном потерпевшем (физическом или юридическом лице).

5. Криминалистически значимые сведения о типичном предмете преступного посягательства (понятие, классификация, характеристика, условия и особенности охраны, особенности технологии производства и оборота, а также сведения о лицах, связанных с этими процессами).

6. Сведения о некоторых типичных обстоятельствах совершения преступления: месте, времени и обстановке.

7. Характеристику связи преступлений рассматриваемой категории с другими преступными посягательствами и отдельными действиями, не являющимися уголовно наказуемыми деяниями, но имеющими сходство с ними по некоторым объективным признакам.

8. Криминалистически значимые сведения о типичных для данного вида преступлений причинах и условиях, способствующих их совершению.

После детального исследования сущности понятия и структуры криминалистической характеристики преступлений выделенной категории представляется возможным перейти к рассмотрению вопросов, касающихся содержания ее основных элементов и определения закономерных корреляционных связей и зависимостей между ними.

§ 2. СОДЕРЖАНИЕ И ОСНОВНЫЕ ЭЛЕМЕНТЫ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ПЛАСТИКОВЫХ КАРТ И ИХ РЕКВИЗИТОВ

2.1. Понятие пластиковой карты как предмета и орудия совершения преступления

Как было подчеркнуто ранее, криминалистическая характеристика преступлений, совершенных с использованием пластиковых карт и их реквизитов, представляет собой динамичную систему описания их криминалистически значимых признаков, которые проявляются в особенностях способа, механизма и обстановки подготовки, совершения и сокрытия преступления. Она дает представление о преступном посягательстве, субъекте и потерпевшем, об иных обстоятельствах преступной деятельности, а также является основой для формирования методических рекомендаций, обеспечивающих успешное решение задач раскрытия, расследования и предупреждения преступлений выделенной категории.

Все элементы, составляющие данное понятие, органически связаны между собой. Формы связей различны между отдельными элементами, причем характер связи можно различать по степени детерминации, по содержанию, направленности, типу процессов и тому подобное. С точки зрения потребностей криминалистической науки наибольший интерес представляют выделение и изучение таких видов связей элементов характеристики, которые носят характер именно определенных закономерностей и опираются на данные обобщения следственной практики, на изученные статисти-

ческие совокупности уголовных дел и, одновременно, характеризуют степень жесткости такой связи[29]. При этом, однако, необходимо иметь в виду, что одни и те же элементы, их отдельные параметры, части, стороны и совокупности, информативные в криминалистическом отношении для одних групп и подгрупп исследуемой категории преступлений, оказываются неинформативными или слабо информативными в других группах и подгруппах. Все это не может не отражаться на содержательной стороне криминалистической характеристики преступлений рассматриваемого вида (группы)[30].

Принимая во внимание вышеизложенное, исследование элементов и содержательной стороны рассматриваемой научной категории проведем в последовательности, определяемой спецификой расследования данного вида преступлений, потребностями следственно-оперативной практики и исходя из частоты их встречаемости.

Анализ эмпирических источников показал, что квалификация хищений чужого имущества, как правило, не вызывает особых проблем у следователей и сотрудников подразделений по борьбе с экономическими преступлениями (БЭП). Одновременно с этим, квалификация таких преступлений, как: *изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов*; *в сфере компьютерной информации*; *незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну*, – вызывает значительные затруднения у следователей и дознавателей (соответственно – у 83, 91 и 94 %)[31]. Это приводит к тому, что преступления выделенного вида расследуются без учета их специфики лишь с использованием хорошо известных и отработанных методик имущественных преступлений (в 91 % случаев). Прямо подтверждают данное положение и результаты анкетирования сотрудников следственных подразделений органов внутренних дел – подавляющему большинству опрошенных респондентов (73 %) не известны те отдельные методические рекомендации по расследованию хищений, совершенных с использованием пластиковых карт, которые имеются в настоящее вре-

---

[29] См.: Криминалистика: Учебник / Под ред. В.А. Образцова. – М., 1995. – С. 47.

[30] См.: Криминалистическая характеристика преступлений: Сб. науч. трудов. – М., 1994. – С. 88.

[31] Здесь и далее по тексту работы, если не указано иное, используются результаты диссертационного исследования П.Б. Смагоринского (Криминалистическая характеристика хищений чужого имущества, совершенных с использованием пластиковых карт, и ее применение в следственной практике: Дис. … канд. юрид. наук. – Волгоград, 2000. – Приложения № 1-2).

мя[32], отчасти известны – 19 % и известны – всего лишь 8 % (10 человек из 123 опрошенных). В большинстве случаев квалификация по новым вышеуказанным составам преступлений отсутствует вообще. В итоге на стадии предварительного следствия в 41 % случаев производство по уголовному делу приостанавливается, из которых: в 78 % случаев – по причине неустановления лица, подлежащего привлечению в качестве обвиняемого, в 22 % – по причине неустановления его местопребывания; обвинительный приговор выносится лишь по 16 % уголовных дел, рассмотренных судом. Естественно, такое положение дел нельзя считать удовлетворительным.

Отмеченное ориентирует на определение понятия преступных посягательств рассматриваемой группы с криминалистических позиций и на более детальное исследование их уголовно-правовых аспектов. Подтверждая правильность такого научного подхода, Р.С. Белкин писал: «Мы глубоко убеждены в том, что в основе системы частных криминалистических методик должна лежать уголовно-правовая квалификация преступлений... ею определяется содержание предмета доказывания, т. е. в главных чертах круг тех обстоятельств, на установление которых и направлено расследование и которые оказывают заметное влияние на содержание частных криминалистических методик и всех их составляющих»[33]. В связи с этим представляется, что анализ понятия и некоторых уголовно-правовых признаков преступлений, совершенных с использованием пластиковых карт и их реквизитов, весьма существенен для разработки полноценной криминалистической характеристики.

Проведенное исследование показывает, что **под преступлением, совершенным с использованием пластиковой карты или ее реквизитов**, исключительно **с криминалистической точки зре-**

---

[32] См., например: *Довжук В.Н.* Организационные и методические особенности расследования мошенничеств с использованием кредитных карточек // Информационный бюллетень СК МВД России. – 1997. – № 3; *Скоромников К.С.* Некоторые особенности расследования хищений денежных средств в банковских компьютерных системах и сетях // Расследование преступлений повышенной общественной опасности: Пособие для следователей / Под ред. проф. Н.А. Селиванова, канд. юрид. наук А.И. Дворкина. – М., 1998. – С. 386-401; *Баяхчев В.Г., Улейчик В.В. и др.* Расследование хищений, совершаемых в кредитно-финансовой сфере с использованием электронных средств доступа (пластиковых карт): Метод. рекомендации // Информационный бюллетень СК МВД России. – 1999. – № 1; Расследование преступлений в сфере экономики: Руководство для следователей / Под общ. ред. И.Н. Кожевникова. – М., 1999.– Гл. XVIII.

[33] *Белкин Р.С.* Курс криминалистики: В 3-х т. Т. 3: Криминалистические средства, приемы и рекомендации. – С. 325.

ния и определенной степенью условности, **следует понимать виновно совершенное общественно опасное деяние, запрещенное Уголовным законом Российской Федерации под угрозой наказания, посягающее на общественные отношения в сфере создания, оборота и защиты пластиковых карт.** При этом *в качестве основного классифицирующего признака* принадлежности преступления к этой группе *выделяется использование пластиковой карты как предмета и (или) средства совершения преступления*. Видимо, данное положение нуждается в дополнительном пояснении.

Как не без основания полагают некоторые ученые-криминалисты, при отсутствии в исходной информации данных о предмете преступления трудно решить вопрос о возбуждении уголовного дела и квалификации содеянного. Отчасти, это обусловлено тем, что нередко деяния, которые, на первый взгляд, содержат, например, признаки хищения, на самом деле образуют состав иного преступления или их идеальную совокупность либо не содержат состава преступления вообще. В то же время преступники часто используют внешне законные операции в целях незаконного обогащения, скрывают корыстную направленность своих действий путем заключения целого ряда формальных сделок, перевода денежных средств на счета фирм, зарегистрированных на «подставных» лиц, конвертации наличных денег в безналичные (и наоборот), в ценные бумаги, валютные ценности, а также перевода за границу[34]. Поэтому *криминалистически значимые сведения о предмете посягательства входят в понятие соответствующей характеристики хищений чужого имущества.* Они находятся в корреляционной зависимости с типичными данными о месте хищения, об используемых при совершении преступления производственных, финансовых либо учетных операциях, о способах хищения, субъектах, характере корыстной заинтересованности преступников, а при определенных обстоятельствах – и о времени хищения. Это означает, что при наличии достоверных данных о предмете преступления легче установить другие элементы криминалистической характеристики[35].

С позиций уголовно-правовой науки, имущество представляет собой предмет хищения различной формы. Он всегда материален,

---

[34] См.: *Сологуб Н.М., Евдокимов С.Г., Данилова Н.А.* Хищения в сфере экономической деятельности: Механизм преступления и его выявление: Метод. пособие. – М., 2002. – С. 4.

[35] См.: *Сологуб Н.М., Рохлин В.И., Евдокимов С.Г.* Методика расследования, прокурорский надзор и особенности поддержания государственного обвинения по делам о хищениях чужого имущества. – СПб., 1997. – С. 4-5.

является частью внешнего мира и, как всякая вещь, обладает некими натуральными физическими параметрами (весом, объемом, числом, количеством, и т. д.) – вещными свойствами. Вместе с этим следует подчеркнуть, что предметом хищения может быть только та вещь, которая имеет определенную экономическую ценность. Этому условию удовлетворяют лишь товарно-материальные ценности в любом состоянии и виде, а также деньги (валюта), валютные ценности, ценные бумаги и иные платежные документы, в числе которых ***пластиковые кредитные либо расчетные карты***, являющиеся эквивалентом стоимости. Как особый товар, они выражают цену других видов имущества и могут являться предметом хищения. Поскольку они имеют непосредственное отношение к теме настоящей работы, исследуем их подробно.

В соответствии со ст. 142 Гражданского кодекса Российской Федерации (ГК РФ) ***ценной бумагой признается документ, удостоверяющий с соблюдением установленной формы и обязательных реквизитов имущественные права, осуществление или передача которых возможны только при его предъявлении.*** При этом ***документ – это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать***[36]***.*** С передачей ценной бумаги физическому или юридическому лицу к нему переходят все удостоверяемые ею права в совокупности. *В случаях, предусмотренных законом или в установленном им порядке, для осуществления и передачи прав, удостоверенных ценной бумагой, достаточно доказательств их закрепления* ***в специальном компьютеризованном реестре.*** К ценным бумагам относятся: государственная облигация, облигация, вексель, чек, депозитный и сберегательный сертификаты, банковская сберегательная книжка на предъявителя, коносамент, акция, приватизационные ценные бумаги и другие документы, которые законами о ценных бумагах или в установленном ими порядке отнесены к числу ценных бумаг (ст. 143 ГК РФ).

Специалисты не без основания отмечают, что одним из основных свойств ценных бумаг, которое делает их для преступников заманчивым предметом хищения и сближает в этом смысле с деньгами (валютой), является возможность обмена ценной бумаги на наличные деньги в различных формах, например путем погашения,

---

[36] См.: Закон Российской Федерации от 20.02.95 г. № 24-ФЗ «Об информации, информатизации и защите информации». – Ст. 2.

купли-продажи, обмена, возврата эмитенту, переуступки и других[37]. При этом **эмитент** – *юридическое лицо или органы исполнительной власти либо органы местного самоуправления, несущие от своего имени обязательства перед владельцами ценных бумаг по осуществлению прав, закрепленных ими*[38].

Ценные бумаги используются также как средство безналичных расчетов между сторонами при совершении сделок, являются предметом залога, накапливаются и хранятся в банках, принося доход (дивиденты), передаются по наследству, служат подарком, т. е. выступают в роли определенного эквивалента стоимости, которая определяется номиналом либо рыночной ценой[39].

С криминалистических позиций важно подчеркнуть то обстоятельство, что всегда существует корреляционная связь между ценной бумагой – предметом и (или) средством совершения преступлений выделенного нами вида – и потерпевшим (или субъектом). Она проявляется в том, что во многих случаях достаточно легко можно установить тех лиц, которым по закону принадлежат имущественные права на нее, и тех, кто может использовать ее по назначению. Права, удостоверенные ценной бумагой, могут принадлежать лишь определенному кругу лиц, а именно:

1) предъявителю ценной бумаги, если это ***ценная бумага на предъявителя***;

2) названному в ценной бумаге лицу – ***именная ценная бумага***;

3) названному в ценной бумаге лицу, которое может само осуществить эти права или назначить своим распоряжением (приказом) другое управомоченное лицо, если это ***ордерная ценная бумага*** (ч. 1 ст. 145 ГК РФ).

Особое значение имеют ценные бумаги на предъявителя, поскольку для передачи другому лицу прав, удостоверенных такой бумагой, достаточно просто вручить ее этому лицу (ч. 1 ст. 146 ГК

---

[37] См., например: *Егоршин В.М., Александров А.И., Исмагилов Р.Ф.* Экономическая безопасность как составляющая национальной безопасности России // МВД России – 200 лет: Сб. науч. трудов. Ч. 2. – СПб., 1998. – С. 74-76; *Колесников В.В., Поздышев А.М.* Криминологическое состояние банковской сферы и компьютерные преступления // Компьютерная преступность: состояние, тенденции и превентивные меры ее профилактики: Материалы междунар. науч.-практ. конф. Ч. 2. / Под ред. В.П. Сальникова. – СПб., 1999. – С. 133.

[38] См.: Закон Российской Федерации от 22.04.96 г. № 39-ФЗ «О рынке ценных бумаг». – Ст. 2.

[39] См.: *Ляпунов Ю.И., Пушкин А.В.* Общее понятие хищения чужого имущества // Уголовное право. Особенная часть: Учебник / Под ред. проф. Н.И. Ветрова, проф. Ю.И. Ляпунова. – М., 1998. – С. 208-209.

РФ). При этом, в отличие от других видов ценных бумаг, переход прав на ценные бумаги на предъявителя и осуществление закрепленных в них прав не требуют идентификации владельца[40]. Данным «обезличенным» свойством бумаг рассматриваемой категории активно пользуются криминальные элементы в своих корыстных целях. Этим же свойством обусловлен и специальный порядок наложения ареста на них: **ценные бумаги на предъявителя не подлежат аресту, если они находятся у добросовестного приобретателя** (ч. 2. ст. 116 УПК РФ) – лица, которое приобрело ценные бумаги, произвело их оплату и в момент приобретения не знало и не могло знать о правах третьих лиц на эти ценные бумаги, если не доказано иное[41]. Примечательно, что в соответствии с требованиями ч. 3 ст. 116 УПК РФ в протоколе о наложении ареста на ценные бумаги всегда должны быть отражены следующие фактические данные, а именно:

1) общее количество ценных бумаг, их вид, категория (тип) или серия;

2) номинальная стоимость;

3) государственный регистрационный номер – цифровой (буквенный, знаковый) код, который идентифицирует конкретный выпуск эмиссионных ценных бумаг;

4) сведения об эмитенте – юридическом лице, несущим от своего имени обязательства перед владельцами ценных бумаг по осуществлению прав, закрепленных ими, или о лицах, их выдавших либо осуществивших учет прав их владельца, а также о месте производства такого учета;

5) сведения о документе, удостоверяющем право собственности на ценные бумаги[42].

В условиях широкой компьютеризации рыночной экономики России, неразрывно связанной с мировой экономической системой, на рынке ценных бумаг все в больших масштабах используются ***бездокументарные ценные бумаги*** – ценные бумаги, владелец которых устанавливается на основании записи в системе ведения реестра владельцев ценных бумаг или, в случае депонирования ценных бумаг, на основании записи по счету депо[43]. Законодательство Российской

---

[40] См.: Закон Российской Федерации от 22.04.96 г. № 39-ФЗ «О рынке ценных бумаг». – Ст. 2.

[41] См.: Там же.

[42] В большинстве случаев следы незаконного использования кредитных либо расчетных пластиковых карт или иных документов обнаруживаются при анализе этих и других первичных учетных документов.

[43] См.: Указ. Закон. – Ст. 2.

Федерации ***разрешает лицу****, получившему специальную лицензию,* ***производить фиксацию имущественных прав***, закрепляемых именной или ордерной ценной бумагой, в том числе находящейся в бездокументарной форме, ***с помощью средств электронно-вычислительной техники.*** При этом лицо, осуществившее фиксацию права в бездокументарной форме, несет ответственность за сохранность официальных записей, обеспечение их конфиденциальности, представление правильных данных о таких записях, совершение официальных записей о проведенных операциях (ст. 149 ГК РФ). ***Юридическая сила документа***, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, ***может подтверждаться электронной цифровой подписью*** (ЭЦП*) – аналогом собственноручной подписи.* Ее юридическая сила признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования. Право удостоверять идентичность ЭЦП осуществляется на основании лицензии, порядок выдачи которой определяется законодательством Российской Федерации[44]. Базовым здесь является Закон Российской Федерации от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи». Его действие распространяется на отношения, возникающие при совершении гражданско-правовых сделок, а также в других предусмотренных законодательством Российской Федерации случаях, когда ЭЦП с юридической точки зрения признается равнозначной собственноручной подписи в обычных – бумажных документах. Так, например, Гражданский кодекс Российской Федерации разрешает применять для удостоверения прав распоряжения денежными суммами, находящимися на счете, электронные средства платежа и другие документы с использованием в них аналогов собственноручной подписи, кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом (ч. 2 ст. 160; ч. 3 ст. 434; ч. 3 ст. 847). ***Одним из таких электронных средств или документов является пластиковая карта.*** В выделенном Федеральном законе содержится ряд следующих основополагающих правовых определений, понятие которых позволяет более полно раскрыть содержание рассматриваемых элементов криминалистической характеристики.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

---

[44] См.: Закон Российской Федерации от 20.02.95 г. № 24-ФЗ «Об информации, информатизации и защите информации». – Ст. 5, чч. 2-4.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

- создание электронной цифровой подписи в электронном документе с использованием закрытого ключа ЭЦП;
- подтверждение с использованием открытого ключа ЭЦП подлинности электронной цифровой подписи в электронном документе;
- создание закрытых и открытых ключей электронных цифровых подписей.

Сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи (***персональный идентификационный номер, состоящий из 4–8 знаков, называемый ПИН-кодом***).

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе (***номер, состоящий из 12–19-ти знаков, открыто***

записываемый на подложку пластиковой карты и (или) в ее электронную память).

Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ ЭЦП и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной подписью электронном документе.

Пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

1) сертификат ключа подписи, относящийся к электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

2) подтверждена подлинность электронной цифровой подписи в электронном документе;

3) электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи[45].

Продолжая исследование вопроса, следует акцентировать внимание на том обстоятельстве, что *к особой разновидности ценных бумаг, удостоверяющих определенные имущественные права, относятся* и так называемые ***«денежные суррогаты»*** или ***«суррогаты валюты»*** – документы, которые в строго ограниченных пределах выполняют функцию средства безналичного платежа (в соответствии со ст. 861 и 862 ГК РФ) за оказание гражданину возмездной услуги (транспортной, телефонной и иной), носящей материальный характер. Рассматриваемая разновидность ценных бумаг, имея номинальную стоимость, равную цене услуги, фактически заменяет собой обычные деньги (валюту) как средство платежа[46]. В соответствии с Указанием Центрального банка России от 07.06.2000 г. № 799-У, **платежная (расчетная) карта –** *это средство для совершения сделок по приобретению товаров (услуг) и (или) по получению наличных денежных средств, расчеты по которым производятся согласно условиям договора между эмитентом карты и лицом, их использующим;* ***банковская карта*** *– это платежная (расчетная) карта, эмитентом которой является кредитная организация.* При этом важен тот факт, что платежные (расчетные) карты по приобретению услуг могут распространяться эмитентом путем их розничной продажи пользователям. Розничная продажа таких карт, как правило, осуществляется двумя следующими способами:

1) ч е л о в е к о м (продавцом). При осуществлении такой операции договор их розничной купли-продажи считается заключенным в надлежащей форме ***с момента выдачи продавцом покупателю кассового или товарного чека или иного документа, подтверждающего оплату*** пластиковой расчетной карты как товара (ст. 493 ГК РФ).

2) а в т о м а т о м[47]. В этом случае договор розничной купли-продажи считается заключенным с момента совершения покупателем действий, необходимых для получения товара (ст. 498 ГК РФ).

---

[45] Подробнее см.: Закон Российской Федерации от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи». – Ст. 3-4.

[46] См.: Комментарий к Уголовному кодексу Российской Федерации. – 2-е изд., изм. и доп. / Под общ. ред. проф. Ю.И. Скуратова, В.М. Лебедева. – М., 1998. – С. 334-335.

[47] **Автомат** – самодействующее техническое устройство (аппарат, машина), производящее работу по заданной программе без непосредственного участия человека. –

Так, например, начиная с 2000 года Министерство путей сообщения Российской Федерации (МПС РФ) приступило к введению в оборот унифицированной пластиковой смарт-карты, которая используется в качестве универсального именного платежно-расчетного документа для безналичной оплаты любого вида услуг, предоставляемых отечественным железнодорожным транспортом. В их числе: проезд на пригородных поездах и в метро; пользование автоматическими телефонами, торговыми автоматами, справочными терминалами и камерами хранения, расположенными в вагонах подвижного состава и на станциях. Контроль за санкционированностью использования данного документа осуществляется комбинированным способом, а именно:

1) а в т о м а т о м – с помощью автоматизированного контрольно-пропускного пункта (КПП), турникета и иного терминального устройства, оборудованного считывателями индивидуального штрихкода и компьютерной информации, содержащейся в интегральной микросхеме памяти (электронном реквизите) карты;

2) к о н т р о л е р о м МПС РФ (работником) – с помощью специального мобильного (ручного) или стационарного считывателя – ридера, который, при помещении в него пластиковой карты, отображает на своем дисплее фамилию и имя держателя, ее номер и срок действия.

В перспективе у владельцев таких универсальных «железнодорожных» карт появится возможность использовать их для покупок в привокзальных магазинах, киосках и ресторанах, а также для оплаты бытовых услуг, например за пользование залом ожидания, комнатой матери и ребенка, санузлом, прачечной, парикмахерской и других[48].

Учитывая отсутствие в следственной практике единообразия в уголовно-правовой оценке корыстного безвозмездного изъятия рассматриваемых предметов преступного посягательства, нам представляется правильным использование для решения этого вопроса Постановления Пленума Верховного Суда РСФСР[49], в котором специально разъяснено следующее:

См.: Словарь русского языка: В 4-х т. Т. 1 / АН СССР, Ин-т рус. яз.; Под ред. А.П. Евгеньевой. – 3-е изд., стереотип. – М., 1985–1988. – С. 22.

[48] Подробнее см.: *Цымбал Е.* Новые технологии на железных дорогах // Комсомольская правда. – 1999. – 3 дек. – С. 10.

[49] Постановление Пленума Верховного Суда РСФСР от 23.12.80 г. № 6 «О практике применения судами РСФСР законодательства при рассмотрении дел о хищениях на транспорте» // БВС РСФСР. – 1981. – № 4. – С. 5-8 (пп. 5 и 6).

1. Действия лиц, совершивших хищение талонов на горючие и смазочные материалы, которые непосредственно дают право на получение имущества, а равно хищение абонементных книжек, проездных и единых билетов на право проезда в метро и на других видах городского транспорта, находящихся в обращении как документы, удостоверяющие оплату услуг, независимо от использования похищенных знаков по назначению или сбыта их другим лицам, должны квалифицироваться как оконченное преступление.

2. Действия лиц, похитивших билеты для проезда на железнодорожном, воздушном, водном и автомобильном транспорте или другие знаки, которые могут быть использованы по назначению лишь после внесения в них дополнительных данных (заполнение текста, компостирование и т. п.), с целью последующей реализации и присвоения вырученных от их продажи средств, могут квалифицироваться как приготовление к хищению, а в случаях частичной или полной реализации похищенных документов, соответственно, как покушение либо оконченное преступление. В этих случаях предметом преступления будут являться деньги, полученные от их продажи третьим лицам.

3. В случаях подделки похищенных билетов и предъявления их транспортной организации для оплаты (возврата денег) под любым предлогом либо сбыта (продажи) таких поддельных документов гражданам, действия виновных должны квалифицироваться как подделка документов и мошенничество.

Изложенное оптимально подходит к раскрытию признаков изготовления или сбыта поддельных кредитных либо расчетных пластиковых карт и иных платежных документов (ст. 187 УК РФ). Стоит, однако, отметить, что изготовление указанных документов будет подпадать под признаки рассматриваемой статьи, видимо, лишь тогда, когда будет доказано, что эти действия были совершены исключительно с целью сбыта поддельной кредитной либо расчетной пластиковой карты или иного платежного документа. При этом *под изготовлением необходимо понимать как частичную их подделку* (фальсификацию отдельных реквизитов), *так и полное их изготовление*, когда обеспечивается их существенное сходство с подлинными по ряду признаков – по материалу подложки и отдельных реквизитов, форме, цвету, содержанию реквизитов и другим.

Следует также согласиться с утверждением о том, что сбыт поддельной карты следует расценивать как хищение чужого иму-

щества в форме мошенничества, где в роли потерпевшего выступает приобретатель карты[50].

Анализ материалов уголовных дел о хищениях, совершенных с использованием пластиковых карт, проведенный П.Б. Смагоринским показывает, что в 61 % случаев ***предметом преступного посягательства*** были деньги (61 % – безналичные, 39 % – наличные), в 50 % – товары (продукты) и иное имущество, в 33 % – пластиковые карты как особая разновидность ценной бумаги, в 12 % – нефтепродукты (бензин), в 4 % – охраняемая законом компьютерная информация (персональные данные и сведения, составляющие коммерческую или банковскую тайну), в 3 % – автомототранспорт. При этом в качестве ***орудия совершения преступления*** чаще всего использовались: пластиковые карты различных видов и назначения (в 87 % случаев); ЭВМ, программы для ЭВМ[51] и иные СВТ (69 %); поддельные бухгалтерские документы (61 %); принтеры (51 %); поддельные документы, удостоверяющие личность держателя карты (паспорт, удостоверение, водительские права и другие) – в 23 % случаев; механические устройства, материалы и инструменты, используемые в целях подделки пластиковых карт и документов (22 %).

С научной точки зрения из международной практики борьбы с преступлениями рассматриваемой категории интересны следующие аналитические данные: в зарубежных странах *с помощью утраченных и похищенных пластиковых карт* совершается 75 % имущественных преступлений, *поддельными картами* – 21 %, *с использованием поддельных слипов* – 3 %, иными орудиями – 1 %[52].

С учетом вышеизложенного, представляется возможным заключить следующее:

1. Чужое имущество как предмет хищения – это вещи, деньги (валюта), валютные ценности, ценные бумаги и другие предметы материального мира, обладающие определенной стоимостью, которые включены в экономический оборот и по поводу которых существуют отношения собственности, нарушаемые преступлением.

---

[50] См.: Комментарий к Уголовному кодексу Российской Федерации / Под ред. проф. Н.Ф. Кузнецовой. – М., 1998.– С. 443.

[51] **Программа для ЭВМ** – это объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата. – См.: Ст. 1 Закона Российской Федерации от 23.09.92 г. № 3523-1 «О правовой охране программ для электронно-вычислительных машин и баз данных».

[52] См.: *Charles H. McCaghy*. Computer Crime // Crime in american society. – N.Y., 1980. – P. 223.

2. Кредитные либо расчетные пластиковые карты являются разновидностью ценных бумаг и могут быть предметом имущественного преступления.

3. Пластиковые карты как документы являются **средством** совершения сделок по приобретению товаров (услуг) и (или) по получению наличных денежных средств, а также санкционированного доступа к охраняемому имуществу, в том числе к охраняемой законом (конфиденциальной) компьютерной информации. Это свойство обусловливает их использование в качестве орудия совершения преступления.

В связи с тем, что в настоящее время в отечественной юридической науке все еще не существует сколь-нибудь четкого определения понятия пластиковой карты как предмета либо средства совершения преступления, дискутируются различные точки зрения по их криминалистической классификации, выскажем собственное суждение по этим вопросам.

Сложность в формулировках данных понятий существует, скорее всего, по следующим причинам:

1) отсутствие единого нормативно-правового акта, определяющего понятие пластиковой карты как юридического документа, находящегося в особой (нестандартной) форме, и регламентирующего процесс его оборота (обращения) и (или) эмиссии в товарно-денежных и иных общественных отношениях;

2) конструктивная, содержательная и функциональная неоднородность пластиковых карт.

Косвенно подтверждают эти положения и результаты проведенного П.Б.Смагоринским исследования. Так, большинство (59 %) опрошенных им сотрудников следственных подразделений ОВД затруднились ответить на вопрос анкеты относительно определения содержания понятия пластиковой карты, а из ответивших респондентов (41 %) определили ее как материальный носитель информации (86 %), индивидуальный платежно-расчетный инструмент (83 %), чужое имущество (53 %), машинный носитель информации (34 %), «ключ доступа» к охраняемому имуществу (17 %), одна из форм машинного (электронного) документа (8 %).

По определению Современного экономического словаря, *под кредитной либо иной расчетной картой понимается именной платежно-расчетный документ в виде пластиковой карты*, выдаваемый банком своим вкладчикам *для безналичной оплаты ими товаров и услуг в розничной торговой сети, снабженной компь-*

ютерными устройствами, передающими запрос на оплату товара в банк[53].

В свою очередь, в Толковом словаре по информатике мы находим следующее понятие пластиковой карты – это «*физический носитель машинных данных и команд, выполненный в форме прямоугольной пластины*»[54].

Исследователи в области уголовного права едины в том, что рассматривают пластиковую карту в узком ракурсе платежного документа, но расходятся во мнениях относительно отнесения ее к разряду ценной бумаги. Так, по мнению одних авторов, пластиковая карта не является ценной бумагой, но обладает ее свойствами удостоверять, устанавливать или предоставлять имущественные права либо удостоверять или устанавливать такие же обязанности[55], по мнению других, это обезличенное расчетное средство платежа, которое заменяет собой обычные деньги, является суррогатом валюты и относится к особой разновидности ценных бумаг, удостоверяющих определенные имущественные права[56].

Как было указано ранее, в соответствии с законодательством Российской Федерации пластиковая карта может также использоваться как средство удостоверения электронного документа, права распоряжения бездокументарными ценными бумагами и денежными средствами, находящимися на банковском счете (банковская карта).

С криминалистических позиций Н.А.Анчабадзе полагал, что пластиковая карта является средством «удостоверения юридического факта, который может нести как определенные права, так и обязанности»[57]. Проведя собственное исследование вопроса, он пришел к важному выводу о том, что «**реквизиты пластиковой карты подпадают под понятие электронного документа**»[58].

---

[53] См.: *Райзберг Б.А., Лозовский Л.Ш., Стародубцева Е.Б.* Современный экономический словарь. – М., 1997. – С. 167.

[54] *Першиков В.И., Савинков В.М.* Толковый словарь по информатике. – М., 1991. – С. 137.

[55] См.: Комментарий к Уголовному кодексу Российской Федерации / Под ред. проф. Н.Ф. Кузнецовой. – М., 1998.– С. 443.

[56] См.: Комментарий к Уголовному кодексу Российской Федерации. – 2-е изд., изм. и доп. / Под общ. ред. проф. Ю.И. Скуратова, В.М. Лебедева. – М., 1998. – С. 334-335.

[57] *Анчабадзе Н.А.* Организационно-правовые и криминалистические вопросы предотвращения хищений, совершаемых в финансовой сфере с использованием пластиковых карточек, мошенническим путем. – Волгоград, 2002. – С. 10.

[58] Там же. – С. 12.

Более определенного и правильного взгляда в этом вопросе придерживается Г.С. Панова, считающая, что *пластиковая карта*[59] – *это обобщающий термин, который обозначает все виды карт, различных как по назначению, набору оказываемых с их помощью услуг, так и по своим техническим возможностям и организациям, их выпускающим.* «Важнейшая особенность всех пластиковых карт независимо от степени их совершенства состоит в том, – указывает она далее, – что на них хранится определенный набор информации, используемый в различных прикладных программах для ЭВМ (СВТ). Таким образом, пластиковая карта может служить пропуском в здание, средством доступа к компьютеру и компьютерной информации, водительским удостоверением, использоваться для оплаты телефонных переговоров и т. д. В сфере денежного обращения пластиковые карты являются одним из прогрессивных средств организации безналичных расчетов»[60]. Существуют и другие точки зрения по этому вопросу. Однако ни одно из них в полной мере не отражает всех компонентов данного понятия, которые имеются в действительности.

С учетом вышеуказанного, исходя из анализа научных работ и публикаций отечественных и зарубежных исследователей по рассматриваемой проблематике, обобщенных данных следственной практики, синтезируя имеющиеся сведения, логично заключить следующее:

1. С криминалистических позиций ***под картой целесообразнее всего понимать документ, выполненный на основе металла, бумаги или полимерного (синтетического) материала – пластика стандартной прямоугольной формы, хотя бы один из реквизитов которого находится в форме, доступной восприятию средствами электронно-вычислительной техники и электросвязи.*** В своей части это определение полностью удовлетворяет общеправовому понятию документа – зафиксированной на материальном носителе информации с реквизитами, позволяющими идентифицировать эту информацию[61]. Из этого четко усматриваются два основных юридических признака документа:

---

[59] Далее по тексту настоящей работы термин «пластиковая карта» будет использоваться условно, независимо от вида материала, из которого изготовлена ее подложка.

[60] *Панова Г.С.* Новые банковские продукты и услуги // Банковское дело: Учебник / Под ред. проф. О.И. Лаврушина. – М., 1999. – С. 517.

[61] См.: Закон Российской Федерации от 20.02.95 г. № 24-ФЗ «Об информации, информатизации и защите информации». – Ст. 2.

а) материальный носитель, на котором зафиксирована (отражена) информация;

б) наличие определенных реквизитов, позволяющих идентифицировать информацию.

2. С уголовно-процессуальной точки зрения в понятие карты мы вкладываем содержание понятия документа, данное Л.М. Карнеевой, а именно: *документом в уголовном процессе является материальный носитель информации, на котором должностное лицо или гражданин зафиксировали в установленном порядке сведения об обстоятельствах, имеющих значение для дела, в письменной, фотографической, электронной или иной форме с целью их сохранения и последующего использования в раскрытии и расследовании преступления*[62]. Таким образом, ***карта будет являться доказательством***, если изложенные в ней сведения имеют значение для установления обстоятельств, подлежащих доказыванию по уголовному делу (ст. 84 УПК РФ), и ***вещественным доказательством*** в случае, когда она служила орудием преступления или сохранила на себе следы преступления, была объектом преступных действий, а также может служить средством для обнаружения преступления и установления обстоятельств уголовного дела (ст. 81 УПК РФ). Определив содержание понятия пластиковой карты как специфичного объекта криминалистического исследования, сосредоточим внимание на изучении ее признаков.

Исходя из предложенного криминалистического определения видно, что общим классифицирующим основанием данной группы объектов будет являться совокупное наличие у них следующих признаков:

1) **машинописного документа** – письменного документа, при создании которого знак письма наносят техническими средствами;

2) **документа на машинном носителе** – документа, созданного с использованием носителей и способов записи, обеспечивающих обработку его информации электронной вычислительной машиной (ЭВМ)[63].

Следовательно, любая пластиковая карта как предмет или средство совершения преступления рассматриваемой категории обяза-

---

[62] Подробнее см.: *Карнеева Л.М.* Доказательства и доказывание в уголовном процессе. – М., 1994. – С. 43.

[63] См.: Государственный стандарт Российской Федерации ГОСТ Р 51141-98 «Делопроизводство и архивное дело. Термины и определения» (введен в действие с 01.01.99 г. Постановлением Госстандарта России от 27.02.98 г. № 28). – П. 2.1.16 и 2.1.17.

тельно должна содержать какую-либо компьютерную информацию и иметь в своем конструктивном исполнении соответствующее техническое устройство для того, чтобы эта информация была доступна восприятию ЭВМ, системой ЭВМ, их сетью или иным средством электронно-вычислительной техники. Сделаем ударение на том, что **под компьютерной информацией понимаются** *сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, находящиеся на машинном носителе, в ЭВМ, системе ЭВМ или их сети*[64]. Иными словами, это ***сведения, циркулирующие в электронной вычислительной среде, зафиксированные на материальном носителе в форме, доступной восприятию ЭВМ, или передающиеся по каналам электросвязи посредством электромагнитных сигналов из одной ЭВМ в другую, из ЭВМ на периферийное устройство, либо на управляющий датчик оборудования***. Одновременно с указанным, пластиковая карта – это документ. Поэтому, как любой иной документ, по своим признакам (параметрам) она должна отвечать определенным требованиям – стандартам. Рассмотрим их.

Исследуя историю вопроса, следует отметить, что впервые в качестве документа карты стали использоваться уже в 1914 г. в США. Некоторые магазины, чтобы «привязать к себе» побольше богатых клиентов, стали выдавать им специальные бумажные карты. В 1928 г. бостонской компанией Farrington Manufacturing были выпущены первые металлические пластинки, на которых с помощью специального штампа выдавливались (эмбоссировались) адрес и фамилия кредитоспособного клиента. Продавец вкладывал такую пластинку в специальную машинку, называемую импринтером, и буквы, выдавленные на ней, отпечатывались на торговом чеке[65]. Металлическая карта в данном случае использовалась как клише. Этот метод был сохранен, и в настоящее время он реализуется в современных пластиковых картах. Пластиковые карты как документы в своем развитии прошли длительный путь, занявший многие десятилетия. В процессе формирования технологий их оборота (обращения) в 1986 г. была создана Международная организация стандартов ISO (International Standarts Organisation). По мере совершенствования компьютерных технологий она разрабатывает определенные требования и правила, предъявляемые к внешнему

---

[64] Данное определение получено из анализа содержания понятий, изложенных в ст. 2 Закона Российской Федерации от 20.02.95 г. № 24-ФЗ «Об информации, информатизации и защите информации» и ч. 1 ст. 272 УК РФ.

[65] См.: Пластиковые карты. – 4-е изд., перераб. и доп. – М., 2002. – С. 5.

виду карты, материалу и размеру подложки, наличию обязательных реквизитов, форме и формату их записи, а также техническим устройствам, обеспечивающим их оборот. Как известно, **стандартом называется** *нормативно-технический документ, регламентирующий требования и правила к изделиям, технологическим процессам и принятый соответствующей компетентной организацией в качестве официального документа*[66]. На основании этих документов государства – члены ISO разрабатывают и утверждают свои собственные национальные стандарты, дублируя в них основные требования ISO. Примечательно, что на конец 1998 г. членами данной организации были более 200 стран, включая Россию[67].

В соответствии с российским стандартом ГОСТ Р 50809 «Нумерация и метрологическое обеспечение идентификационных карт для финансовых расчетов» все карты должны иметь следующие геометрические параметры:

- ширина – 85,595 ± 0,125 мм;
- высота – 53,975 ± 0,055 мм;
- толщина – 0,76 ± 0,08 мм;
- радиус окружности в углах – 3,18 ± 0,125 мм[68].

Этот отечественный ГОСТ был разработан на основе стандарта ISO 7810 «Карты идентификационные. Физические характеристики» (1985 г.), который предусматривает 3 формата карт, один из которых – ID-1 – соответствует указанным линейным размерам.

Проведенный анализ содержания карт различных видов показывает их сходство с обычными бумажными документами ***по составу обязательных реквизитов*** – совокупности установленных обозначений, позволяющих идентифицировать документ[69]. Такими ***общими (постоянными) обозначениями для пластиковых карт являются:*** стандартная пластина (подложка документа); название вида карты; наименование организации – производителя заготовки карты (изготовителя бланка документа), ее эмблема или товарный знак (знак обслуживания); название **эмитента** – органи-

---

[66] См.: *Першиков В.И., Савинков В.М.* Толковый словарь по информатике. – М., 1991. – С. 382.

[67] См.: *Панова Г.С.* Новые банковские продукты и услуги // Банковское дело: Учебник / Под ред. проф. О.И. Лаврушина. – М., 1999. – С. 517.

[68] См.: Пластиковые карты. – 4-е изд. перераб. и доп. – М., 2002. – С. 46.

[69] Состав реквизитов бумажных документов см.: Государственный стандарт Российской Федерации ГОСТ Р 6.30-97 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов» (введен в действие с 01.07.98 г. Постановлением Госстандарта России от 31.07.97 г. № 273; с изм. от 21.01.2000 г. № 9-ст). – П. 2.1.

зации, которая нанесла индивидуальные недостающие реквизиты на заготовку карты (произвела ее персонификацию) и выдала ее для использования, ее эмблема или знак обслуживания; регистрационный номер карты; срок действия; машинный носитель информации[70]; средства защиты от подделки. ***В качестве дополнительных (переменных) реквизитов используются:*** материал подложки; вид машинного носителя или их комбинация; формат записи данных на машинный носитель; фоновый цвет и (или) рисунок карты; код эмитента; идентификатор электронной копии документа; персональные данные о владельце (держателе) карты (для юридического лица – его название, для физического лица – фамилия и имя, собственноручная подпись, фотография, отпечаток пальца руки, половая принадлежность, индивидуальный рисунок (знак, символ) или фотография тотема).

2.2. Криминалистическая классификация пластиковых карт

С учетом сведений, характеризующих пластиковую карту как предмет и орудие совершения преступления, а также в целях придания системности настоящему исследованию, классифицируем пластиковые карты по ряду следующих оснований[71].

По материалу подложки

1. Пластиковые – большинство используемых в настоящее время карт изготавливают из полимерного (синтетического) материала – поливинилхлорида (ПВХ), полихлорвинила (ПХВ) или ацетат поливинилхлорида (АПВХ), позволяющего в соответствии со стандартом ISO 7810 выполнять рельефную и (или) обычную печать знаков и графических изображений. Химическая формула и физические свойства пластика напрямую зависят от способа записи компьютерной информации на карту. В свою очередь, способ записи предопределяет тот или иной информационно-несущий материал, который в качестве отдельного реквизита является машинным носителем такой информации в рассматриваемом документе.

---

[70] Под «**машинным носителем информации** (**МНИ**)» понимается любое техническое устройство либо физическое поле, предназначенное для фиксации, хранения, накопления, преобразования и передачи компьютерной информации.

[71] Известно, что частные криминалистические классификации, помимо своего гносеологического значения, как одного из средств познания, являются существенной частью криминалистической систематики. Они также представляют собой одно из средств практической деятельности, которое разрабатывается криминалистикой специально для нужд борьбы с преступностью.

2. Бумажные (картонные). Карты этой категории находятся на втором месте по объему оборота. Они дешевы в изготовлении и не долговечны. Как правило, это документы одноразового или краткосрочного пользования: проездные билеты на различные виды пассажирского транспорта (автомобильного, железнодорожного, водного и воздушного); пропуска на охраняемые объекты и в хранилища; удостоверительные (идентификационные) документы личности (бэйджики участников конференций, деловых встреч, совещаний и других собраний). Для увеличения срока службы таких карт их подложка в некоторых случаях покрывается прозрачной полимерной пленкой методом напыления или ламинирования.

3. Металлические – наименьшее количество карт, находящихся в настоящее время в обороте. Они изготавливаются из тонколистового упругого композиционного металла. За счет простоты их производства и долговечности подложки, эти документы используются в тех технологических процессах, в которых необходима многократность и частота их применения при сравнительно больших механических нагрузках. В качестве примера можно привести так называемые «телефонные (таксофонные)» и «парковочные карты».

По способу фиксации информации и виду машинного носителя

1. Графические – карты, информация на которых зафиксирована в виде какого-либо объекта (или их группы), изображение которого получено посредством рисования линий, штрихов и светотени с помощью красителей и соответствующих технических средств (методы печати изображений и знаков на карту подробно описываются в следующей главе). Графическое изображение является самой ранней и простой формой записи информации на карту. Этот способ используют для оформления следующих реквизитов: эмблемы или товарного знака (знака обслуживания) организации – изготовителя заготовки карты (бланка документа); эмблемы или знака обслуживания организации-эмитента; фонового цвета и (или) рисунка карты, используемых в качестве средства защиты от подделки и (или) опознавания вида документа в локальной системе документооборота.

2. Машинописные – информация выражена в виде письма (текста), знаки которого нанесены на карту красителем с помощью технических печатных средств. Данным способом оформляется название карты, производителя заготовки и эмитента, регистрационный номер и срок ее действия, отдельные элементы защиты от подделки, код эмитента, номинал, персональные данные о держателе кар-

ты (для юридического лица – его название, для физического лица – фамилия и имя) и другие реквизиты.

3. Эмбоссированные – карты, информация на которых зафиксирована в форме рельефных (объемных) графических изображений и знаков письма, выдавливаемых на поверхности подложки с помощью клише методом высокой печати. Графические изображения и знаки выдавливаются из подложки с оборотной стороны на лицевую. Спецификации, которым должны соответствовать группы рельефно заформованных (тисненных) знаков на карте, определяются стандартом ISO 7811-1 «Карты идентификационные. Метод записи»[72]. Чаще других эмбоссируются регистрационный номер и срок действия (годности) карты, фамилия и имя ее держателя.

При изготовлении карт может также использоваться метод *идент-печати*. Суть этой технологии заключается в том, что графические изображения и знаки не выдавливаются из подложки, а вдавливаются в нее.

Эти способы фиксации информации используют в следующих целях:

а) Для убыстрения оформления первичных расчетно-кассовых документов по операциям с использованием платежных карт: информация из эмбоссированных реквизитов, работающих как клише, с помощью импринтера моментально отпечатывается в соответствующих графах слипа (чека). Слип состоит из трех скрепленных между собой листов бумаги. На оборотной стороне каждого листа нанесен специальный видимый или невидимый копировальный слой, позволяющий путем механического давления перемещаемой вручную каретки импринтера перекопировать информацию с эмбоссированных реквизитов карты и клише импринтера в нужные графы бланка слипа.

б) Для защиты карты и слипов от подделки.

в) Для считывания информации с карты средствами электронно-вычислительной техники.

4. Штрих-кодовые. Компьютерная информация в этих картах представлена в виде параллельных черно-белых штриховых линий одинаковой высоты, но разной ширины. Их наносят на подложку печатающими устройствами СВТ (принтерами либо специальными электронно-цифровыми маркираторами). В качестве азбуки ис-

---

[72] Например, общую спецификацию на эмбоссированные реквизиты для карт системы VISA см.: *Анчабадзе Н.А.* Организационно-правовые и криминалистические вопросы предотвращения хищений, совершаемых в финансовой сфере с использованием пластиковых карточек, мошенническим путем. – Волгоград, 2002. – С. 66-69.

пользуется универсальный торговый код. Карты рассматриваемого вида относительно популярны в связи с низкой себестоимостью и дешевизной считывающего оборудования (ручного или планшетного сканера с инфракрасной лампой).

В то же время они обладают самой низкой степенью защиты от подделки и поэтому не используются в платежно-расчетных операциях. При этом для повышения уровня защищенности закодированной информации используют следующие технологии:

1) штрих-код покрывают слоем специальной флюоресцентной краски, которая визуально непрозрачна при обычном (дневном или искусственном) освещении, но способна светиться (становится видимой) в инфракрасных (ИК) или ультрафиолетовых (УФ) лучах[73];

2) штрих-код наносят двумя специальными ферромагнитными красками одинакового цветового тона, но с разными магнитными свойствами, создающими дискретное распределение полос штрих-кода;

3) используется трехмерный штрих-код, когда штрихи эмбоссируются на подложке карты – имеют ширину, высоту и глубину.

5. Индукционно-структурные (магнитные) карты. Информация на них закодирована с помощью специальных магнитных меток, которые в определенном порядке наносятся на поверхность подложки или внедряются (вплавляются) в нее. Для кодирования используется индивидуальный для каждой карты алгоритм расположения магнитных меток на подложке, называемый топологией – зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности магнитных меток. Топология меток на карте обязательно должна совпадать с топологией активных зон считывателя. В качестве азбуки кодирования, как правило, используется Азбука Брайэля (азбука для слепых), код Бодо (международный телеграфный код) или оригинальная локальная система кодирования. Карты этого вида работают на физическом принципе магнитной индукции, обладают высокой степенью надежности и работоспособности, их практически невозможно подделать. Однако они имеют ограниченное (локальное) использование, поскольку «привязаны» к своему считывателю. В случае утраты карты его необходимо заменять, поскольку оно распознает только один неизменяемый индивидуальный код[74]. Чтобы этого не

---

[73] См.: Пластиковые карты. – 4-е изд., перераб. и доп. – М., 2002. – С. 14 (рис. 1).

[74] Подробнее см.: Организация входного контроля в вычислительных центрах // Иностранная печать о техническом оснащении полиции капиталистических государств. – 1991. – № 12. – С. 30-33.

произошло, одновременно с изготовлением считывателя делают несколько карт с одним кодом. Индукционно-структурные карты используют преимущественно в автоматизированных системах санкционирования доступа на охраняемый объект или в хранилище в качестве ключа.

6. Оптические. К этой группе относятся пластиковые карты, основанные на использовании следующих оптических методов защиты и записи информации.

6.1. О*птически комбинированные карты*. Их изготавливают по следующей технологии. В листе пластика термическим или механическим способом выдавливаются небольшие прямоугольные ниши. Затем в них вклеиваются бумажные элементы – реквизиты, содержащие идентификационную (конфиденциальную) информацию о держателе карты, например фотографию, отпечаток пальца руки, личную подпись и другие. Полученную заготовку накрывают листом другого пластика, прозрачного для определенных видов электромагнитных излучений, как правило, для УФ или ИК. Листы пластика термически сплавляют между собой (ламинируют) и вырезают по стандартным линейным размерам. В итоге получается документ, у которого при обычном освещении видны только реквизиты, содержащие информацию общего пользования, тогда как охраняемая законом информация скрыта от визуального просмотра. Напротив, сканирующее оптическое устройство при кратковременном освещении карты УФ- и (или) ИК-лучами считывает конфиденциальную информацию и передает ее в ЭВМ для распознавания и принятия решения.

6.2. *Оптические кодовые карты*. При их создании используется технология чередования прозрачных и непрозрачных зон в виде штрих-кода, точек и штрихов или кружков и прямоугольничков. В считывающем устройстве с одной стороны установлен источник УФ- и (или) ИК-света, а с другой – его приемник – электронные фотоэлементы (фотодиоды, фототранзисторы или полупроводниковый прибор с зарядовой связью – ПЗС матрица)[75]. Свет, проходя через оптически прозрачные зоны карты, расположенные в определенном порядке, воспринимается приемником, трансформируется в электромагнитные сигналы, которые усиливаются и передаются в микроЭВМ для обработки. Такие пластиковые карты используются в охранных системах для разграничения доступа.

---

[75] Понятие и принцип действия ПЗС-матрицы см.: *Кузнецов Ю.А., Шилин В.А.* Микросхемотехника БИС на приборах с зарядовой связью. – М., 1988.

6.3. *Голографические* – наиболее защищенные от подделки и дорогостоящие в изготовлении пластиковые карты. Для кодирования и записи информации в них используются специальные информационные оптические слои в виде голограмм, дифракционных решеток, микроэкранов либо миниатюрных призм Френеля[76]. Карты этой группы используют как идентификационные документы (удостоверения, студенческие и ученические билеты, страховые полисы, пропуска и другие).

6.4. *Лазерные карты.* Основаны на использовании лазерной (оптической) технологии записи информации. Карта рассматриваемого вида была изобретена в 1981 г. Дж. Дрэкслером[77]. Запись информации производится с помощью сфокусированного оптического луча (лазера), который в определенном порядке оставляет на специальном информационном (термоперезаписываемом) слое многослойного пластика дорожку механических следов («ямок»), имеющих различные оптические свойства и характеристики: оптический контраст между следом и следовоспринимающим слоем; коэффициент отражения света от следа.

Эти физические параметры должны соответствовать стандарту ISO 11694-4 «Карты идентификационные. Карты с оптической памятью – линейный метод записи данных». Например, ширина «ямки» (ширина дорожки) должна быть 0,5 мкм (0,0005 мм), длина – в пределах от 0,83 до 3,56 мкм (0,00083 – 0,00356 мм), а их глубина – 0,125 мкм (0,000125 мм)[78]. Нижний слой пластика подложки карты имеет зеркальное напыление, поэтому луч лазера отражается от указанных элементов, но под различным углом и с различной степенью интенсивности. Интенсивность света, отраженного от краев «ямки» либо от «ямки» в целом (в зависимости от алгоритма кодирования информации), соответствует логической цифре «1» двоичного машинного кода, а отраженного от дна «ямки» и (или) промежутков между ними на дорожке – логической цифре «0». Данные сигналы регистрируются ИК-лазером с длиной волны 780 нм (в воздухе), расположенном в считывающем устройстве, и распознаются специальным программным обеспечением ЭВМ – устройствами интерфейса[79], которые изготавливают по стандарту ISO 11694-

---

[76] Подробнее см.: Метод изготовления идентификационных карточек // Иностран. печать о тех. оснащении полиции кап. государств. – 1992. – № 8. – С. 32-37.

[77] См.: Пластиковые карточки в России / Сост. А.А. Андреев, А.Г. Морозов и др. – М., 1995. – С. 29.

[78] Подробнее см.: *Гук М.* Дисковая подсистема ПК. – СПб., 2001. – С. 134-135.

[79] Интерфейс – это совокупность унифицированных технических и программных средств, используемых для сопряжения устройств в вычислительной системе или

2 «Карты идентификационные. Карты с оптической памятью – линейный метод записи данных».

По механизму образования **оптических следов – пит** (от англ. «pits»–ямка) на термозаписываемом слое нами выделяются:

• *карты с абляционной записью* – луч прожигает (термоперфорирует) в информационно несущем слое пластика сквозное отверстие заданных микроскопических размеров и отражательных оптических параметров (**сквозная пита**);

• *карты с везикулярной (пузырьковой) записью* – луч вспучивает воздушный пузырек на границе соприкосновения информационного и защитного слоев пластика в форме микроскопической линзы (**объемной пузырьковой питы**);

• *карты с поверхностно-текстурированной записью* – луч изменяет (термически сглаживает) оптимизированный предварительный рельеф поверхности информационного слоя пластика, выдавливая на нем в определенном порядке микроскопические **плоские питы** различной длины;

• *карты с точечным сплавлением* – луч лазера в определенном порядке точечно сплавляет между собой две пленки многослойного пластика: таким образом получается **объемная сварная пита**.

Оптический реквизит карт рассматриваемого вида занимает значительную часть площади ее оборотной стороны. Его размеры и размещение на подложке определяются стандартом ISO 11694-3 «Карты идентификационные. Карты с оптической памятью – линейный метод записи данных». В последнее время этот реквизит, в основном, стали изготавливать из специальной «*цифровой бумаги*», разработанной английской фирмой Imagedata, представляющей собой новый тип оптического машинного носителя информации[80].

Основное преимущество карт – возможность хранения больших объемов текстовой и графической компьютерной информации (от 1,4 до 4,2 Мбайт). Вместе с этим рассматриваемая технология позволяет производить только однократную запись данных и их многократное считывание. Она получила название «WORM-технология» (от англ. «Write Once Read Multiple» – «писать один раз – читать многократно»). В настоящее время существуют два основных и, к сожалению, программно несовместимых формата записи компьютерной информации на лазерные карты: SIOC – фирмы Олимпус и DELA –

сопряжения между системами. – См.: *Першиков В.И., Савинков В.М.* Толковый словарь по информатике. – М., 1991. – С. 127.

[80] См.: *Богумирский Б.С.* Руководство пользователя ПЭВМ: В 2-х ч. Ч. 1. – СПб., 1992. – С. 47.

компании Дрэкслер[81]. По мнению специалистов, основным недостатком, препятствующим широкому распространению лазерных карт, является дороговизна изготовления и относительно большие габариты устройств считывания и записи информации[82].

7. Электромагнитные карты – карты с магнитной полосой (magnetic stripe card). Наиболее часто используемая и многочисленная категория карт. В основе метода записи информации на них лежит общеизвестное физическое явление – остаточный магнетизм – способность отдельных (ферромагнитных) материалов приобретать и сохранять намагниченность под воздействием внешнего магнитного поля. Принцип кодирования данных заключается в создании на магнитной проволоке[83] или полосе (ленте) участков (магнитных доменов) с различной степенью напряженности магнитного поля или противоположными направлениями магнитной ориентации.

В зависимости от типа магнитной полосы карты и применяемого формата записи компьютерной информации количество дорожек с записью электронных реквизитов варьируется от одной до четырех. Например, в соответствии со стандартами ISO 7811-3 «Карты идентификационные. Метод записи» (для банковских карт), ISO 7501-2 «Карты идентификационные. Машиночитаемые проездные документы» установлены три магнитные дорожки с данными.

Выделяются три технологических способа создания магнитной полосы на карте, зависящие от материала подложки и количества циклов ее использования, а именно:

1) магнитный слой наносится (напыляется по трафарету) на подложку в виде специального лака, содержащего частицы ферромагнитного вещества;

2) слой наносят на подложку с использованием типографского оборудования и специальной ферромагнитной краски;

3) на подложку наклеиваются полоски магнитной ленты, используемой для производства аудио- (узкая полоса) или видеокассет (широкая полоса).

В момент прохождения магнитной полосы через записывающее устройство, на обмотку его электромагнитной головки подается электрический импульс, который возбуждает в зазоре электромаг-

---

[81] См.: Оптические дисковые системы: Пер. с англ. / Г. Боухьюз, Дж. Браат, А. Хейсер и др. – М., 1991. – С. 212.

[82] См.: Пластиковые карты. – 4-е изд., перераб. и доп. – М., 2002. – С. 450.

[83] Машинным носителем информации является проволока из бериллиево-медного сплава, покрытая магнитным слоем (ферромагнетиком). – См.: *Першиков В.И., Савинков В.М.* Толковый словарь по информатике. – М., 1991. – С. 256.

нитное поле, ориентирующее микроскопические частицы ферромагнетика в определенном порядке. В итоге, на магнитной полосе появляются магнитные домены (метки). Именно они и считываются электромагнитной головкой соответствующего технического устройства, а затем декодируются программой для ЭВМ. Отличие состоит лишь в том, что магнитные метки, перемещаемые вдоль воздушного зазора считывающей головки, уже сами возбуждают в магнитопроводе переменное магнитное поле, которое индуцирует (порождает) электромагнитные колебания в обмотке.

Таким образом, идет процесс передачи информации от «отправителя» (записывающего устройства) к «получателю» (считывающему устройству) через «канал связи» – магнитный «транзитный» слой.

Для одновременной записи или считывания информации с магнитной полосы, имеющей несколько дорожек, электромагнитные головки объединяют в блоки.

После рассмотрения общих криминалистических признаков электромагнитных карт исследуем их частные признаки. Анализ эмпирических материалов позволяет сгруппировать их следующим образом.

7.1. *По стойкости к размагничиванию.* Важной характеристикой магнитной полосы является напряженность размагничивания – сопротивление ферромагнетика к размагничиванию (коэрцитивность). Иными словами, речь идет о величине магнитного поля, необходимого для записи или стирания информации. По этому основанию выделяют следующие виды карт.

Карты с низкой степенью коэрцитивности. При изготовлении магнитной полосы используется оксид железа Fe_2O_3, который является магнитомягким материалом. Визуально такие карты можно отличить от других по коричневому цвету магнитной полосы. Чем светлее этот цвет, тем меньше коэрцитивная сила. Такие карты имеют самую низкую степень защиты от подделки (по сравнению с другими картами рассматриваемого вида) и поэтому используются в качестве одноразовых проездных документов или пропусков.

Карты с высокой степенью коэрцитивности производят из магнитотвердых материалов – оксида хрома или феррита бария. Магнитная полоса рассматриваемых карт имеет черный цвет. Чем цвет насыщенней, тем выше коэрцитивность карты, а следовательно, и ее защита от подделки.

7.2. *По ширине магнитной полосы*. По этому признаку выделяются следующие группы карт.

Карты с узкой магнитной полосой изготавливают из материалов, имеющих низкую или среднюю степень коэрцитивности, ори-

ентируясь на стандарт ISO 7811-2 «Карты идентификационные. Метод записи». Это самая не защищенная от подделки категория электромагнитных карт. На территории Российской Федерации такие карты в основном используются для оплаты услуг электросвязи, в качестве проездных документов на городском транспорте (трамвай, троллейбус, автобус, метро), а также в качестве пропусков на охраняемые объекты. Информация на эти карты кодируется в виде магнитных штрихов. В зависимости от целей использования рассматриваемого реквизита карты применяют два способа электромагнитного штрих-кодирования информации, а именно:

1) В целях защиты документа от подделки на магнитную полосу наносят штрихи, имеющие одинаковую ширину и высоту, но разное расстояние друг от друга. Такое кодирование не предусматривает перемагничивание записанной информации, которая остается неизменной до окончания срока службы или цикла использования карты.

2) Для многоразовой оплаты услуги или фиксации частоты доступа на охраняемый объект. В этих целях используют электромагнитное простое штрих-кодирование: на магнитную полосу наносят магнитные штрихи, имеющие одинаковые ширину, высоту и расстояние друг от друга. Каждый магнитный штрих соответствует 1 условной единице, например 1 минуте телефонного разговора по таксофону (либо работы в сети Интернет) или 1 проходу через автоматизированный турникет контрольно-пропускного пункта. Каждый раз при наступлении указанного события один магнитный штрих размагничивается (стирается) головкой считывающего устройства. Этот процесс продолжается до тех пор, пока на магнитной полосе не останется ни одного магнитного штриха. После чего карта перемагничивается (перезаписывается) или выбрасывается за ненадобностью. Данным обстоятельством активно пользуются преступники.

Карты с широкой магнитной полосой, по сравнению с последними, имеют высокую степень защиты. Она достигается за счет следующих технологий:

- изготовления полосы из магнитных материалов, имеющих среднюю и высокую коэрцитивность;
- различного формата записи информации на трех дорожках;
- использования персонального идентификационного номера (ПИН-кода).

Физические параметры, которым должна удовлетворять магнитная полоса карт рассматриваемого вида, определяются стандар-

том ISO 7811-6 «Карты идентификационные. Метод записи». Ее ширина составляет 12,7 мм, что соответствует ширине стандартной магнитной ленты, используемой при производстве видеокассет (ГОСТ 20958-80). На этой полосе в соответствии со стандартом ISO 7811-3 «Карты идентификационные. Метод записи» располагаются три дорожки[84].

Первые две дорожки (ISO 1 и ISO 2) предназначены для идентификационных целей и технологически работают в режиме «только считывание информации». По завершении цикла использования карты информация на магнитных дорожках перезаписывается. Например, записываются персональные данные на нового клиента, чтобы он смог воспользоваться картой для совершения определенных операций. Линейные параметры расположения дорожек на магнитной полосе и способ кодирования (записи) на них информации установлен стандартом 7811-4 «Карты идентификационные. Метод записи».

Следует обратить внимание на то обстоятельство, что закодированная на дорожках ISO 1 и ISO 2 информация должна совпадать по своему содержанию с данными реквизитов карты, которые напечатаны или эмбоссированы на подложке.

Запись информации на дорожку ISO 3 регламентируется отдельным стандартом 7811-5 «Карты идентификационные. Метод записи». В соответствии с ним дорожка может использоваться не только в режиме «только считывание», но и «многократная перезапись информации». Этот стандарт позволяет отражать на дорожке **след последней операции, выполненной с помощью карты.** ISO 3 часто именуют «THRIFT» или «MUNTS», по названию некоторых американских фирм, разрабатывающих дорогостоящее терминальное оборудование для обеспечения использования дорожки в технологических процессах. По этой причине подавляющее большинство эмитентов не используют ее возможности в целях защиты карты от подделки, чем и пользуются преступники[85]. Таким образом, дорожка не содержит никакой информации и остается «свободной».

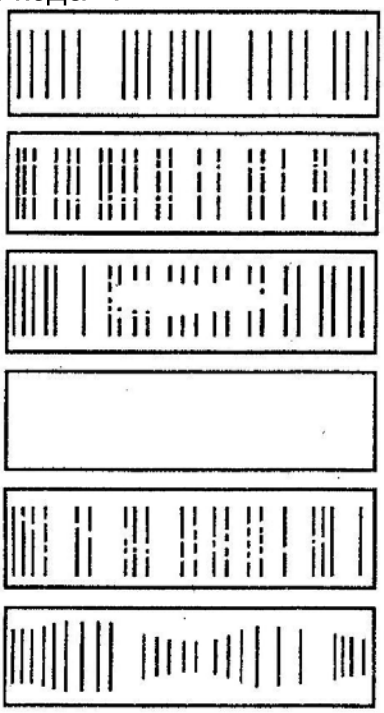
---

[84] Здесь и далее по тексту работы при описании криминалистических признаков карт с широкой магнитной полосой используются результаты исследования, проведенного Патриком Гелль. Подробнее см.: *Гелль П.* Магнитные карты и ПК / Пер. с фр. – М., 2001. – С. 27-49.

[85] См.: Расследование преступлений в сфере экономики: Руководство для следователей / Под общ. ред. И.Н. Кожевникова. – М., 1999. – С. 315.

С криминалистических позиций интерес представляют методы, с помощью которых можно обнаружить визуально не видимые следы записи информации на магнитных дорожках. Среди них выделяют следующие.

Использование специального визуализатора магнитного изображения («магнитного разоблачителя»)[86] – баллончика с пульверизатором, содержащего аэрозоль никеля. По аналогии с обнаружением невидимых поверхностных следов пальцев рук, содержимое баллончика в течение нескольких секунд распыляется по поверхности магнитной полосы. В результате этого визуально проявляется **магнитный след** («рисунок») записи информации в виде штрих-кода[87].



Без повреждений

Повреждения, вызванные частым использованием

Частичное размагничивание (карта находилась в слабом магнитном поле, вблизи намагниченных предметов и т.д.)

Отсутствие записи или полное размагничивание, вызванное близостью сильного магнитного поля

Стирание, вызванное повторяющимся контактом с другими предметами (карта не защищена кожухом)

Деформированная дорожка (деформация карты или сбой при записи)

Использование специального порошка, реагирующего на магнитные домены. Данный метод, как и предыдущий, хорошо известен в криминалистике. Порошок состоит из смеси одной части тонера – черного порошка, используемого для заправки картриджей ксероксов и лазерных принтеров (он очень хорошо притягивается к намагниченным участкам дорожек и отображает след), и 3–5 частей крахмала (зерна крахмала притягивают к себе излишки более мелких частиц тонера и создают бело-черный контраст штри-

[86] Например, марки «Transcode (JELT-CM)».
[87] См.: *Гелль П.* Указ. соч. – С. 49.

хов). При обработке магнитной полосы карты с помощью мягкой кисти и указанного порошка частицы черного порошка тонера расположатся поверх магнитных доменов, а зерна белого крахмала – между ними, визуально отобразив магнитный след – штрих-код[88].

Карты с нестандартной магнитной полосой. К этой категории нами относятся электромагнитные карты, имеющие нестандартные размеры бумажной подложки и магнитной полосы. В качестве примера приведем билеты на самолет Аэрофлота и проезд по железной дороге во Франции. Ширина бумажной подложки этих карт составляет 8,5 см, длина – 20,3 см; ширина магнитной полосы, содержащей 4 дорожки, – 1,5-1,7 см, а ее длина – 20,3 см. Карты имеют локальное использование в рамках одного национального эмитента, не соответствуют стандартам ISO и поэтому подробно не рассматриваются в настоящей работе.

8. Карты на интегральных микросхемах. В обиходе их называют «смарт-картами» (от англ. «smart cards» – интеллектуальные карты). Они получают в нашей стране все большее распространение. По мнению специалистов, поводом для их появления явилась потребность повышения уровня защищенности пластиковых карт от подделки и физического износа[89].

Пластиковая карта с микросхемой была запатентована в 1974 г. французским журналистом Роланом Морено. Он также высказал идею о том, что пластиковая карта может быть не только с одним, но и с большим количеством микросхем, одна из которых может выполнять функцию обычного микропроцессора ЭВМ[90].

Интегральная микросхема (ИМС) – это микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функций электронной схемы, элементы и связи которого неразрывно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие. При этом зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы и связей между ними называется **топологией**[91].

Интегральная микросхема была изобретена в 1958 г. независимыми друг от друга американскими инженерами Д. Килби из компании

---

[88] Подробнее см.: *Гелль П.* Указ. соч. – С. 46-48.

[89] См., например: *Матюхин В.Г., Пярин В.А.* Концепция обеспечения информационной безопасности платежной системы на основе интеллектуальных карт // Системы безопасности связи и телекоммуникаций. – 1998. – Март-апрель. – С. 8-12.

[90] См.: Банковское дело: Учебник / Под ред. О.И. Лаврушина. – М., 1999. – С. 528.

[91] См.: Закон Российской Федерации от 23.09.92 г. № 3526-1 «О правовой охране топологий интегральных микросхем». – Ч.1 ст. 1.

«Texas Instruments» и Р. Нойсом, который впоследствии основал корпорацию «Intel», являющуюся в настоящее время флагманом в производстве микропроцессоров для ЭВМ[92].

С технической точки зрения ***ИМС***, используемая в пластиковой карте как реквизит для записи и считывания информации, является полупроводниковым прибором. По своему функциональному назначению она ***может выполнять роль машинной памяти*** – постоянного (ПЗУ) и (или) оперативного (ОЗУ) запоминающего устройства, а также ***быть микропроцессором*** – программно-управляемым устройством, осуществляющим обработку компьютерной информации. Для этого микросхема содержит матрицу – накопитель информации и функциональные элементы, необходимые для усиления электромагнитных сигналов при записи и считывании данных, обеспечения режима синхронизации сигналов, их шифрования/дешифрования и другие. В качестве этих элементов выступают интегральные электрорадиоэлементы и их схемы – транзисторы, диоды, конденсаторы, резисторы, индуктивности и другие[93]. **Матрица памяти** состоит из интегральных диодов, биполярных или «металл-диэлектрик-полупроводник» (МДП) транзисторов, размещенных в электроуправляющих узлах двухкоординатной матрицы (кремниевой пластины). Таким образом, диоды и транзисторы являются *ячейками памяти*: информация определяется наличием (хранение цифры «0») или отсутствием (хранение цифры «1») диода или транзистора в узле.

По конструктивному исполнению рассматриваемая группа микросхем относится к разряду *совмещенных*: все активные элементы (например, транзистор) и часть пассивных изготовляют по *полупроводниковой технологии* в пластине кремния[94], а часть пассивных элементов – *по тонкопленочной технологии*: толщина пленок, из которых изготовлены электрорадиоэлементы, не превышает 1 мкм (0,001 мм); толщина проводящей металлической пленки (электрического проводника) меньше длины свободного пробега в ней электронов. Тонкопленочные элементы формируют различными методами: термическим испарением материалов в вакууме;

---

[92] См.: *Богумирский Б.С.* Руководство пользователя ПЭВМ: В 2-х ч. Ч. 1. – СПб., 1992. – С. 27.

[93] См.: *Коледов Л.А.* Технология и конструкции микросхем, микропроцессоров и микросборок: Учебник для вузов. – М., 1989. – С. 31. – Рис. 1.22.

[94] Микросхема карты, как правило, имеет следующие размеры: ширина – 11 мм; высота – 8 мм; толщина – 0,7 мм. Пластина кремния этой микросхемы имеет следующие размеры: ширина – 4 мм; высота – 3 мм; толщина – 0,15 мм.

электрохимическим осаждением из растворов; химическим осаждением из газовой фазы[95].

Часть подложки, отведенную под одну микросхему, отделенную от других частей вместе со сформированными на ней пассивными элементами *в полупроводниковой технологии,* называют **кристаллом**, а *в пленочной технологии* – **платой**[96]**.**

Микросхемы памяти для пластиковых карт выпускают без корпуса: корпусом для них служит подложка карты, в которую они имплантируются на стадии изготовления карты. Все параметры процесса производства карт рассматриваемой категории, а также расположения на них реквизитов определяются стандартом ISO 7816 «Карты идентификационные. Карты с интегральной микросхемой с контактами» (6 частей), действующим с 1989 г.

Карты с интегральной микросхемой по своим эксплуатационным характеристикам значительно превосходят карты с магнитной полосой.

С криминалистических позиций микропроцессорные карты представляется возможным подразделить на следующие виды.

8.1. *По способу записи информации на микросхему.*

Не перепрограммируемые карты. Запись информации на них осуществляется только один раз в процессе изготовления микросхемы на одной из завершающих технологических операций и хранится бесконечно долгое время. Для кодирования информации применяется бинарный машинный код. Не перепрограммируемые карты привязаны к своему считчику и поэтому используются как постоянные безличные документы (пропуска, дисконтные карты, ЭЦП и т. д.) или электронные ключи доступа на охраняемый объект (через турникеты автоматизированных КПП). Круг применения таких карт очень узок – в локальной системе или сети ЭВМ одного эмитента.

Однократно программируемые карты отличаются от предыдущих тем, что информация на микросхему записывается пользователем частями (порциями, импульсами) до тех пор, пока объем памяти матрицы не будет исчерпан, либо один раз с одновременным занятием всей области памяти. Запись осуществляется путем разрушения (пережигания) полупроводниковых диодов или специальных перемычек матрицы памяти. Для этого через соответствующие диоды или электрические проводники – перемычки, соединяющие адресные шины с эмиттерами МДП-транзисторов, пропускают ток необходимого значе-

---

[95] См.: *Коледов Л.А.* Указ. соч. – С. 20.

[96] Подробнее см.: Там же. – С. 21-22.

ния[97]. Плавкие перемычки изготавливают из сплавов титана с вольфрамом, поликремния и других материалов (по аналогии спирали обычной лампы накаливания – электрической лампочки).

Пластиковые карты рассматриваемого вида используют в локальной системе или сети ЭВМ одного эмитента следующим образом.

1) В операциях, где необходим счет количества раз использования карты: для поминутной оплаты услуг связи (телефонные карты); для оплаты услуг метрополитена (абонементные проездные билеты на несколько поездок в метро); для оплаты покупаемого бензина или ГСМ; в целях фиксации количества раз прохода лиц через автоматизированные КПП. В этих операциях карты выступают как безличные документы, имеющие номинал, выраженный в условных единицах. При совершении операции приемное терминальное устройство пережигает в матрице памяти соответствующее количество диодов или плавких перемычек. Процесс записи информации заканчивается тогда, когда на матрице не останется ни одного целого диода или ни одной не пережженной перемычки. При наступлении этого события карта выбрасывается за ненадобностью, поскольку микросхема не подлежит восстановлению (перезапись информации на нее невозможна).

2) В качестве документов, удостоверяющих личность (паспорт, удостоверение, студенческий билет, карта постоянного клиента, клубная карта, пропуск и другие).

Перепрограммируемые карты позволяют их пользователям многократно перезаписывать информацию. Кроме того, их микросхемы можно использовать как ОЗУ. При изготовлении матрицы в качестве ячеек памяти используются специальные высокоинтегрированные на атомно-молекулярном уровне МДП-транзисторы: лавинно-инжекционные с плавающим затвором; лавинно-инжекционные с плавающим и управляющим затворами; со структурой «металл-нитрид кремния-оксид кремния-полупроводник» (МНОП-транзисторы). Если подложка перепрограммируемой карты в месте интеграции в нее микросхемы изготовлена из оптически прозрачного для УФ-лучей пластика, то запись информации осуществляется в электрическом режиме, а стирание – дистанционно под воздействием УФ-излучения, исходящего из соответствующего устройства. При этом информация стирается одновременно из всех ячеек памяти микросхемы. Если же пластик не прозрачен для УФ-лучей, то и запись и стирание информации происходят в электрическом режиме[98]. Пластиковые карты рассматривае-

---

[97] См.: *Коледов Л.А.* Указ. соч. – С. 200.

[98] Подробнее см.: Там же. – С. 116-121.

мой группы – это, как правило, именные документы (банковские, медицинские, студенческие, пенсионные и др.).

8.2. *По функциональному назначению микросхемы.*

Карты с интегральной памятью. К этой группе относятся карты с не перепрограммируемой и однократно программируемой микросхемой постоянной памяти. В данном случае пластиковая карта содержит только одну интегральную микросхему, которая используется исключительно как машинный носитель информации. Такие карты имеют одну логическую зону памяти. Они привязаны к считывающему терминальному устройству и поэтому имеют локальное применение в системах или сети ЭВМ одного эмитента.

Микропроцессорные карты (микроЭВМ). В отличие от всех ранее рассмотренных видов карт они не только хранят на своем машинном носителе информацию, но и обрабатывают ее[99]. Стандартом внутренней логической организации этих карт является архитектура SPOM (Self Programming On Memory), разработанная и запатентованная в 1978 г. французской фирмой Bull CP8 Transac. В соответствии с ней пластиковая карта должна содержать в своем строении определенный набор взаимосвязанных микроэлектронных модулей, выполняющих следующие функции[100].

1) **Микропроцессор**[101] – большая или сверхбольшая интегральная микросхема, выполняющая функции центрального процессора (Central Processing Unit – «CPU») – процессора, осуществляющего в данной вычислительной системе основные операции по обработке данных и управлению работой других частей этой системы («мозг» ЭВМ). Состоит из устройства управления (УУ), арифметико-логического устройства (АЛУ) и процессорной памяти (ПП)[102].

2) **Сопроцессор (coprocessor)** – специализированная интегральная микросхема, выполняющая роль дополнительного процессора, расширяющего функциональные возможности микропроцессора[103]. Отвечает за разграничение доступа к информации,

---

[99] См.: Пластиковые карты. – 4-е изд., перераб. и доп. – М., 2002. – С. 15. – Рис. 2.

[100] Подробнее см.: *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты. – М., 2000. – С. 397-398.

[101] О понятии, эволюции, основных технических характеристиках, классификации, основных моделях и архитектуре строения микропроцессоров см.: *Богумирский Б.С.* Указ. соч. – С. 27-39.

[102] См.: *Першиков В.И., Савинков В.М.* Толковый словарь по информатике. – М., 1991. – С. 201, 315.

[103] См.: Там же. – С. 373.

хранящейся в матрице памяти, а также за выполнение процедур криптографического преобразования данных в целях их защиты от несанкционированного использования: обеспечивает исполнение ПИН-кода. Фактически, сопроцессор является модулем системы безопасности данных (Security features).

3) **Оперативное запоминающее устройство** (ОЗУ) или так называемая «RAM-память» (Random-access memory – оперативная память) – энергозависимая (разрушаемая при снятии электропитания) память используется в качестве рабочей памяти для временного хранения данных, поступающих от микро- и сопроцессора. В настоящее время типовая микропроцессорная карта имеет объем памяти ОЗУ от 128 до 256 Кбайт.

4) **Постоянное запоминающее устройство** (ПЗУ) или «ROM-память» (Read-only memory – только читаемая память) – энергонезависимая (не разрушаемая при отключении электропитания) память – содержит операционную систему[104] и программные приложения (набор служебных программ для ЭВМ, которые не изменяются в процессе работы). Последние определяют функциональное назначение пластиковой карты, набор операций для совершения которых она может использоваться, а также возможности ее коммутации с различными терминальными устройствами. Эта информация записывается в ПЗУ при изготовлении карты.

5) **Программируемое постоянное запоминающее устройство** (ППЗУ) или «EPROM-память» (Electrically Programmable Read-only memory – электрически программируемая только читаемая память). Эта память может быть прочитана много раз, но запись информации на нее осуществляется только единожды. В процессе персонализации карты эмитентом в ППЗУ записываются данные о ее держателе (фамилия, имя и другая конфиденциальная информация, позволяющая идентифицировать его личность).

6) **Электрически стираемое программируемое постоянное запоминающее устройство** (ЭСППЗУ) или «EEPROM-память» (Electrically Erasable Programmable Read-only memory – электрически стираемая программируемая только читаемая память). Информация в ЭСППЗУ может быть многократно перезаписана и считана с помощью специального программно-аппаратного устройства, на-

[104] Программы для ЭВМ, которые обеспечивают управление другими программами и реализуют функции планирования, управления вводом-выводом данных и т.п. – См.: Там же. – С. 361.

зываемого «программатор»[105]. Эта память содержит различные конфиденциальные данные, например о последних проведенных с использованием карты операциях, ключ криптографического преобразования и другие. Помимо вышеуказанного, ЭСППЗУ является также коммуникационным модулем (портом), связывающим микропроцессор со считывающим и (или) записывающим терминальным устройством. Для этого к электрической схеме ЭСППЗУ подключены металлические коммутационные контакты.

Очевидно, что, обладая указанным **микропроцессорным комплектом микросхем** – базовым набором микросхем, предназначенных для совместного применения в целях автоматической обработки информации для решения вычислительных и информационных задач, *пластиковая карта становится* не чем иным, как *микроЭВМ*[106]*.* В настоящее время эта ЭВМ может иметь 8-, 16- или 32-разрядный управляющий процессор и общую память, объемом от 16 до 256 Кбайт. Память позволяет хранить и обрабатывать максимальную идентификационную информацию о реквизитах карты, особых условиях ее использования, об эмитенте, владельце (картодержателе), последних совершенных с ее помощью операциях и многое другое. Например, если это банковская карта, то, по мнению специалистов, она фактически представляет собой электронную чековую книжку, содержащую информацию о последних 200 произведенных платежно-расчетных операциях, данные о которых можно считывать с экрана соответствующего терминала[107]. Оформление чека в данном случае производится с использованием клавиатуры электронного терминального устройства (банкомата, контрольно-кассовой машины (ККМ)[108], автоматизированной кассовой сети (АКС), бимчекера)[109], к которому подключается карта.

---

[105] **Программатор** иногда используется преступниками как орудие совершения преступления. В этом качестве он будет рассмотрен далее по тексту работы при исследовании способов совершения преступлений выделенной категории.

[106] О понятии и устройстве микроЭВМ подробнее см.: *Каяцкас А.А.* Основы радиоэлектроники: Учеб. пособие. – М., 1988. – П. 20.5 «Микропроцессорные БИС и микроЭВМ».

[107] См.: *Панова Г.С.* Новые банковские продукты и услуги // Банковское дело: Учебник / Под ред. проф. О.И. Лаврушина. – М., 1999. – С. 528.

[108] **Контрольно-кассовая машина (ККМ)** – специализированная ЭВМ, выполняющая счетно-суммирующие, вычислительные и чекопечатающие функции. – См.: П. 1 Типовых правил эксплуатации контрольно-кассовых машин при осуществлении денежных расчетов с населением // Письмо Министерства финансов Российской Федерации от 30.08.93 г. № 104.

[109] **Бимчекер** – это миниатюрная ручная мобильная ККМ, работающая по принципу сотового радиотелефона, предназначенная исключительно для проведения

Несмотря на то, что рассматриваемая категория карт является наиболее защищенной от подделки, в 1998 г. в городе Омске она впервые в мире была подделана 19-летним сотрудником отделения АКБ «Нефтеэнергобанк» Евгением Монастыревым. Данный субъект являлся одним из разработчиков системы пластиковых карт «Золотое кольцо» со встроенными микропроцессорами. С помощью указанного орудия преступления им было совершено хищение несколько тысяч долларов США со счетов клиентов названного банка[110].

В настоящее время наиболее массовыми сферами применения микропроцессорных карт являются кредитно-банковская и услуг сотовой электросвязи (в виде так называемых SIM-карт – от англ. «Subscriber Identity Module» – модуля идентификации абонента). К началу 2002 г. общее количество карт, используемых в этих сферах, превысило 3 млрд (около 2 млрд – банковских и 1 млрд SIM-карт) и продолжает увеличиваться. Общий оборот денежных средств по операциям только с банковскими картами в том же году во всем мире составил свыше 3,3 трлн долларов США[111]. Вместе с тем, по данным компании VISA International, объем покупок товаров в виртуальных магазинах глобальной сети Интернет через сотовые радиотелефоны составит в 2003 г. 66 млрд долларов США[112].

Крупнейшими мировыми производителями карт рассматриваемого вида являются такие зарубежные фирмы, как: Gemplus, Bull CP8 Transac, Solaic Sligos (Франция); AT&T, Data card (США); Philips TRT (Германия); Toshiba (Япония). Микросхемы к ним, в основном, производят: Amtel, Motorolla (США); Hitachi, Oki (Япония); Philips (Германия)[113].

Карты – мини-ЭВМ. Иначе их называют «суперсмарт-картами» (от англ. «supersmart cards» – сверхинтеллектуальные карты). Они являются пиком технического совершенства карточных продуктов. Примером может служить многоцелевая микропроцессорная карта фирмы Tochiba, используемая в крупнейшей международной пла-

---

безналичных расчетно-кассовых операций с использованием платежно-расчетных карт.

[110] Подробнее см.: *Милкус А., Мызалин В.* Если денег дома нет – потрясите Интернет // Комсомольская правда. – 1998. – 18 дек. – С. 18.

[111] Получено путем обобщения данных, приведенных в книгах: *Голдовский И.* Указ. соч. – С. 20, 29; Пластиковые карты. – 4-е изд., перераб. и доп. – М., 2002. – С. 143, 154, 166, 179.

[112] См.: *Голдовский И.* Указ. соч. – С. 28.

[113] См.: *Панова Г.С.* Новые банковские продукты и услуги // Банковское дело: Учебник / Под ред. проф. О.И. Лаврушина. – М., 1999. – С. 529.

тежной системе VISA International[114]. В дополнении к архитектуре строения микропроцессорной карты она имеет миниатюрный жидкокристаллический экран, вспомогательную клавиатуру для ввода буквенно-цифровых данных и автономный источник электропитания. Эта карта объединяет в себе функции кредитной и дебетовой карты, часов, календаря, калькулятора, записной книжки, а также осуществляет автоматическую конвертацию валюты по действующему на момент ее подключения к терминальному устройству (банкомату или бимчекеру) курсу[115].

Выпускается также суперсмарт-карта с расширенными функциями для использования в комплексных автоматизированных цифровых системах. В конструктивное исполнение такой карты, помимо вышеуказанных элементов, добавлены микрофон, динамик и радиопередатчик. Картодержатель может осуществлять ввод информации с помощью миниатюрной клавиатуры либо с микрофона через блок анализатора речевой информации, что существенно повышает уровень ее защиты от подделки (карта запрограммирована на фоноскопические характеристики голоса ее держателя). На ее лицевой панели расположены миниатюрные: клавиатура, жидкокристаллический цифровой дисплей, микрофон и фотоэлементы, выполняющие роль автономного источника электропитания. На тыльной стороне карты находится миниатюрная головка динамика и металлические контакты. Карта включается и предоставляет доступ к информации или на охраняемый объект автоматически после идентификации контрольной фразы, произнесенной в микрофон ее законным держателем. В последнем случае сигнал на открытие запирающих устройств или отключение сигнализации подается по радиоканалу на приемное («считывающее») устройство. После этого, в памяти карты и ЭВМ, управляющей системой санкционирования доступа, автоматически фиксируется: дата; точное время (час, минуты, секунды); имя держателя карты, чей голос был идентифицирован; номер пункта доступа на охраняемый объект (шифр КПП или турникета); иная информация о произведенной операции. Большой объем памяти карты позволяет регистрировать не только идентификационные биометрические признаки ее держателя (фоноскопию голоса, личную подпись, отпечатки пальцев рук, характеристики ладони, рисунок кровеносных сосудов сетчатки глаза и т. п.), но и хранить дополни-

---

[114] На начало 2002 г. этой платежной системой обслуживалось 1,3 млрд карт с денежным оборотом 2 трлн долларов США – см.: Пластиковые карты. – 4-е изд., перераб. и доп. – М., 2002. – С. 154.

[115] См.: *Панова Г.С.* Указ. соч. – С. 529.

тельные сведения о нем (адрес места жительства, паспортные данные, группа крови, реквизиты водительского или иного удостоверения, данные полиса пенсионного страхования, номер и состояние счета в банке, семейное положение, место работы или учебы и другие персональные данные)[116].

С технической точки зрения, карты рассматриваемого вида относятся к классу мини-ЭВМ[117]. По мнению специалистов, из-за высокой стоимости карты этого вида не имеют сегодня широкого распространения, однако сфера их применения, вне всяких сомнений, будет расти в силу их перспективности[118].

По способу подключения к считывающему устройству ЭВМ, системы или сети ЭВМ

1. Контактные карты. Большая часть всех используемых в настоящее время карт. Они подключаются к считывающему устройству путем непосредственного механического контакта. При этом следовоспринимающей поверхностью, на которой остаются наиболее информативные с криминалистических позиций следы, будет реквизит карты, выполняющий роль машинного носителя информации. Например, для карт, изготавливаемых по стандарту ISO 7816-4 «Карты идентификационные. Карты с интегральной микросхемой с контактами», таким реквизитом будет запрограммированная микросхема и ее металлические контакты.

Следует обратить внимание на тот факт, что эмбоссированные, лазерные и электромагнитные карты всегда будут контактными.

2. Бесконтактные карты. Процесс чтения либо чтения и записи информации с реквизитов этих карт осуществляется дистанционно – по магнитному или электромагнитному каналу связи, устанавливаемому по схеме «излучатель сигнала (передатчик) считывающего устройства – машинный носитель информации (реквизит) карты – регистрирующий элемент (приемник) считывающего устройства». Машинным носителем информации на промежуточных стадиях являются:

- магнитное поле, характеризуемое напряженностью и направлением (полюсностью);

---

[116] Подробнее см.: Идентификация личности человека по голосу // Иностран. печать о тех. оснащении полиции кап. государств. – 1992. – № 1. – С. 23-26.

[117] О содержании понятия «мини-ЭВМ» см.: *Ушаков Н.Н.* Технология производства ЭВМ: Учебник. – 3-е изд., перераб. и доп. – М., 1991. – С. 8-9.

[118] См.: *Панова Г.С.* Указ. соч. – С. 529.

• электромагнитное излучение, характеризуемое мощностью, диапазоном частот и коэффициентом отражения или преломления от реквизита карты.

Примером могут служить пластиковые микропроцессорные карты, выполненные по стандарту ISO 10536-2 «Карты идентификационные. Бесконтактные карты с интегральной микросхемой». Такие карты взаимодействуют со считывающим устройством системы или сети ЭВМ на расстоянии до 10 см. Запись/считывание информации и электропитание схемы карты осуществляются в форме радиосигнала через приемопередающую антенну, имплантированную в подложку карты. Причем, если в электромагнитном поле антенного устройства считывателя попадает более одной карты, специальный модуль распознавания «радиокарт» обеспечивает бесперебойную коммуникацию с первой вошедшей в зону его действия картой[119].

3. Коммуникационно-комбинированные карты (CombiCard). К этой категории относятся микропроцессорные карты, имеющие контактную и бесконтактную микросхемы[120].

Они сочетают в себе функциональные возможности карт двух вышерассмотренных видов и дополнительно могут оборудоваться магнитной полосой и другими машинными носителями информации, отвечающими требованиям стандартов ISO. Например, Российская интеллектуальная карта с микропроцессором и широкой магнитной полосой, производимая ОАО «Ангстрем» и НТЦ «Атлас» (г. Зеленоград Московской области).

По мнению отдельных специалистов, «будущее – за комбинированными системами, где будет использоваться смешанный вариант микропроцессорных карт с магнитной полосой»[121].

По назначению

1. Платежно-расчетные документы. Как было отмечено ранее, карты этой группы являются средством для совершения сделок по приобретению товаров (услуг) и (или) по получению наличных денежных средств, расчеты по которым производятся в соответствии с условиями договора между эмитентом карты и лицом, их использующим[122]. Такие карты чаще других являются предметом или средством совершения преступления. Их можно условно классифицировать по следующим основаниям.

---

[119] См.: Пластиковые карты. – 4-е изд., перераб. и доп. – М., 2002. – С. 83.

[120] Подробнее см.: Там же. – С. 84-86.

[121] *Зуев А.* Смарт-технология и карточки для мелких платежей // Банковские технологии. – 1996. – № 8. – С. 82.

[122] См.: Указание Центрального банка России от 07.06.2000 г. № 799-У.

1.1. *Банковские карты* – средства для составления расчетных или иных документов, подлежащих оплате за счет клиента кредитно-банковской организации. При этом клиентом признается физическое или юридическое лицо, заключившее договор с кредитной организацией-эмитентом (банковского счета или вклада, кредитный договор и пр.), предусматривающий осуществление операций с использованием банковских карт[123]. Анализ законодательства Российской Федерации и нормативных документов, регламентирующих оборот банковских карт, дает основание отнести эти операции к безналичным расчетам (ст. 862 ГК РФ), близким по своему правовому содержанию расчетам по инкассо (ст. 874–876 ГК РФ), осуществляемым электронным способом.

Сведения, которые содержатся в памяти банковской карты, относятся к разряду банковской тайны[124].

В зависимости от способа записи информации и вида машинного носителя карты рассматриваемого вида изготавливают по следующим международным стандартам.

1) ISO 7812 «Карты идентификационные. Система нумерации и процедура регистрации идентификаторов эмитентов» (5 частей). Части этого стандарта определяют правила, по которым составляются номера банковских карт, а также способ вычисления из него ПИН-кода.

2) ISO 7813 «Карты идентификационные. Карты для финансовых транзакций» – определяет общие спецификации, которым должны удовлетворять все карты, используемые в автоматизированных системах обеспечения безналичных электронных расчетов.

3) ISO 4909 «Банковские карты. Содержание 3-й дорожки магнитной полосы» – регламентирует формат и содержание данных, записываемых на дорожку «ISO 3» карт с магнитной полосой. Эта дорожка должна отражать идентификационные данные о последних платежно-расчетных операциях, совершенных с применением карты. Однако, в целях экономии денег, необходимых для закупки более дорогостоящих программно-аппаратных средств, обеспечи-

---

[123] См.: Ст. 1 Положения о порядке эмиссии кредитными организациями банковских карт и осуществления расчетов по операциям, совершаемым с их использованием // Письмо Центрального банка России от 09.04.98 г. № 23-П.

[124] **Банковская тайна** – это сведения о реквизитах банковского счета и вклада, процедуре доступа к ним, об операциях по счету и вкладу, персональных данных о клиентах, а также иные сведения. – См.: Ст. 857 Гражданского кодекса; ст. 26 Закона Российской Федерации от 03.02.96 г. № 17-ФЗ «О банках и банковской деятельности».

вающих функционирование этой полосы, эмитенты не используют этот стандарт. Поэтому на дорожке «ISO 3» карт с магнитной полосой не содержится никакой информации.

Существует также российский стандарт ГОСТ Р 50809 «Нумерация и метрологическое обеспечение идентификационных карт для финансовых расчетов», определяющий основные характеристики банковских карт, эмитируемых отечественными кредитно-финансовыми организациями. В соответствии с ним на карте должны находиться следующие обязательные реквизиты.

1) На лицевой стороне: название организации-эмитента, ее эмблема или знак обслуживания; регистрационный номер карты (12 – 18 цифр); наименование организации – производителя карты (платежной системы), ее эмблема или товарный знак (знак обслуживания); срок действия карты (двузначный номер месяца/последние две цифры года); фамилия и имя держателя (на англ. языке); банковский идентификационный номер (БИН – 4 цифры) в платежной системе; металлические контакты интегральной микросхемы.

2) На оборотной стороне: заводской номер или номер партии, двузначный номер месяца/последние две цифры года выпуска карты изготовителем; широкая магнитная полоса; специальная защищенная от подделки бумажная полоса с образцом подписи законного держателя карты; юридический адрес эмитента; требование возврата карты эмитенту в случае, если она была найдена чужим лицом.

По схеме проведения безналичных расчетов банковские карты возможно подразделить на следующие виды.

Кредитные карты (credit cards) – связаны с открытием текущего кредитного счета (кредитной линии) в банке-эмитенте, что дает возможность их держателю распоряжаться всей суммой полученного кредита при покупках товаров, оплате услуг или получении кассовых ссуд. Являясь именным платежным документом, они в то же время не принадлежат с имущественной точки зрения их держателю и подлежат возврату в банк после полного (с процентами) погашения кредита. На территории Российской Федерации эти карты в основном используют иностранные граждане, поскольку отечественные кредитно-финансовые учреждения, опасаясь за возврат кредита, не выдают их своим клиентам – гражданам России.

Чековые гарантийные карты (cheque guarantee cards) – являются разновидностью кредитных карт. Они выдаются владельцу текущего счета в банке для идентификации его личности как чеко-

дателя и гарантии платежа по чеку[125]. Операции по карте базируются на кредитной линии, которая позволяет владельцу счета пользоваться кредитом по овердрафту. При этом банк гарантирует предприятию сферы торговли или услуг получение денег по чеку в пределах установленного лимита лишь в том случае, если на счете чекодателя отсутствует необходимая сумма.

По картам исследуемого вида устанавливается ежедневный лимит – предельная сумма платежа, гарантированная чековой картой. Если же сумма выплаты по чеку превысит сумму средств на счете чекодателя, с его владельца взимается комиссия за использование кредитной линии и процент по овердрафту. Поэтому клиенты – иностранные граждане предпочитают пользоваться кредитной картой как более удобной с указанных позиций.

Дебетовые карты (debit cards). В отличие от карт предыдущих групп, они принадлежат их держателю, который одновременно является их владельцем. Фактически он покупает пластиковую карту и ее номинал, эквивалентный номиналу той или иной валюты, который вносится на его банковский счет. Большинство карт, выдаваемых клиентам российскими кредитно-финансовыми учреждениями, являются дебетовыми.

С криминалистических позиций банковские карты также можно подразделить *по категории места проведения платежно-расчетной операции*, а именно:

Карты для электронных банковских автоматов (банкоматов). Это так называемые АТМ-карты (от англ. «Automated Teller Machine» – автоматическая кассовая машина). Они позволяют держателю дистанционно с помощью банкомата осуществлять платежно-расчетные операции по своему специальному карточному счету, открытому в кредитной организации – эквайрере[126]. При этом **банкомат** – это электронный программно-технический комплекс (ПТК), предназначенный для выдачи и приема наличных денежных средств, составления документов по операциям с использованием банковских карт, выдачи ин-

---

[125] Подробнее см.: П. 2.2 Правил расчетов чеками на территории Российской Федерации // Письмо Центрального банка России от 20.01.92 г. № 18-11/52.

[126] **Эквайринг** – деятельность кредитной организации, включающая в себя осуществление расчетов с предприятиями торговли (сферы услуг) по операциям, совершаемым с использованием платежно-расчетных карт, и осуществление операций по выдаче наличных денежных средств держателям банковских карт, не являющимся клиентами данной кредитной организации. – См.: Ст. 1 Положения о порядке эмиссии кредитными организациями банковских карт и осуществления расчетов по операциям, совершаемым с их использованием // Письмо Центрального банка России от 09.04.98 г. № 23-П.

формации по счету, осуществления безналичных платежей, конвертации валюты и т. д.[127] Фактически, банкомат представляет собой специализированную ЭВМ, выполняющую функции банковского служащего – кассира-операциониста.

Карты для электронных кассовых (торговых) *терминалов* – POS-карты (от англ. «Position-Of-Sale terminals» – точка оформления покупки). Под **электронным кассовым терминалом** понимается электронное программно-техническое устройство, предназначенное для совершения операций с использованием банковских карт[128]. Эти карты, так же как и карты предыдущей группы, «привязаны» к банковскому чековому или сберегательному счету держателя карты. Карта POS выполняет функции банковского чека, однако ее применение более надежно, так как идентификация держателя производится в момент совершения сделки: в электронном режиме с помощью бимчекера или ридера ККМ; в механическом режиме с использованием импринтера – механического устройства, предназначенного для переноса оттисков рельефных (эмбоссированных) реквизитов карты на **слип** – документ, составленный на бумажном носителе[129].

1.2. *Карты с фиксированной покупательной способностью (store value cards)*. В отличие от дебетовых банковских карт эти платежно-расчетные документы имеют фиксированный номинал – количество «условных единиц». Их платежно-расчетная способность уменьшается по мере проведения соответствующих операций, например поминутного разговора по таксофону. В виде условных единиц они переносят потраченные при покупке карты денежные средства на предмет оплаты до полной потери своей покупательной силы. Это так называемые «таксофонные», «проездные», «парковочные», «гостиничные», «бензиновые» и иные карты, имеющие локальное применение (в рамках одного эмитента). Вместе с тем их нельзя путать со *скрэтч-картами* (от англ. «scratch» – «царапина»)[130] одноразовой предоп-

---

[127] См.: Там же.

[128] См.: Там же.

[129] См.: Там же.

[130] Карты называются так потому, что для их использования необходимо острым предметом удалить защитный визуально непрозрачный слой («соскрести», «сцарапать» его) с определенного места подложки, чтобы стал виден цифровой номер – код одноразовой экспресс-оплаты. С помощью клавиатуры электронного терминального устройства (сотового радиотелефона или ПЭВМ), подключенного к сети электросвязи (сети ЭВМ), этот номер вводится в управляющую ЭВМ (сервер сети)

латы различных услуг, например экспресс-оплаты услуг сотовой электросвязи и Интернет, у которых машинный носитель не используется в платежно-расчетной операции, а служит лишь для защиты карты от подделки.

После полной отработки своего «денежного ресурса» карты выбрасываются за ненадобностью. Однако они могут быть заново активированы («подзаряжены») с помощью специального устройства – программатора, работающего под управлением персональной ЭВМ и специализированного программного обеспечения. Данным обстоятельством активно пользуются преступники.

1.3. *Электронные кошельки* – пластиковые платежно-расчетные карты, которые не связаны с открытием какого-либо счета у эмитента. Логически они выполняют роль обычного кошелька для хранения наличных денег с той лишь разницей, что в них находятся не обычные деньги, а их суррогаты– виртуальные деньги в виде электронных монет (ciber coin) или «купюр» более высокого номинала. Карта «подзаряжается электронными деньгами» у эмитента путем записи в ее память вида валюты и ее номинала соответствующих сумме валюты, внесенной картодержателем наличными деньгами в кассу эмитента. По механизму использования карты рассматриваемой категории сходны с картами предыдущей группы. Однако сфера их применения значительно шире. С их помощью можно производить не только безналичные, но и наличные расчетные операции, например обналичивать электронные деньги в обычные.

Сфера применения таких карт ранее ограничивалась рамками одного эмитента и использовалась в следующих платежных системах: Mondex, Geld Karte, Proton, VISACash. Вместе с тем внедрение этих карт в оборот активизировалось одновременно с принятием в начале текущего века и тысячелетия нового международного стандарта на электронный кошелек «CEPS»[131] (от англ. «Common Electronic Purse Standart» – общий стандарт на электронный кошелек). Благодаря ему, в настоящее время быстрыми темпами начали развиваться такие технологии электронной наличности, как: eCash (от англ. «electronic Cash» – электронные наличные деньги) фирмы DigiCash (от англ. «Digital Cash» – цифровые наличные деньги), Web Money Transfer («деньги для передачи по сети ЭВМ»), PayCash («оплата наличными деньгами»), CyberCash (от англ.

организации – эмитента карты. После чего сумма денежных средств, указанная в виде номинала карты, зачисляется на счет клиента – ее держателя.

[131] Подробнее см.: *Голдовский И.* Безопасность платежей в Интернете. – СПб., 2001. – С. 17-18.

«Cybernetic Cash» – «кибернетические наличные деньги»), SmartCity и другие. Например, технология SmartCity представляет собой комплексное решение на основе применения микропроцессорных карт стандарта CEPS, совместимого со стандартом обработки данных EMV, который позволяет использовать карты – электронные кошельки во многих платежных системах. Благодаря этому симбиозу, карты SmartCity обладают следующими характерными функциональными особенностями: автоматический учет и обработка всех наличных и безналичных платежно-расчетных операций; возможность одновременной работы в платежных системах различных эмитентов; поддержка нескольких кошельков и разных видов валют на одной карте; возможность проведения дебетовых и кредитных операций одновременно; многоязычный интерфейс[132].

1.4. *Дисконтные карты (discount cards)* – карты, эмитируемые предприятиями торговли и сферы услуг. Они выдаются постоянным клиентам и удостоверяют наличие определенной имущественной скидки (льготы), которая не взимается с картодержателя при оплате покупаемого товара или полученной услуги. Имущественная скидка определяется процентным номиналом, указанным на карте, а в случае его отсутствия – процентным или бонусным номиналом, заявленным продавцом на момент совершения расчетно-кассовой операции с использованием карты. Дисконт может устанавливаться на отдельные виды товаров (услуг) – избирательный дисконт либо на все товары (услуги) – общий дисконт. При этом денежная сумма, не взимаемая по дисконтной карте с ее предъявителя, отражается в кассовом чеке, на кассовой ленте, слипе или электронном документе, оформляемом при совершении операции. К этой категории пластиковых карт относятся и так называемые «клубные или ресторанные бонусные карты» или «карты почетных гостей».

2. Идентификационные карты (identification cards) – конфиденциальные документы, удостоверяющие личность или идентифицирующие электронный терминал в системе либо сети ЭВМ.

2.1. *Идентификационные карты личности.* Они содержат в своей памяти максимально полную идентифицирующую информацию об их держателе (персональные данные о личности)[133], а

---

[132] Подробнее см.: Технология SmartCity // *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты. – М., 2000. – С. 372-380.

[133] **Охраняемая законом информация о гражданах** – сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность. – См.: ст. 11 Закона Российской Федерации от 20.02.95 г. № 24-ФЗ «Об информации, информатизации и защите информации».

именно: фамилия, имя, отчество; адрес места работы и (или) жительства; фотография; отпечаток пальца руки, размер ладони, фоноскопия голоса и (или) рисунок сетчатки глаза; образец подписи; иные сведения о личности. Вся эта информация по своему правовому статусу относится к категории конфиденциальной – охраняемой законом. К картам выделенного вида относятся: карта учащегося общеобразовательного учреждения или студента, удостоверение личности, пенсионное удостоверение, международное студенческое удостоверение, полис обязательного медицинского страхования, медицинская карта пациента, именной пропуск на охраняемый объект и многие другие. Подчеркнем, что идентификационные карты личности – это именные документы.

2.2. *Идентификационные карты электронных терминальных устройств.* В память этих карт записывается код опознавания электронного терминального устройства в системе или сети ЭВМ по типу «свой – чужой». К ним относятся хорошо известные всем абонентам сотовой электросвязи SIM-карты, важным реквизитом которых является модуль идентификации абонента в сети радиосвязи («Subscriber Identity Module» – SIM). В его памяти содержится международный идентификационный номер абонента – IMSI (International Mobile Subscriber Identity), который является аналогом международного идентификационного номера мобильного терминала – IMEI (International Mobile Equipment Identity)[134], но никоим образом не зависит от него; закрытый (секретный) ключ авторизации[135] – Ki (Key Identity), который в паре с IMSI позволяет производит идентификацию абонента в сети (по такому принципу работает электронная цифровая подпись); персональные данные клиента – пользова-

[134] **IMEI** записывают во внутреннюю микросхему памяти сотового радиотелефона при его изготовлении. Этот идентификационный номер является заводским идентификационным номером радиотелефона как технического устройства. Он включается в технический паспорт и указывается в виде маркировки на корпусе радиотелефона. Маркировка представлена в виде человекочитаемой алфавитно-цифровой записи и машиночитаемого штрих-кода.

[135] **Авторизация** – это разрешение, предоставляемое эмитентом карты для проведения операции с ее использованием и порождающее его обязательство по исполнению представленных документов, составленных с использованием ее реквизитов. – См.: Ст. 1 Положения о порядке эмиссии кредитными организациями банковских карт и осуществления расчетов по операциям, совершаемым с их использованием // Письмо Центрального банка России от 09.04.98 г. № 23-П.

теля сотового радиотелефона, записываемые в процессе его эксплуатации, например электронная записная книжка[136].

После заключения Договора о предоставлении услуг сотовой электросвязи указанная карта выдается клиенту. При этом в его присутствии идентификационный микропроцессорный модуль удаляется из подложки методом штамповки и механически подключается к электрическим контактам сотового радиотелефона. При попадании последнего в зону действия данной радиосвязи модуль автоматически распознает код своего оператора и подключает телефон к сети. Абонент извещается об этом событии звуковым сигналом. Такое же событие происходит при выходе электронного терминала из зоны действия радиосвязи.

Карты рассматриваемого вида содержат в своей памяти сведения, относящиеся к разряду коммерческой тайны[137]. Поэтому они защищаются IMSI и ключом авторизации. С помощью модуля идентификации абонента в сети радиосвязи оператор обеспечивает конституционное право граждан (клиентов) на тайну телефонных переговоров и электронных SMS-сообщений[138] (от англ. «Single Message System» – «специальная система обмена сообщениями»).

3. Электронные ключи (e-Key). К этой группе нами относятся карты, выполняющие роль простого ключа (по аналогии с ключом механического замка), который предоставляет доступ физическому лицу на охраняемый объект, в помещение, хранилище или к компьютерной информации через специализированные автоматические КПП и иные терминальные охранные устройства, функционирующие на базе ЭВМ. Такие карты открывают электронные и электромеханические замки, задвижки и другие запорные приспособления, отключают охранную сигнализацию, дезактивируют средства защиты информации от несанкционированного доступа. В некоторых системах безопасности помимо «открывания двери» карты одновременно включают устройства автоматической регистрации параметров доступа на охраняемый объект: номер терминального устройства в ох-

---

[136] Не все SIM-карты имеют данный раздел в своей памяти. – Подробнее см.: *Потресов С.* На вечную память (хранение данных в мобильных телефонах) // CHIP. – 2003. – Март. – С. 88-90.

[137] В соответствии со ст. 139 ГК РФ, информация составляет коммерческую тайну в случае, когда она имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель такой информации принимает меры к охране ее конфиденциальности.

[138] Ч. 2 ст. 23 Конституции РФ.

ранной системе; дату и время дезактивации защиты; категорию ключа. Вместе с тем **они не позволяют идентифицировать личность и относятся к документам на предъявителя**.

4. Средства удостоверения электронных документов. В этом качестве пластиковая карта используется исключительно как аппаратно-программное средство обеспечения электронной цифровой подписи. На ее подложку и машинный носитель информации записывается открытый ключ ЭЦП (цифровой номер карты), а держателю карты вручается закрытый (секретный) ключ ЭЦП (ПИН-код). Данный вид пластиковых карт применяют только для заверения электронных документов с использованием указанной идентификационной пары. Созданный с использованием программ для ЭВМ электронный документ подписывается и заверяется ЭЦП так, если бы это был бумажный документ, заверенный собственноручной подписью уполномоченного на то должностного лица и (или) скрепленный печатью. При этом законодательство Российской Федерации с юридической точки зрения признает равенство ЭЦП в электронном документе указанным удостоверительным реквизитам в бумажном документе[139].

5. Комбинированные (многофункциональные) карты (multipurpose cards) – карты, которые по своему назначению выполняют не менее двух различных функций. Например, совмещают в себе функции удостоверения личности, электронного кошелька и пропуска на охраняемый объект. В последнее время они достаточно активно стали внедряться отечественными эмитентами – различными предприятиями и учреждениями. С помощью этих карт сотрудники конкретной организации проходят через автоматизированные КПП на свои рабочие места, получают зарплату в банкоматах, установленных на ее территории, оплачивают питание в столовых, а также другие товары и услуги ведомственных предприятий, имеют определенные имущественные скидки и другое.

По категории держателя

Держатель пластиковой карты – это физическое лицо, использующее карту по назначению на основании договора с эмитентом либо являющееся уполномоченным представителем клиента эмитента. Поскольку клиент эмитента может быть как физическим, так и юридическим лицом, карты целесообразнее всего подразде-

---

[139] О технологии использования таких карт подробнее см.: Закон Российской Федерации от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи».

лить и по этому основанию. Таким образом, имеем следующую их классификацию.

1. Карты физических лиц. В этом случае законным держателем карты является физическое лицо, имеющее соответствующие надлежащим образом оформленные документы, подтверждающие право владения и (или) распоряжения картой. Такими документами являются: паспорт или водительское удостоверение, если карта именная; товарный чек или чек ККМ, свидетельствующий о законном приобретении (покупке) карты у эмитента, если карта на предъявителя; договор с эмитентом или доверенность на право распоряжения (владения) картой, выданная физическим лицом – клиентом эмитента (для именных карт и карт на предъявителя); сертификат ключа ЭЦП (идентификационной пары) и сертификат средств ЭЦП (пластиковой карты), выданные удостоверяющим центром (для карт, являющихся средствами удостоверения электронных документов).

2. Корпоративные карты. Данная категория карт является собственностью юридического лица. Как правило, это банковские карты, которые позволяют их держателю – физическому лицу распоряжаться денежными средствами, находящимися на счете юридического лица, в пределах расходного лимита, установленного эмитентом в соответствии с условиями договора с клиентом – юридическим лицом[140]. Правом их использования обладает узкий круг физических лиц, уполномоченных от имени данного юридического лица расходовать в тех или иных пределах средства своей компании. На основе корпоративной карты организация также может выдать своим сотрудникам собственные именные карты. В основном, таким правом пользуются руководители различного ранга (исполнительные директоры, начальники служб и отделов, главные бухгалтеры и их заместители). На имя этих лиц открываются персональные счета, «привязанные» к карточному счету юридического лица. Всю имущественную и иную ответственность перед эмитентом по операциям, совершенным с использованием таких карт, несет организация, а не держатели карт[141].

Проведенное исследование показало, что криминалистически значимые сведения о пластиковой карте как предмете и основном

---

[140] См.: Ч. 1 п. 3.2 ст. 3 Положения о порядке эмиссии кредитными организациями банковских карт и осуществления расчетов по операциям, совершаемым с их использованием // Письмо Центрального банка России от 09.04.98 г. № 23-П.

[141] Подробнее см.: *Панова Г.С.* Новые банковские продукты и услуги // Банковское дело: Учебник / Под ред. проф. О.И. Лаврушина. – М., 1999. – С. 518.

орудии совершения преступлений отмеченной категории являются базовыми элементами их криминалистической характеристики. Они определяют содержание остальных ее составляющих. Рассмотрим их подробнее.

2.3. Сведения о некоторых типичных обстоятельствах совершения преступления и личности преступника

Важным условием качественного расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов, является правильное установление такого объективного элемента обстановки, как ***место преступления***. Оно является важным источником исходной информации о способе подготовки и совершения преступления выделенного вида, о личности преступника и особенностях потерпевшего, о времени и иных обстоятельствах.

В настоящее время в криминалистической науке не существует четкого определения этого понятия. По вопросу его содержания имеются различные точки зрения. Например, в отечественной юридической литературе и следственной практике в основном используются три термина: «*место происшествия*», «*место совершения преступления*» и «*место преступления*». При этом понятие и содержание «места совершения преступления» преимущественно используются в аспекте понятия места происшествия, которое употребляется в широком смысле. Этой проблеме было уделено достаточное внимание в работах Р.С. Белкина, А.Н. Васильева, И.Ф. Герасимова, В.А. Ручкина и других. Таким образом, видимо, целесообразно придерживаться общепринятого в криминалистике определения, в соответствии с которым *местом преступления признается* лишь та *территория, на которой оно было совершено*, а **местом происшествия**, соответственно, является *участок местности либо помещение, где произошло расследуемое событие, а также территория, где были обнаружены связанные с преступлением следы и предметы*[142].

Применительно к теме настоящей работы вышеуказанное положение имеет следующее отношение: *место происшествия и место совершения преступления могут не совпадать в пространстве*. Это обусловлено рядом объективных и субъективных факторов,

---

[142] См.: Криминалистика: Учебник для вузов МВД России. Т. 2: Техника, тактика организация и методика расследования преступлений / Редкол.: Смагоринский Б.П. (отв. ред.), Волынский А.Ф., Закатов А.А., Филиппов А.Г. – Волгоград, 1994. – С. 129.

среди которых следует выделить все возрастающую унификацию и взаимоинтеграцию средств электронно-вычислительной техники с современными системами цифровой электросвязи, имеющими неограниченный радиус действия и микропроцессорные модули управления. К этому также необходимо добавить мобильность и миниатюризацию указанных телекоммуникационных средств. Таким образом, с каждым годом расширяется география электронных платежных систем, основанных на безналичных финансовых операциях. Их базовым компонентом является **транзакция** – *электронно-цифровое информационное сообщение о проведении платежно-расчетной и иной финансовой операции*. Например, по мнению отдельных исследователей, такие системы электронной наличности, как «Mondex» и «DigiCash», уже попали в поле зрения отечественных правоохранительных органов, поскольку деньги в них оборачиваются в виртуальной (компьютерной) среде, не оставляя при этом следов, по которым можно было бы осуществлять контроль законности их происхождения. Этим создаются идеальные условия для отмывания денег, уклонения от уплаты налогов и иных обязательных платежей[143].

С научной точки зрения интерес представляет тот факт, что, начиная с 1992 г., отечественным преступным группировкам с помощью новейших средств электронно-вычислительной техники и спутниковой связи удалось подключиться к международной подпольной банковской системе для проведения собственных расчетно-кассовых операций в целях финансового обеспечения преступной деятельности[144]. Международной юридической практике известны также реальные случаи использования подпольной схемы криминальных расчетов в целях легализации денежных средств, полученных от продажи оружия и наркотиков. Она заключается в следующем. Преступник, являющийся гражданином одного государства, получает от «покупателя товара» – подданного другого государства не наличные деньги, а банковскую карту с ПИН-кодом. Вернувшись на территорию своего государства, преступник снимает из установленного в относительно безлюдном месте банкомата требуемую «чистую» сумму наличных денег в соответствующей валюте. Такая криминальная схема получила большое

---

[143] См.: *Максимова Е.Н.* Электронные анонимные платежи как инструмент и объект преступной деятельности // Компьютерная преступность: состояние, тенденции и превентивные меры ее профилактики: Материалы междунар. науч.-практ. конф. Ч. 2 / Под общ. ред. В.П. Сальникова. – СПб., 1999. – С. 154.

[144] Подробнее см.: Подпольная банковская система // Борьба с преступностью за рубежом. – 1992. – № 8. – С. 3-9.

распространение в государствах Центральной, Восточной и Южной Азии, например в Китае, Индии и Пакистане. Ее услугами широко пользуются европейцы – члены организованных преступных групп и сообществ[145].

С учетом изложенного следует подчеркнуть, что *пространственное несовпадение места совершения общественно опасного деяния с местом реального наступления общественно опасных последствий – типично для преступлений, совершенных с использованием пластиковых карт и их реквизитов*. Поэтому местом совершения данных преступлений будут как конкретные точки и участки местности, так и те помещения организации или жилища, в которых установлены электронные терминалы – банкомат, ККМ с импринтером или считывателем машинного кода, бимчекер, ридер КПП, ПЭВМ и другие, позволяющие производить какие-либо операции с пластиковыми картами и их реквизитами. Следовательно, по делам рассматриваемой категории *мест происшествия будет несколько*, в том числе значительно удаленных друг от друга и расположенных как в разных странах, так и на различных континентах. Ярким примером этому может служить факт того, что 14 декабря 1996 г. компания «America On Line (AOL)» исключила Россию из списка своих постоянных клиентов по причине резкого увеличения количества мошенничеств с использованием банковских карт со стороны российских пользователей. По словам официального представителя AOL в Российской Федерации, специалисты компании зафиксировали «лавинообразное увеличение попыток российских клиентов расплачиваться за услуги, предоставляемые компанией на рынке электронных платежей и взаиморасчетов, с помощью чужих номеров кредитных карт зарубежных клиентов»[146]. В общей сложности, AOL обслуживала клиентов в 40 городах России, предоставляя им весь спектр услуг, равно как и пользователям других государств. Это значит, что любой желающий мог с помощью модема и своего персонального компьютера, указав свое имя и номер кредитной карты, зарегистрироваться на сайте AOL[147] в

---

[145] См.: Основы борьбы с организованной преступностью: Монография / Под ред. В.С. Овчинского, В.Е. Эминова, Н.П. Яблокова. – М., 1998. – С. 19.

[146] America On line защищает своих абонентов // Защита информации. Конфидент. – 1997. – № 2. – С. 10.

[147] **Сайт** – интерактивная программа для ЭВМ, обеспечивающая обмен информацией между ее создателем и пользователями сети Интернет. В нашем случае сайт выполняет функции виртуального магазина услуг, предоставляемых компанией AOL держателям банковских карт, а именно: пользователь сети Интернет (заказчик) выбирает на интерактивной рекламной электронной странице (витрине магазина)

глобальной компьютерной сети Интернет и получать возмездные услуги. Компания верит своим клиентам и не проверяет их кредитоспособность (совпадение указанного имени с именем лица, обладающего банковским счетом и соответствующей картой[148], номер которой был указан). Российские клиенты были лишены права на получение услуг AOL с того момента, когда в головном офисе компании стали раздаваться звонки от возмущенных держателей кредитных карт, которые стали получать счета и уведомления из России за якобы оказанные им там услуги. У сотрудников AOL возникли также подозрения, по поводу резкого увеличения числа подключений к сайту компании и длительности сеансов работы с ним российских клиентов, поскольку стоимость сеанса этой связи в России на тот момент времени составляло около 34 долларов США за 1 час (что было в 3 раза дороже, чем в США), и далеко не все могут себе позволить такие расходы[149].

Видимо, в силу вышеуказанных обстоятельств в 13 % случаев установить место преступления рассматриваемого вида не представилось возможным. Изучение следственной практики, проведенное П.Б. Смагоринским, показало, что им чаще всего являются: торговый зал магазина (предприятия сферы торговли) – 31 %; клиентское помещение гостиницы, бара, ресторана, ж/д вокзала, станции метро, почты (предприятия сферы услуг) – 24 %; точка либо участок местности, где установлен стационарный электронный терминал для проведения операций с использованием пластиковых карт (место установки таксофона, банкомата, автоматизированной бензоколонки и КПП метрополитена) – 19 %; обменный пункт валюты, операционный зал либо касса банка – 15 %; территория объекта, охраняемого с помощью автоматизированной компьютерной системы и электронных контрольно-пропускных терминалов (база, склад, гараж, автостоянка) – 11 %.

Если проанализировать соотношение мошенничества с использованием пластиковых карт по сервисным предприятиям (мерчантам),[150] то выясняется, что в 26,4 % случаев они совершаются в

название необходимой ему услуги, отмечает ее, а затем оплачивает путем сообщения программе своего имени и номера банковской карты. После совершения указанных операций услуга оказывается тому, чье имя было указано, а деньги перечисляются на счет магазина со счета того держателя, реквизиты карты которого были указаны.

[148] Такой банковский счет называется «**специальным карточным счетом – СКС**».

[149] См.: Указ соч. – С. 10.

[150] **Мерчант** – предприятие торговли или сферы услуг – физическое или юридическое лицо, которое в соответствии с подписанным им соглашением (договором) с

ресторанах и барах, 25 % – в гостиницах, 20,7 % – в магазинах, 10,6 % – в казино и варьете, 9,9 % – на бензозаправках, 7,4 % – в местах установки телефонных терминалов[151].

С учетом изложенного можно сделать вывод о том, что ***типичным местом совершения преступления*** *выделенной категории является пространственная точка, на которой осуществляются какие-либо операции с использованием реквизитов пластиковых карт и СВТ, обеспечивающих их обработку*. Вместе с тем, рассматривая связь места совершения преступления с предметом посягательства, нельзя не поддержать точку зрения Н.М. Сологуба, С.Г. Евдокимова и Н.А. Даниловой, определяющих место хищения как место создания источников хищения (либо сокрытия недостачи при хищении имущества, вверенного преступнику), а также место изъятия и (или) обращения чужого имущества в пользу преступника и других лиц[152]. При этом под источником хищения ими понимается материальная база, используемая в процессе хищения, а именно: подотчетные ценности; резервные ценности, создаваемые преступником на своем производственном участке (рабочем месте); сторонние ценности; неучтенная продукция[153].

Криминалистически значимые сведения о месте совершения преступления выделенной категории находятся в корреляционной зависимости с характеристикой ***типичных потерпевших*** – физических и юридических лиц, которым был причинен значительный имущественный ущерб. Так, например, в случае совершения мошенничества в отношении держателя карты, проанализировав данные о часто посещаемых им местах (конкретный магазин, бар, ресторан, гостиница, бензозаправка и др.), что зависит от его привычек, можно точно определить место совершения преступления, выйти на след преступника, а в некоторых случаях – установить его личность (в данном случае им вероятнее всего будет сотрудник обслуживающего предприятия, где потерпевший чаще всего расплачивается с помощью карты). В то же время, получив при осмотре места происшествия информацию о реквизитах, содержащих

эмитентом или эквайрером несет обязательства по приему документов, составленных с использованием платежно-расчетных карт в качестве оплаты за предоставляемые товары (услуги).

[151] См.: Организованная преступность и частные инвестиции: Учеб. пособие / Под ред. В.И. Попова, А.С. Овчинского. – М., 1998. – С. 330.

[152] См.: *Сологуб Н.М., Евдокимов С.Г., Данилова Н.А.* Хищения в сфере экономической деятельности: механизм преступления и его выявление: Метод. пособие. – М., 2002. – С. 33-34.

[153] См.: Там же. – С. 9.

сведения о личности держателя карты, и сопоставив их с показаниями свидетелей – работников мерчанта, устанавливают конкретного потерпевшего – постоянного клиента, а иногда и преступника, который маскируется под него с помощью поддельного удостоверения личности. Следует также помнить о том, что в большинстве случаев при совершении операции с применением пластиковой карты всегда остаются документы, позволяющие установить лицо, совершившее данные действия, и (или) определить потерпевшего – законного держателя карты. В этом случае имеет место жесткая взаимосвязь криминалистических признаков пластиковой карты конкретного вида с типичным местом совершения преступления и данными о личности потерпевшего.

Отмеченные ***криминалистически значимые связи потерпевшего с предметом и (или) орудием преступления, местом его совершения и преступником*** необходимо учитывать в процессе раскрытия и расследования хищений выделенной категории.

Исследуя ***вопрос о времени совершения преступления с использованием пластиковой карты или ее реквизитов***, представляется, что его необходимо рассматривать в контексте уголовно-правового понятия окончания преступного деяния, когда временем совершения каждого преступления признается время окончания общественно опасного деяния независимо от времени наступления последствий (ч. 2 ст. 9 УК РФ). Рассматриваемый элемент криминалистической характеристики обусловлен многоэпизодностью указанных преступных деликтов. Таким образом, следует вести речь о *продолжаемом преступлении*, слагающемся из ряда тождественных деяний, направленных на достижение единой цели и своей совокупностью образующих единое преступление.

Комплексный анализ материалов уголовных дел и содержания различных учетно-регистрационных бухгалтерских документов по операциям с использованием пластиковых карт показывает, что дата, время (с точностью до минут и секунд) и место совершения преступления рассматриваемого вида в большинстве случаев достаточно легко устанавливаются путем изучения реквизитов различных документов, остающихся при проведении каждой операции с использованием пластиковой карты. Чаще всего эти документы оформляются при помощи автоматических и полуавтоматических электронных терминальных устройств (см. таблицу).

Таблица

Местонахождение документов – вещественных доказательств, остающихся после проведения операции, совершенной с использованием пластиковой карты или ее реквизитов

Название терминального регистрирующего устройства	Режим оформления документа	Название документа	Местонахождение документа
Таксофон	Автомат.	Таксофонная карта	– у лица, осуществившего операцию
Турникет (терминал) автоматизированного КПП	Автомат.	Пластиковая карта	– у лица, осуществившего операцию
ЭВМ, управляющая системой охраны объекта и (или) турникетом	Автомат.	Электронный журнал	Пульт централизованной охраны объекта (ПЦО)
ЭВМ или видеомагнитофон системы видеонаблюдения и контроля доступа на охраняемый объект	Автомат.	Видеодокумент (на машинном носителе информации)	Пункт охраны объекта
Сервер – управляющая ЭВМ сети электросвязи и авторизации операций по картам	Автомат.	Электронный сводный отчет: outgoing.file; incoming.file; detailed position; account position	База данных сервера оператора электросвязи, эмитента, эквайрера или процессингового центра платежной системы
Технологическая ЭВМ оператора электросвязи, эмитента, эквайрера или процессингового центра платежной системы	Полуавтомат.	Сводный отчет об операциях по карте за определенный промежуток времени (выписка по счету) – биллинг	Оригинал – у эмитента карты; копия – в виде бумажной распечатки у держателя карты
Импринтер	Полуавтомат.	Слип	1-й экземпляр – у лица, предъявившего карту для совершения операции (держателя карты); 2-й – у кассира, осуществившего операцию по карте; 3-й – в банке-эквайрере

Продолжение таблицы

Контрольно-кассовая машина (ККМ) с ридером – считывателем электронных реквизитов с пластиковых карт	Полуавтомат.	1. Кассовый чек	– у лица, предъявившего карту для совершения операции (держателя карты)
		2. Контрольная кассовая лента	– у кассира, осуществившего операцию по карте
		3. Электронный журнал	– в фискальной памяти ККМ; в ее памяти счетчиков (регистров) совершенных операций
Торговый автомат (автомат по продаже товаров)[154]	Автомат.	1. Квитанция; 2. Платежно - расчетная карта	– у лица, осуществившего операцию
		3. Контрольная кассовая лента	– в торговом автомате
		4. Электронный расходный реестр	– в памяти торгового автомата
Банкомат	Автомат.	1. Квитанция; 2. Банковская карта	– у лица, осуществившего операцию
		3. Контрольная кассовая лента	– в банкомате
		4. Электронный журнал	– в фискальной памяти банкомата; в его памяти счетчиков (регистров) совершенных операций
		5. Электронный расходный реестр	– в памяти банкомата
Бимчекер	1. Полуавтомат.	1. Кассовый чек	– у лица, предъявившего карту для совершения операции (держателя карты)
	2. Автомат.	2. Электронный журнал	– в фискальной памяти бимчекера; в его памяти счетчиков (регистров) совершенных операций

По существующим правилам при работе на всех ККМ, бимчекерах и в банкоматах в обязательном порядке применяется кон-

[154] Подробнее см.: Ст. 498 «Продажа товаров с использованием автоматов» ГК РФ.

трольная кассовая лента. Она является копией кассового чека или квитанцией торгового автомата или банкомата и должна храниться у мерчанта в упакованном виде в течение 15 дней после проведения последней инвентаризации и проверки товарного отчета. На кассовых чеках должны применяться условные шифры, штампы с указанием следующих реквизитов: название лица (физического или юридического), которым выдан чек; дата и время проведения операции; шифр электронного терминального устройства, отпечатавшего чек; порядковый номер чека или проведенной операции за контрольно-учетный период; наименование произведенной операции; сумма и наименование валюты операции[155]. При этом под кассовым чеком (чеком покупателя) понимается квитанция кассы о приеме денег от клиента в виде чека, свидетельствующего об оплате товара или оказываемой возмездной услуге и дающего право получить оплаченный товар или услугу[156].

В соответствии со ст. 1 Закона Российской Федерации от 22.05.03 г. № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт» ***контрольно-кассовая техника***, используемая при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт, представляет собой ***контрольно-кассовые машины (ККМ), оснащенные фискальной памятью***, ***электронно-вычислительные машины (ЭВМ)***, ***в том числе персональные (ПЭВМ)***, ***программно-технические комплексы (ПТК).*** Причем **фискальная память** – это *комплекс программно-аппаратных средств в составе контрольно-кассовой техники, обеспечивающих некорректируемую ежесуточную (ежесменную) регистрацию и энергонезависимое долговременное хранение итоговой информации, необходимой для полного учета наличных денежных расчетов и (или) расчетов с использованием платежных карт, осуществляемых с применением контрольно-кассовой техники, в целях правильного исчисления налогов*. Эта информация называется «***фискальные данные***». По каждой расчетно-кассовой операции они одновременно фиксируются в фискальной памяти электронного терминала в форме

---

[155] См.: Положение по применению контрольно-кассовых машин при осуществлении денежных расчетов с населением в Российской Федерации // Постановление Совета Министров – Правительства РФ от 30.07.93 г. № 745 (с изм. и доп. от 03.09.98 г. № 1027). – П. 5 и 7.

[156] См.: *Райзберг Б.А., Лозовский Л.Ш., Стародубцева Е.Б.* Современный экономический словарь. – М., 1997. – С. 383.

электронного документа и на бумажной контрольной ленте, если электронный терминал укомплектован соответствующим модулем печати.

Вместе с тем, если осуществляется не финансовая, а информационная операция, чек не оформляется (за исключением банкомата). В этом случае, исследованию подлежат иные документы, которые оформляются средствами автоматического документирования операций и событий. Обычно они входят в состав автоматизированных охранных систем. Так, например, для охраны банкоматов и других терминальных устройств, касс, торговых и производственных площадей в последнее время достаточно широко стали применяться системы скрытого видеонаблюдения и контроля доступа, запечатлевающие все события, происходящие на охраняемой территории. Такие системы предусматривают фиксацию событий в реальном масштабе времени с одновременным отображением на видеопленке или машинном носителе информации о дате и текущем времени (иногда продолжительности) происходящего события, которое интересует следствие.

К сожалению, точно установить дату и время происшедшего события возможно не всегда. Дело в том, что некоторые терминальные устройства, не предусматривают автоматическую фиксацию операций, совершаемых с использованием пластиковых карт и их реквизитов. Они не оборудуются и специальными охранными и документирующими системами. Рассматриваемые терминальные устройства, как правило, работают с картами – безличными документами: с фиксированной покупательной способностью или электронными ключами. В качестве примера можно привести отдельные виды таксофонов, турникеты КПП, простейшие электронно-механические запорные устройства и другие. Особое значение в вопросе определения даты и времени совершения преступления здесь будет играть получение и изучение сотрудником органа предварительного расследования сведений о периодах и времени работы конкретных потерпевших, помещений или участков местности предприятий (учреждений, организаций), где установлено соответствующее терминальное устройство, а также его индивидуальный график работы.

Очевидно, что существует жесткая причинно-следственная связь между преступлением и тем, кто использовал отдельные негативные особенности оборота пластиковых карт для его совершения.

Известно, что отдельные ***сведения о личности преступника*** являются неотъемлемым структурным элементом криминалистической характеристики любого вида преступлений, в том числе совершенных с использованием пластиковых карт и их реквизитов.

С этих позиций субъект преступного посягательства является предметом исследования криминалистики. Такая информация, как указывал Р.С. Белкин, «позволяет сузить круг лиц, среди которых может находиться преступник, и дает возможность выдвинуть версии о мотиве и цели преступления, способе его совершения и сокрытия (как и наоборот), месте нахождения искомых объектов и т. п.»[157].

Как не без основания полагают многие исследователи, подготовка и совершение преступления выделенного вида требует наличия у преступника определенных знаний в области особенностей оборота пластиковых карт[158], подробно рассмотренных ранее по тексту настоящей работы. Набор специальных знаний диктуется избранным преступником способом преступления, или наоборот – имеющийся набор сведений определяет выбор того или иного способа.

Анализ следственной и судебной практики показывает, что одному лицу достаточно сложно решить весь комплекс возникающих проблем по подготовке, совершению и сокрытию преступного деяния. Поэтому, нередко, на этих этапах действуют разные лица. Так, например, кражи пластиковых платежно-расчетных карт совершают проститутки, воры – карманники и домушники, обслуживающий персонал гостиниц. Эти субъекты сразу же сбывают похищенные карты, не рискуя самостоятельно осуществить мошеннические операции с их использованием или просто не владея достаточными знаниями для успешного окончания такой операции. В связи с чем на следующем этапе совершения преступного посягательства рассматриваемой категории чаще всего действуют преступники из числа работников предприятий – мерчантов, к которым карты или составленные с их использованием слипы поступают как напрямую, так и через цепочку посредников[159]. В свою очередь, указанные лица передают необходимую информацию об этих картах и их реквизитах преступникам, специализирующимся на подделке данных документов. После чего собственно и совершается преступление с

---

[157] *Белкин Р.С.* Криминалистика: проблемы, тенденции, перспективы. От теории к практике. – М., 1988. – С. 178.

[158] Например, см.: *Астапкина С.М.* Защита интересов банков и вкладчиков от преступного использования пластиковых платежных средств // Криминальные расчеты: уголовно-правовая охрана инвестиций. – М., 1995. – С. 69; *Улейчик В.В.* Расследование хищений, совершаемых в кредитно-финансовой сфере с использованием электронных средств доступа // Компьютерная преступность: состояние, тенденции и превентивные меры ее профилактики: Материалы междунар. науч.-практ. конф. Ч. 2 / Под ред. В.П. Сальникова. – СПб., 1999. – С. 152-153.

[159] См.: *Астапкина С.М.* Указ. соч. – С. 69.

использованием подлинных или поддельных карт либо только их реквизитов.

Иногда имеют место и случаи инсценировок, когда исполнителем преступления является сам держатель карты, заявивший об ее утрате, либо работник мерчанта, эквайрера или эмитента, заявивший об утрате карты, находившейся в его ведении в силу исполнения должностных обязанностей[160].

Зарубежная[161] и отечественная практика борьбы с «карточным мошенничеством» свидетельствует о том, что среди субъектов могут быть работники почтовых учреждений, входящие в состав организованных преступных групп и сообществ, специализирующихся на совершении этих преступлений. Например, известен случай, когда в московском аэропорту «Шереметьево-2» была разоблачена преступная группа грузчиков, которые, действуя по заданию преступного сообщества, контролировавшего эту территорию, изымали банковские карты из международных почтовых отправлений[162].

Анализ содержания печатных публикаций в официально зарегистрированном и издаваемом на территории Российской Федерации Журнале компьютерных хулиганов «Хакер», а также электронных информационных сообщений на хакерских сайтах сети Интернет позволяет сделать вывод о существовании так называемых **«кардеров»** (от англ. «card» – карта) – лиц, специализирующихся на незаконной деятельности в сфере оборота пластиковых карт и их реквизитов. При этом в среде кардеров существует четкое разделение «труда». Первые – организуют и руководят деятельностью преступной группы либо разрабатывают и организуют исполнение конкретной криминальной операции. Их на блатном жаргоне называют «элитой» (на англ. «elite») – это лучшие, хорошо охраняемые и высокопрофессиональные представители кардерского преступного сообщества (по типу «воров в законе»). Как правило, они неизвестны другим членам ОПГ. Связь с ними поддерживается с использованием средств Интернета и другими методами, не позволяющими точно установить личность и местопребывания абонента. Вторые – добывают орудия и материалы для разработки средства совершения преступления: пластиковые карты, их образцы (заготовки) и конфиденциальные реквизиты – «дампы», а также

---

[160] См.: Организованная преступность и частные инвестиции: Учеб. пособие / Под ред. В.И. Попова, А.С. Овчинского. – М., 1998. – С. 336.

[161] См., например: *Charles H. McCaghy.* Computer crime // Crime in American society. – N.Y.; London, 1980. – P. 232.

[162] См.: Организованная преступность и частные инвестиции. – С. 336.

специальные технические средства для негласного получения необходимой информации. Третьи – изготавливают соответствующие орудия совершения преступления: поддельные пластиковые карты и (или) слипы, а также документы, подтверждающие «законное» право владения и распоряжения ими. Четвертые – «мулы», «ишаки» (от названия домашнего животного) – являются курьерами. Они отвечают за перевозку орудий совершения преступления и денег, полученных от их использования. Пятые – собственно совершают преступления с использованием поддельных пластиковых карт и их реквизитов. В криминальной среде их называют «троперами» (от англ. «trooper» – солдат) или «танкистами», т. е. лицами, первыми «принимающими на себя огонь» правоохранительных органов и «гибнущими» в случае провала криминальной операции.

Рассматриваемые субъекты обладают достаточно высокими знаниями и практическими навыками в области компьютерной техники, новых телекоммуникационных и репрографических печатных технологий, криптографии и электронного бухгалтерского документооборота. У многих кардеров есть индивидуальный «ник» (кличка) – псевдоним, под которым они общаются между собой, в том числе и в сети Интернет. Кардеры имеют свои сайты в сети Интернет, проводят электронные конференции (форумы) по «обмену опытом», публикуют на электронных досках объявления с предложениями своих «услуг» или «работы», имеют свой жаргонный словарь (приложение 2). В таких «литературных» источниках имеются все необходимые сведения и специальные программы для ЭВМ, направленные на вовлечение подростков и молодежи в противоправную деятельность, а также повышение профессионального мастерства начинающего правонарушителя – методики, конкретные способы и соответствующие программные средства совершения и сокрытия «карточных преступлений», от самых простых до очень изощренных и сложных. Особое опасение вызывает тот факт, что российские кардеры тесно контактируют с зарубежными, обмениваясь с ними преступным опытом. В подтверждении этому можно привести следующий пример.

Весной 2003 г. сотрудниками УБЭП ГУВД г. Москвы была пресечена деятельность преступной группы из числа студентов столичных вузов, которые в течение четырех месяцев с использованием поддельных банковских карт совершали хищения наличных денежных средств из банкоматов, установленных на улице Садовое кольцо. Общая сумма причиненного ущерба составила более 700 тыс. долларов США. Все обязанности по подготовке и совершению

преступлений были четко распределены между участниками преступной группы следующим образом.

Первые – А.М. и Ю.К., являющиеся студентами московского технического вуза, занимались незаконным получением конфиденциальных реквизитов карт. С этой целью ими был разработан и использован комплекс технических устройств для негласного получения информации. Он состоял из цифровой микровидеокамеры и специального устройства, считывающего данные с магнитной полосы карты. Эти орудия совершения преступления искусно камуфлировались под технологические элементы банкомата. При этом микровидеокамера устанавливалась с таким расчетом, чтобы зафиксировать ПИН-код, набираемый с клавиатуры данного терминала; считыватель, выполненный в виде рамки, прикреплялся к входному отверстию, в которое вставляется карта для осуществления операции. Таким образом, в руках у преступников оказывались все необходимые реквизиты.

Вторые – по полученным конфиденциальным реквизитам изготавливали поддельные карты.

Третьи – с помощью поддельных карт и соответствующего ПИН-кода снимали наличные денежные средства из банкомата.

Четвертые – прикрывали первых и третьих в момент проведения криминальной операции.

Пятые – обеспечивали преступную группу соответствующими орудиями и материалами, применяемыми в ходе подготовки и совершения хищения. Для этого по сети Интернет ими были установлены контакты с кардерами из Франции. На их счета российскими преступниками отправлялась часть похищенных средств, а на адреса электронной почты (e-mail) сведения о реквизитах карт потерпевших для повторного использования в корыстных целях. Взамен французские «коллеги» отправляли персонализационное оборудование, расходные материалы к нему и стандартные заготовки пластиковых карт с магнитной полосой.

Как следует из вышеизложенного, вся преступная деятельность субъектов условно делится на три основных, довольно обособленных этапа: первый – подготовка к преступлению; второй – непосредственная реализация преступного замысла; третий – использование предметов преступления.

Известно, что при описании криминалистической характеристики преступлений, выделяются несколько этапов, отражающих своеобразные, ***типичные закономерности формирования*** тех или иных ***действий преступников на определенных этапах***. Специфика последних обусловливает профессиональный состав пре-

ступных групп, личностные характеристики их участников, процесс и особенности следообразования. Зная эту специфику, можно понять содержание, формы и способы преступной деятельности каждого члена группы на интересующем следствие этапе, получив тем самым максимально полное представление о механизме преступления. В конечном итоге это позволяет создать модель конкретного длящегося во времени преступления, а затем – спрогнозировать весь процесс его раскрытия и расследования.

Этап подготовки преступлений рассматриваемого вида в большинстве случаев завершается созданием преступной группы. Причем в 2/3 – это группа лиц по предварительному сговору и лишь в 1/3 – организованная преступная группа (ОПГ). Как показывают исследования, проведенные П.Б. Смагоринским, на данном этапе преступниками в 81 % случаев подготавливались средства совершения преступления, 76 % – заранее составлялся план криминальной операции, 73 % – отрабатывались способы совершения преступления, 68 % – распределялись роли между соучастниками по принятой иерархии и преступным способностям.

В свою очередь, этап реализации преступного замысла начинается с момента прибытия преступника (-ов) на конкретное место совершения хищения либо непосредственного начала осуществления криминальных операций в месте, где установлен электронный терминал. Затем, в зависимости от вида терминального устройства и особенностей проведения конкретной операции, по имеющейся на месте происшествия инструкции (находится у оператора или вывешена на самом терминале) осуществляются необходимые действия с пластиковой картой и терминальным устройством. Этап завершается непосредственным изъятием и (или) обращением чужого имущества в пользу преступника и других лиц. Например, путем незаконного электронного перевода денежных средств со специального карточного счета потерпевшего на свой или указанный организатором ОПГ банковский счет.

Последний этап – использование результатов преступления. Он включает в себя: распределение полученных средств между соучастниками; оплату услуг лицам, оказавшим содействие преступной группе, но не входящим в нее и не принимавшим непосредственного участия в преступлении (консультантам, лицам, предоставившим необходимые документы, оборудование, материалы и другим); создание своеобразного фонда денег («общака») из части похищенных средств для обеспечения преступной деятельности в будущем и нейтрализации возможного

противодействия со стороны властных структур, контролирующих, проверяющих и правоохранительных органов.

Подводя некоторую черту в вопросе изучения содержания структурных элементов криминалистической характеристики преступлений, совершенных с использованием пластиковых карт и их реквизитов, следует отметить, что поскольку способы преступлений являются ее стержневой основой, то целесообразно выделить их исследование в самостоятельный параграф настоящей главы работы.

§ 3. СПОСОБЫ ПРЕСТУПЛЕНИЙ, ОСНОВАННЫЕ НА ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ ПЛАСТИКОВЫХ КАРТ, И ТИПИЧНЫЕ СЛЕДЫ ИХ ПРИМЕНЕНИЯ

Из первого параграфа настоящей главы следует, что под *способом совершения преступления* в криминалистическом смысле *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 события, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить наиболее оптимальные методы решения задач раскрытия и расследования преступления*.

Анализ зарубежной и отечественной специальной литературы, материалов конкретных уголовных дел позволяет выделить следующие общие группы способов совершения хищений имущества, основанные на использовании технологий пластиковых карт:

1. Использование подлинных карт.
2. Использование конфиденциальной информации о реквизитах подлинных карт и их держателях.
3. Использование поддельных карт.
4. Использование несовершенства программно-аппаратного обеспечения технологии обращения пластиковых карт.

Каждая из указанных групп объединяет способы только по одному общему признаку. При этом частные признаки характеризуют индивидуальность конкретных способов, входящих в ту или иную группу и в значительной степени влияющих на предмет доказывания по уголовному делу. Рассмотрим их подробнее.

3.1. Использование подлинных карт

Способы, основанные на мошеннических операциях с подлинными пластиковыми картами, являются наиболее простыми в подготовке и исполнении. Для их реализации не требуются особые специальные знания – достаточно обычных знаний, которыми обладает каждый держатель карты. Именно поэтому они были первыми использованы преступниками в отечественной криминальной практике.

В настоящее время известны следующие их разновидности.

1. Хищение денежных средств, принадлежащих банку, путем получения карты по поддельному удостоверению личности либо на подставное лицо. Преступником по подложным документам (похищенным, найденным, приобретенным по сговору с их законным владельцем) в банке-эмитенте или эквайрере открывается специальный карточный счет (СКС) с внесением на него минимально необходимой денежной суммы. После чего «на законных» основаниях получается банковская карта для ведения платежно-расчетных операций. В качестве документов на открытие счета, как правило, используются чужие гражданские паспорта. Учитывая особенности операционной работы по кредитным картам, мошенники умышленно совершают многократные сверхлимитные операции с последующим невозвращением перерасходованных денежных средств. Найти субъекта в данном случае бывает очень затруднительно, поскольку он документально маскируется под лицо, от имени которого открыт счет.

2. «Воздушный змей». В двух или нескольких банках мошенниками открывается множество СКС, расчеты по которым могут производиться с банковскими картами одной или нескольких платежных систем. На одну из таких карт (ее СКС) ложится некоторая сумма денежных средств в валюте. Как правило, банки, эмитирующие кредитные и дебетовые карты, для привлечения клиентов допускают определенную сумму перерасхода средств при проведении платежно-расчетных операций в том случае, если СКС не закрывается. Иными словами, предоставляется отсрочка по сверхлимитному платежу на определенную сумму, заранее оговоренную в договоре на обслуживание карты. Данной технологической особенностью и пользуются преступники. Они полностью с допустимым перерасходом снимают денежные средства с указанного счета и переводят эту сумму на второй карточный счет, с которого, в свою очередь, все средства также снимаются с перерасходом и переводятся на третий. Это повторяется многократно до тех пор, пока денежная сумма не

достигнет размера, устраивающего мошенников. После чего деньги оперативно снимаются наличными через уличный банкомат. Все криминальные операции должны быть проведены в течение одного биллингового цикла – 30 дней – до момента наступления срока платежей за произведенные операции.

Иногда, для сокрытия следов преступления, мошенники многократно конвертируют валюту с использованием банкоматов различных эмитентов либо производят покупку дорогостоящей вещи на всю похищенную сумму (золотые украшения, меховые изделия и т. д.), расплачиваясь при этом пластиковой картой.

Документы, в которых необходимо искать следы рассмотренного способа совершения преступления:

- справки из процессинговых центров международных платежных систем, к которым относятся карты, о превышении их держателями установленного лимита;
- выписки из сводных (биллинговых) отчетов по СКС, по которым допущен перерасход денежных средств (находятся у эмитента);
- выписки из сводных отчетов по операциям, совершенным с использованием интересующих карт, за определенный период времени (находятся у эквайрера);
- выписки из сводных отчетов по кассовым операциям, совершенным с использованием интересующих карт, за определенный период времени (находятся у мерчанта);
- первичные расчетно-кассовые документы (бумажные кассовые ленты, кассовые чеки, квитанции электронных терминалов, слипы, электронные расходные реестры и другие документы из электронных журналов)[163], оформленные с использованием проверяемых карт, а также по 1-3 операциям, произведенным до и после операции, интересующей следствие (для установления очевидцев (свидетелей) преступления);
- комплект документов на открытие специальных карточных счетов, по которым был допущен перерасход денежных средств (заявление, договор или соглашение об открытии СКС; приходный или мемориальный ордер на перечисление держателем денежных средств на обеспечение СКС; мемориальный ордер по выдаче ценностей – карты; справку по форме 04006007);
- заявления лиц об утрате гражданских паспортов.

---

[163] В соответствии с Законом Российской Федерации от 21.11.96 г. № 129-ФЗ «О бухгалтерском учете» эти документы относятся к первичным учетным документам, которые составляются в момент или непосредственно после завершения финансовых операций и являются первым свидетельством их совершения.

3. Хищение денежных средств недобросовестным держателем карты путем обмана или введения в заблуждение ее эмитента.

3.1. Отказ держателя от операции, совершенной по реквизитам его карты. В процессе проведения расчетов по карточным сделкам достаточно часто возникают ситуации, когда держатели карт оспаривают обоснованность отдельных платежных операций, указанных в биллинге, и требуют возврата списанных с их счета денежных сумм. Иными словами, они отказываются от оплаты счетов, в которых указаны реквизиты принадлежащих им платежно-расчетных карт. Такая возможность предоставлена держателям действующим гражданским законодательством России, нормативными актами и договорами, регулирующими взаимоотношения сторон по этому вопросу. Все участники карточных взаиморасчетов прекрасно понимают, что в сложнейших технических системах, обслуживающих электронные платежи, периодически происходят сбои и отказы в работе программ для ЭВМ и оборудования. В результате чего возникают (или потенциально могут возникнуть) ошибки различного рода, которые приводят к самопроизвольной автоматической регистрации той или иной финансовой операции, реально никем не совершенной; завышению суммы произведенной операции; изменению кода валюты платежа, реквизитов плательщика или его банка. Причем убытки, возникшие вследствие оплаты плательщиком подложного, похищенного или утраченного чека (слипа, банковской карты), возлагаются на плательщика или чекодателя (держателя карты) в зависимости от того, по чьей вине они были причинены (ч. 4 ст. 879 ГК РФ). Таким образом, с учетом вышеуказанных объективных и субъективных обстоятельств организации – эмитенты платежно-расчетных карт изначально закладывают в смету своих расходов специальные финансовые резервы на покрытие возможных потерь. Резервы создаются на основании Инструкции Центрального банка России от 30.06.97 г. № 62а «О порядке формирования и использования резерва на возможные потери по ссудам»[164].

Получив от эмитента возврат и не получив от него денег в счет покрытия денежной суммы, выплаченной мерчанту за проведенную операцию по пластиковой карте, эквайрер зачисляет ее на специальный балансовый счет для спорных сумм. Там она будет числиться, пока по ней не будет принято окончательное решение.

[164] См.: Указание ЦБР от 25.12.97 г. № 101-у.

При этом эквайрер должен как можно быстрее разрешить возникшую ситуацию, так как спорная сумма числится на его балансе и он несет существенные расходы по ее финансированию (обслуживанию). Как правило, на практике, банки-эквайреры списывают спорную сумму со своего резервного счета, оформляя ее как потерю по ссудам. Убыток несет эквайрер, тогда как другие участники карточных расчетов остаются в прибыли[165]. Этот же счет используется и для списания расходных денежных сумм, возникших в результате незаконного использования платежно-расчетных карт.

Отказываясь от реально произведенных с использованием карты возмездных операций, преступники причиняют имущественный ущерб эквайрерам или эмитентам.

С л е д ы п р е с т у п л е н и я : наличие у мошенника товара, приобретенного по криминальной операции, либо первичных расчетно-кассовых документов, подтверждающих факт ее совершения; собственноручная подпись в слипе или ином первичном бухгалтерском документе; данные электронного журнала фиксации событий в биометрических системах санкционирования доступа (идентификации держателя); фото- или видеодокументы, содержащиеся в соответствующих автоматизированных охранных системах; показания свидетелей-очевидцев проведения криминальной операции держателем карты; электронные реквизиты о проведенной криминальной операции, содержащиеся в памяти микропроцессорных карт.

3.2. Инсценировка держателем хищения либо утраты карты.

Суть способа состоит в том, что держатели официально заявляют эмитенту о хищении у них или об утрате карты, одновременно продолжая пользоваться ею. Расчет преступников строится на определенном времени, которое должно пройти до момента блокирования номера карты в авторизационном (процессинговом) центре платежной системы и получении всеми ее участниками специального документа – «Стоп-листа». **Стоп-лист** – это документ, направляемый процессинговым центром платежной системы всем своим членам и содержащий список номеров платежно-расчетных карт, признанных недействительными: утерянных, похищенных, поддельных, выведенных из оборота. Он запрещает осуществлять какие-либо операции с использованием этих реквизитов, а имеющие их карты предписывает изымать из обращения. Механизм изъятия карты зависит от вида управления терминальным устройством. Если это автомат (банкомат, автоматизированный турникет

[165] Подробнее см.: *Специвцева А.В.* Новые пластиковые деньги. – М., 1994.

КПП или другой), то вставленная в его ридер карта механически блокируется и сбрасывается в специальный охраняемый инкассируемый контейнер. У некоторых видов терминальных устройств при наступлении данного события автоматически включается охранная система в целях задержания лица, пытавшегося воспользоваться недействительной картой. Если терминалом управляет человек – оператор, то карта изымается им с одновременным принятием мер к задержанию лица, предъявившего ее для совершения операции. Эти действия регламентированы соответствующими инструкциями.

Вместе с тем у преступника есть достаточно времени, чтобы совершить хищение денежных средств, товаров и избавиться от карты.

Документы, в которых могут быть следы этого способа: пластиковая карта; «Стоп-лист»; Акт об изъятии карты; заявление держателя о хищении у него карты или ее утрате; документы, удостоверяющие личность лица, воспользовавшегося картой; первичные документы, составленные по операции, в ходе которой карта была обнаружена; электронный журнал фиксации операции в биометрических системах санкционирования доступа (идентификации держателя); фото- или видеодокументы из автоматизированных охранных систем, зафиксировавшие факт проведения операции с использованием карты.

3.3. Инсценировка хищения либо утраты карты держателем – членом преступной группы. В некоторых случаях держатель, действуя в составе группы лиц по предварительному сговору, передает соучастникам свою пластиковую карту и ПИН-код для осуществления криминальных операций. Это делается им умышленно во избежании опознания, в случае задержания. После того как все возможные денежные суммы снимаются со счета, они делятся между мошенниками. «Пустая» карта либо уничтожается, либо продается субъектам, заинтересованным в ее дальнейшем незаконном использовании другими способами, которые будут исследованы далее по тексту работы.

Указанным способом очень активно пользуются организованные преступные группы (ОПГ) и сообщества для легализации (отмывания) денежных средств, а также в целях сокрытия других преступлений. Способ также активно используется в подпольной банковской системе[166]. При этом следует обратить внимание на тот факт, что при пере-

[166] Подробнее см.: Основы борьбы с организованной преступностью: Монография / Под ред. В.С. Овчинского, В.Е. Эминова, Н.П. Яблокова. – М., 1998. – С. 19; Подпольная банковская система // Борьба с преступностью за рубежом. – 1992. – № 8. – С. 3-9.

сечении субъектами национальных границ пластиковые карты не подлежат регистрации в таможенных декларациях, следовательно, суммы денежных средств, полученные с их помощью на территории иностранного государства, также не подлежат контролю со стороны правоохранительных органов. Таким образом, с использованием платежно-расчетных карт можно практически бесконтрольно перемещать определенные суммы обезличенных денежных средств в любой валюте. Этими особенностями международного оборота пластиковых карт активно пользуются преступники.

4. Хищение денежных средств путем обмана или введения в заблуждение держателя карты при осуществлении платежно-расчетной операции. Этот способ имеет следующие разновидности.

4.1. Двойная операция» по одной карте. Работник предприятия торговли и сферы услуг (мерчанта), осуществляющий в силу своих служебных обязанностей налично-безналичные расчетно-кассовые операции по пластиковым картам, пользуясь невнимательностью обслуживаемого клиента (иногда находящегося в состоянии алкогольного опьянения), либо умышленно отвлекая его разными способами, негласно производит оформление не одной, а нескольких расходных операций по предъявленной к оплате пластиковой карте. Одна из операций – действительная, другие – фиктивные. Расчет делается на то, что клиент забудет сумму реально оплаченной услуги или товара. Помимо этого, в целях сокрытия следов преступления, на руки клиенту выдается только чек (квитанция) о реально произведенной операции, тогда как другой – остается у кассира и впоследствии уничтожается.

Таким образом, в кассе создается излишек денежных средств на общую сумму, равную сумме негласно произведенных расходных операций по одной карте, который ликвидируется путем изъятия и присвоения наличных денег, товара, а также получения услуги, например ужин в своем баре (ресторане).

4.2. Изготовление поддельного слипа с использованием эмбоссированных реквизитов подлинной действующей платежно-расчетной карты. Данный способ хищения денежных средств является разновидностью предыдущего. Однако он применяется только тогда, когда касса оборудована не ридером, подключенным к ККМ, а импринтером – автономным механическим устройством, предназначенным для переноса оттиска с рельефных (эмбоссированных) реквизитов карты на бумажный платежный документ – слип. В данном случае эти реквизиты используются как печатающие элементы (клише держателя карты), а сам ридер – как печат-

ный станок. Печать осуществляется кассиром вручную путем прокатки специальным печатающим устройством (кареткой с клише мерчанта) по лицевой стороне бланка слипа, под которым находится лицевая сторона карты с эмбоссированными реквизитами. Печатающий механизм (каретка) движется в горизонтальной плоскости по направляющим в поступательно-возвратном направлении (вперед и назад). Под ним находится лоток со специальным элементом для жесткой фиксации подложки карты, на которую укладываются три скрепленных одним корешком бланка слипа. Оттиск на бланке получается за счет давления резинового валика каретки на эмбоссированные знаки через монохромный копировальный красочный слой, нанесенный на оборотные стороны бланков слипов, либо за счет химической реакции бесцветных веществ, одним из которых обработаны лицевые стороны бланков, а другим – оборотные. В первом случае красящее вещество механически переносится на запечатываемую поверхность, во втором – переносится и вступает в химическую реакцию, в результате которой образуется цветной краситель.

После того как карта и бланки слипа указанным порядком уложены в импринтер, кассир с небольшим нажимом движением «вперед» прокатывает по ним кареткой. В результате чего в верхнем левом углу бланка отпечатываются рельефные реквизиты карты. Далее, одним движением «назад», каретка возвращается в исходное положение, отпечатывая с клише идентификационные реквизиты (идентификатор) мерчанта и терминального устройства. Затем бланк слипа извлекается из импринтера и дооформляется собственноручно кассиром и держателем карты с использованием пишущей ручки. С ее помощью в пустые графы – поля бланка заносятся недостающие реквизиты. При этом красящим веществом ручки заполняется первый экземпляр, а на втором и третьем – получаются отпечатки. После подписания слипа лицом, предъявившим карту к оплате, и кассиром его экземпляры отрываются от корешка и направляются по назначению: первый – вручается клиенту, второй – остается на хранении у кассира, а третий – включается в сводный отчет по кассе и инкассируется банком-эквайрером. Впоследствии по нему делаются соответствующие проводки по общей схеме взаиморасчетов, рассмотренные нами ранее.

Из формы и содержания реквизитов слипа видно, что этот *документ является* не чем иным, как **чеком** – письменным распоряжением владельца банковского счета (чекодателя) своему платель-

щику (банку-эмитенту) уплатить сумму денег, указанную в чеке, получателю средств (чекодержателю)[167]. Из этого следует, что *бланки слипа являются бланками строгой отчетности.* Они учитываются в банках-эквайрерах на внебалансовом счете № 91207 «Бланки строгой отчетности» и в подотчет выдаются материально ответственным лицам – кассирам мерчантов.

Пользуясь невнимательностью клиента, мошенники отпечатывают на импринтере сразу два слипа, один из которых заполняется на глазах у держателя карты (подлинный), а другой – скрытно прячется и оформляется в его отсутствии (поддельный). В последнем случае имеет место интеллектуальный подлог с подделкой подписи ничего не подозревающего клиента. Подпись подделывается различными, хорошо известными способами, а именно:

- графическим подражанием оригиналу путем тренировок;
- воспроизведением через обычную копировальную либо специальную химически обработанную бумагу, идентичную по своим свойствам бланку слипа;
- перерисовыванием на просвет;
- передавливанием с оригинала – подлинная подпись обводится с сильным нажимом каким-либо заостренным предметом, а затем полученное контурное изображение подписи в виде вдавленных штрихов обводится пастой шариковой ручки или чернилами.

Первый способ может быть обнаружен методом сравнения признаков почерка в выполнении отдельных букв и штрихов, а также обнаружением неоправданных остановок при написании букв, извилистости штрихов, характеризующих осторожные движения преступника.

Остальные три способа подделки сходны между собой тем, что подделыватель повторяет движения, которыми выполнен оригинал подписи. Такая подделка выявляется по штрихам копировальной бумаги, следам предварительной карандашной подготовки, вдавленным штрихам, признакам подрисовки в виде извилистости штрихов, тупым их окончаниям, неоправданным остановкам пишущего прибора[168].

5. Хищение карты и ПИН-кода с последующим их преступным использованием. Согласно данным зарубежной статистики хищения денег и товаров с использованием украденных пластиковых карт составляют более 70 % общего числа случаев их незакон-

---

[167] Данное утверждение следует из анализа положений ст. 878, 879 и 882 ГК РФ.

[168] См.: *Зинин А.М.* Проверка документов, удостоверяющих личность: Учеб.-практ. пособие. – М., 2002. – С. 28.

ного использования. При этом у преступника всегда в запасе есть минимум трое суток с момента обращения держателя с заявлением об утрате (хищении либо потере) карты, чтобы незаконно воспользоваться картой. Это именно тот минимальный срок, который необходим для блокирования в платежной системе расчетов, производимых по ее номеру[169]. В целом, способы хищения пластиковой карты как предмета, обладающего определенной стоимостью, ничем не отличаются от способов хищения обычных вещей. Они достаточно полно изучены отечественной криминалистической наукой[170]. Вместе с этим существуют следующие особенности, которые присущи преступлениям рассматриваемой категории.

5.1. Хищение карты и ПИН-кода в момент совершения держателем платежно-расчетной операции у банкомата. Данная группа способов основана на специфике оборота карт для банкоматов и имеет корреляционную зависимость с местом установки последних: преступление совершается исключительно на улице в месте установки банкомата. Здесь потерпевший временно выпускает карту из рук, устанавливая ее в считывающее устройство банкомата, и раскрывает секретный ПИН-код третьим лицам, когда набирает его на клавиатуре. Для тех, кто сам когда-либо пользовался картой в банкомате, известно, что часто у них скапливается очередь держателей. Поэтому преступнику, стоящему за жертвой и подглядывающему из-за ее плеча, не составляет большого труда запомнить 4 цифры кода. Дело остается лишь за тем, чтобы изъять карту у ее держателя. Международной юридической практике известны два способа достижения этой цели.

«Ротозейство» («рывок с отвлечением»). Этот способ имеет сходство с сезонными грабежами: меховых шапок – в осенне-зимний и золотых украшений (цепочек и сережек) – в весенне-летний периоды времени. Метод достаточно банален: преступник внезапно срывает их с потерпевшего и быстро убегает с места преступления («совершает рывок»).

---

[169] См.: *Гамза В.А., Ткачук И.Б.* Безопасность коммерческого банка: Учеб.-практ. пособие. – М., 2000. – С. 57.

[170] См., например: *Савельев В.А.* Значение способов сокрытия краж личного имущества граждан в раскрытии, расследовании и предотвращении этих преступлений: Автореф. дис. … канд. юрид. наук. – М., 1990; *Шурухнов Н.Г.* Расследование краж: Практ. пособие. – М., 1999; Организация раскрытия и расследования краж из жилых помещений / Отв. ред. П.М. Туленков. – Волгоград, 1991; *Корнелюк В.С., Резван А.П., Субботина М.В.* Расследование хищений чужого имущества. – Волгоград, 2001.

В случае с пластиковой картой дело обстоит несколько иначе: преступник подсматривает ПИН-код; в момент одновременной выдачи из банкомата карты и наличных купюр, когда руки потерпевшего заняты деньгами, отвлекает его взгляд в сторону от себя и лицевой стороны банкомата, например оброненной мелкой купюрой; выхватывает карту и быстро скрывается. После этого наличные деньги спешно снимаются из других банкоматов до тех пор, пока они есть на счете потерпевшего и не исчерпан кредитный лимит либо пока карта автоматически не изымается банкоматом.

Если преступники действуют в составе группы, то наблюдается четкое разделение криминальных ролей: один – подсматривает ПИН-код и похищает карту; другие – отвлекают потерпевшего и следят за обстановкой вокруг места преступления. После его совершения все разбегаются в разные стороны.

«Ливанская петля». Название способа произошло от названия государства, где он был придуман и впервые реализован в криминальной практике, – это Ливан. Мошенник негласно наклеивает на прорезь банкомата, в которую для осуществления операции штатно вставляется банковская карта, отрезок 35-мм фотопленки. Она имеет тонкую продольную прорезь, совпадающую с приемным технологическим отверстием, и закомуфлирована под наружный элемент корпуса этого терминального устройства. Прорезь выполнена таким образом, чтобы вошедшая в банкомат карта не была возвращена обратно после выполнения расчетной операции: имитируется сбой в работе устройства и блокирование в нем карты. После выполнения указанных подготовительных мероприятий преступник располагается рядом с банкоматом и ожидает свою жертву. Когда карта добросовестного пользователя заблокировалась фотопленкой, мошенник предлагает свою помощь. Он сообщает, что с его картой такое бывало не раз, и предлагает держателю еще раз ввести ПИН-код. Если держатель отказывается, мошенник убеждает его, что данное действие может помочь вернуть карту. После того, как данное действие не привело к желаемому результату, мошенник искренне сожалеет о случившемся, рекомендует обратиться в ближайшее отделение банка за помощью и делает вид, что уходит. Когда держатель ни с чем покидает место происшествия, преступник срывает фотопленку, достает карту и быстро уходит. Имея на руках карту и зная ПИН-код, он совершает хищение денежных средств[171].

---

[171] См.: Способы мошенничества // Программа обучения сотрудников полиции борьбе с мошенничеством с использованием платежных пластиковых карточек / Авт.

Следы преступлений, совершенных вышерассмотренными способами: *идеальные* – в памяти держателя похищенной карты и свидетелей (прохожих); *материальные* – следы крепления фотопленки к считывателю банкомата; одорологические; документальные.

Документальные следы:

1) *Квитанция банкомата*, которая имеет следующие обязательные реквизиты: дата и время совершения операции; номер-идентификатор банкомата; порядковый учетный номер операции и квитанции в электронном журнале и контрольной ленте; номер карты; название операции; сумма операции; валюта операции; код, подтверждающий авторизацию операции; иные данные, допустимые правилами безопасности[172].

2) Выведенная при инкассации распечатка – *контрольная лента*[173].

3) Выписка-распечатка *из электронного журнала* банкомата (*расходного электронного реестра*) – соответствующих электронных документов, составленных по операциям, произведенным держателем в момент утраты карты[174].

4) Указанные в пп. 1-3 документы, но по операциям, совершенным преступником с использованием искомой карты в других местах.

5.2. Хищение, совершенное с использованием потерянных карт через банкоматы и электронные терминалы, не оборудованные системами биометрической идентификации держателя. По данным зарубежной статистики, этим способом совершается более 20 % преступлений исследуемой категории[175]. Содержание данного способа наглядно можно раскрыть с помощью следующего примера.

Как следует из материалов уголовного дела, обвиняемый А. использовал для хищения паспорт, банковскую карту и лист бумаги с

и сост.: Международная платежная система Visa International Association CEMEA, при поддержке Ассоциации «ВИЗА» в России. – 2001.

[172] См.: П. 5.4 ст. 5 Положения о порядке эмиссии кредитными организациями банковских карт и осуществления расчетов по операциям, совершаемым с их использованием // Письмо Центрального банка России от 09.04.98 г. № 23-П.

[173] Подробнее см.: П. 2.6.6 Положения о порядке ведения кассовых операций в кредитных организациях на территории Российской Федерации // Письмо Центрального банка России от 09.10.02 г. № 199-П.

[174] В соответствии с п. 2.8.2 указанного Положения: «Банкоматы, электронные кассиры и автоматические сейфы должны обеспечивать возможность вывода на бумажный носитель информации о проведенных операциях».

[175] См.: *Гамза В.А., Ткачук И.Б.* Безопасность коммерческого банка: Учеб.-практ. пособие. – М., 2000. – С. 57.

ПИН-кодом. Данные вещи находились в сумочке, которая была забыта потерпевшей в салоне автомашины А., когда тот подвозил ее. Утром следующего дня мошенник подъехал к банкомату «Мост-Банка», вставил карту, набрал ПИН-код и снял 50 тыс. рублей (в ценах 1998 г.). Через 20 минут он вернулся к тому же банкомату и аналогичным образом получил вначале 250 тыс. рублей, а затем 500 долларов США. Вскоре А. опять приехал к банкомату и заказал 1 тыс. долларов – банкомат ее выдал, затем еще столько же – банкомат отказал в выдаче указанной суммы денег. Тогда преступник заказал 500 долларов и получил их. Основными доказательствами виновности А. стали: видеозаписи автоматизированной охранной системы банкомата, зафиксировавшие каждую операцию снятия денег; кассовые ленты по всем криминальным операциям; изъятые при обыске у А. чужие именные документы – паспорт и пластиковая карта, а также лист бумаги с ПИН-кодом потерпевшей; протоколы допроса потерпевшей, обвиняемого и предъявления для опознания.

При совершении имущественного преступления рассмотренным способом, но с использованием иной платежно-расчетной карты или карты другого вида (именного удостоверения, пропуска, электронного ключа) алгоритм преступления будет аналогичен вышеуказанному. В этом случае типичными вещественными доказательствами будут: чужая пластиковая карта с отпечатками пальцев рук подозреваемого; распечатка реквизитов криминальных операций из электронного журнала, содержащегося в памяти терминала или базе данных управляющей ЭВМ; фото- или видеодокументы автоматизированных охранных систем, зафиксировавшие совершение операций подозреваемым; носитель с ПИН-кодом; паспорт (удостоверение личности) подозреваемого; похищенное имущество; список лиц, пользующихся правом санкционированного доступа на охраняемый объект (в хранилище) либо на получение имущественных льгот; список лиц, которым выданы номерные пластиковые карты; предметы, сохранившие биологические и иные следы, свидетельствующие о пребывании преступника на охраняемом объекте (в хранилище); заявление потерпевшего о хищении или утрате карты (номерного документа).

Получение исследуемых орудий преступного посягательства может также происходить путем их хищения на этапе рассылки по почте держателю, а также иными способами, которые будут рассмотрены нами далее. Например, отечественной юридической практике известен случай разоблачения организованной преступной группы грузчиков в международном аэропорту «Шереметьево-2» (г. Москва),

специализировавшейся на кражах почтовых отправлений с банковскими картами и ПИН-кодами, которые впоследствии использовались ее членами для хищения денежных средств.

5.3. Хищение и незаконное использование ПИН-кодов и пластиковых карт, удостоверяющих имущественные права либо документы на получение имущества, – средств удостоверения электронных документов. Эти пластиковые карты представляют собой программно-аппаратный аналог собственноручной подписи потерпевшего – электронное факсимиле в виде электронной цифровой подписи. В последнее время они находят все большее применение в деловом электронном документообороте, например для заверения электронных платежно-расчетных документов в ходе торгов на валютных биржах, при транзакциях в международной финансовой системе СВИФТ, а также при оформлении таможенных документов.

Документы, в которых могут быть следы этого способа: пластиковая карта; комплект документов, необходимых для получения и использования ЭЦП (заявление на получение ЭЦП, договор на обслуживание ЭЦП между ее владельцем и удостоверяющим центром, сертификат на пластиковую карту – средство ЭЦП, сертификат ключа ЭЦП); выписка из учетного реестра удостоверяющего центра по конкретной карте – подписи; паспорт подозреваемого; документы, удостоверяющие право использования подписи вторым лицом (лицами); договоры (контракты) и иные документы о сделках имущественного характера, удостоверенные конкретной ЭЦП; ценные бумаги как предмет хищения с использованием ЭЦП, выписки из реестров их эмитентов; комплект разрешительных документов на осуществление деятельности на рынке ценных бумаг, в электронной системе лотовых торгов.

6. Нарушение правил оформления расчетных операций с использованием платежно-расчетных карт работниками мерчанта, эквайрера или эмитента.

6.1. «Маскарад»[176] – один из самых первых и распространенных способов совершения хищений выделенной категории в нашей стране. Он заключается в том, что преступник, завладев чужой пластиковой картой различными способами (путем хищения, скупки краденой карты, «воровской мены», приискания и другими), начинает выдавать себя за законного держателя. Для этого он изготав-

[176] **Маскарад** – поведение, имеющее своей целью скрыть внутреннюю сущность чего-либо; притворство. – См.: Словарь русского языка: В 4-х т. Т. 2 / АН СССР, Ин-т рус. яз.; Под ред. А.П. Евгеньевой. – 3-е изд., стер. – М., 1985–1988. – С. 232.

ливает или подделывает похищенные удостоверительные документы на свое имя, которые предъявляет вместе с картой. Мошенник также тренируется в подделке подписи, образец которой имеется у него (на оборотной стороне карты или в иных похищенных документах), поскольку преступление рассматриваемым способом можно совершить только при оформлении расчетно-кассовой операции с использованием импринтера. На этом подготовительный этап заканчивается и начинается этап непосредственного изъятия чужого имущества – приобретения мошенническим путем того или иного товара или получение наличных денег.

По существующим правилам оформления операций по карте[177] кассир должен сверить подпись на планке карты с образцом подписи в паспорте, а после заполнения слипа – поставленную в нем подпись с ее образцом на карте.

Анализ следственной практики показывает, что, совершая хищение исследуемым способом, преступники, как правило, рассчитывают на несвоевременное направление мерчанту «Стоп-листов», а также халатное или непрофессиональное исполнение операторами терминальных устройств (кассирами) своих должностных обязанностей. Так, в подавляющем большинстве случаев, они не сверяют подпись в паспорте с подписью на планке предъявляемой к оплате карты. Именно эти обстоятельства являются основными причинами и условиями, способствующими совершению мошенничества таким способом. Данное утверждение можно проиллюстрировать следующим примером.

Как следует из материалов уголовного дела, гражданин Российской Федерации К. с целью использования не принадлежащих ему кредитных карт зарубежных банков в ноябре – декабре 1990 г. приобрел в Москве у не установленного следствием лица именные кредитные карты «Visa» и «MasterCard», утраченные гражданином США С., а также водительское удостоверение на его имя, выданное властями штата Калифорния. По заявлению держателя в процессинговом центре российского эмитента «Интуркредиткарт» были блокированы соответствующие счета, а в адрес мерчантов – направлены «Стоп-листы» с номером утраченной карты. Вклеив в водительское удостоверение гражданина С. свою фотографию и научившись подделывать его подпись, имевшуюся на указанных документах, К. стал предъявлять их к оплате в кассах магазинов за

[177] Подробнее см.: П. 2 Инструкции по обслуживанию держателей банковских карт в предприятиях торговли и сервиса // Приложение № 1 к Типовому договору об использовании банковских карт в качестве платежного средства.

приобретаемые товары. Так, 11 декабря 1990 г., находясь в секции № 22 магазина «Калина» в г. Краснодаре, с целью хищения имущества, К. при оплате отобранных товаров предъявил кассиру Г. кредитные карты, а для подтверждения личности – поддельное водительское удостоверение на имя гражданина США С. При этом в слипах он расписался, копируя подпись С. Кассир подделки документов не заметила и, не сверяя реквизиты кредитных карт со «Стоп-листами», отпустила мошеннику товары на общую сумму 1 667 долларов США, что по действующему на момент совершения преступления курсу составило 8 337 рублей.

В общей сложности К. в течение трех месяцев в различных городах России (Москве, Санкт-Петербурге, Владивостоке и других) аналогичным способом совершил еще 29 хищений, причинив ущерб в размере 102 тыс. рублей. Лишь 17 марта 1991 г. при покупке товаров в магазине № 9 «Балтика» г. Санкт-Петербурга кассир-контролер сверила предъявленные к оплате номера кредитных карт со «Стоп-листами», в результате чего К. был задержан.

Следы способа обнаруживаются при исследовании следующих документов: пластиковой карты; поддельных документов, удостоверяющих личность; паспорта подозреваемого; слипов, оформленных по операциям с использованием чужой карты; кассовых отчетов; «Стоп-листов»; заявления держателя об утрате карты; бумажных носителей с тренировочными подписями; выписки по СКС (биллинга); выписки из файл-мастера клиентской базы данных процессингового центра эмитента либо платежной системы о держателе, которому принадлежит карта, использованная преступником.

6.2. Оформление первичных расчетно-кассовых документов по заведомо недействительным платежно-расчетным картам. Совершение хищения таким способом возможно лишь в тех случаях, когда в состав организованной преступной группы, специализирующейся на рассматриваемом виде имущественных посягательств, входят кассиры мерчантов. Они сознательно идут на нарушение соответствующих должностных инструкций и правил, в том числе установленного Порядка ведения кассовых операций в Российской Федерации[178]. Заведомо зная о незаконности использования пластиковой карты, данные лица принимают ее к оплате и оформляют все необходимые расчетно-кассовые документы. При

[178] Подробнее см.: Порядок ведения кассовых операций в Российской Федерации // Письмо Центрального банка Российской Федерации от 04.10.93 г. № 18 (в ред. Письма ЦБР от 26.02.96 г. № 247).

этом подпись держателя, если она необходима, подделывается сообщником, предъявившим карту к оплате, либо самим кассиром.

С помощью рассматриваемого способа мошенникам беспрепятственно удается присваивать денежные средства, поступающие в кассу от операций по картам, покрывать недостачу, незаконно приобретать товары и оплачивать услуги за счет потерпевшего. При этом имущество или наличная валюта изымается в размере незаконно оформленной операции или их совокупности. При внесении в кассу наличных денежных средств по другим законным операциям требуемая сумма изымается кассиром и покрывается документом безналичной формы оплаты по карте – слипом, который включается в отчет по кассе и инкассируется (внедряется в систему межбанковских взаиморасчетов).

В случае получения «Стоп-листа» с номером незаконно используемой карты, кассир информирует об этом своих сообщников.

Документы, в которых необходимо искать следы способа (по конкретным операциям): пластиковые карты; «Стоп-листы»; заявления об утрате карт; кассовые чеки (квитанции); слипы; кассовые ленты; отчеты по кассе за интересующий период времени; кассовая книга; электронный журнал терминала (электронный расходный реестр); выписки по конкретным СКС (биллинг); выписки из файл-мастеров клиентской базы данных процессингового центра эмитента либо платежной системы о держателях, которым принадлежат карты, использованные преступниками.

6.3. Оформление первичных расчетно-кассовых документов по чужим платежно-расчетным картам, временно вышедшим из-под присмотра их держателей, является разновидностью предыдущего способа.

Как следует из материалов одного уголовного дела, в 1993 г. сотрудниками УБЭП ГУВД г. Москвы была пресечена деятельность организованной преступной группы, в состав которой входили проститутки, обслуживающие иностранных граждан, курьеры и кассиры мерчантов. Механизм совершения преступления был достаточно простым и банальным. Проститутки во время «своей работы» похищали пластиковые карты у своих «клиентов» и передавали их своим сообщникам – курьерам. Те, в свою очередь, в зависимости от вида платежно-расчетной карты и наличия ПИН-кода, оперативно снимали наличные деньги в банкоматах либо доставляли их кассирам мерчантов, которые производили по ним расчетно-кассовые операции. После этого карты также быстро и негласно возвращались их держателям. Таким образом, факт мошенничест-

ва обнаруживался потерпевшим только после получения ежемесячной выписки по счету – биллинга.

Основными доказательствами являются: заявление потерпевшего; выписка по СКС (биллинг); материалы внутреннего расследования службы безопасности эмитента; пластиковая карта; справка из процессингового центра платежной системы, содержащая детальную информацию об операциях, совершенных держателем карты за интересующий период времени; кассовые чеки (квитанции); слипы; кассовые ленты; отчеты по кассе за интересующий период времени; кассовая книга; электронный журнал терминала (электронный расходный реестр); фото- или видеодокументы автоматизированных охранных систем, зафиксировавшие факт совершения криминальных операций.

6.4. Негласное изменение условий Договора об обслуживании специального карточного счета. Данный способ может быть использован только сотрудником организации-эмитента, который связан с обслуживанием СКС держателей карт. Он состоит в том, что мошенник входит в преступный сговор с держателем карты с целью хищения денежных средств, принадлежащих эмитенту. Имея доступ к компьютерной системе учета клиентов либо операционной работы по СКС, преступник тайно вносит в соответствующие электронные документы несанкционированные изменения, влияющие на конечные результаты вычислений расчетов по СКС. Например, неправомерно увеличивает размер кредитного лимита по конкретному счету (карте), лимита выдачи наличной валюты по одной операции или дневного лимита; устанавливает в авторизационной системе специальный статус счета, позволяющий в определенных пределах сверхустановленного для конкретной категории карт лимита осуществлять расходные операции; незаконно пополняет денежные средства, расходуемые соучастником со своего СКС[179]. Полученные за счет этих криминальных операций денежные средства преступники делят между собой.

Следы этого способа могут быть обнаружены при исследовании следующих документов: материалов контрольных документальных проверок и ревизий; справки из процессингового центра платежной системы, содержащей детальную информацию об операциях, совершенных держателем карты, и комиссиях, взимаемых с эмитента или причитающихся ему, а также удерживаемых эмитентом с клиента (эти сведения

[179] См.: *Гамза В.А., Ткачук И.Б.* Указ. соч. – С. 60.

содержатся в файлах «incoming file», «detailed position» и «account position»); договора об обслуживании СКС; выписки из СКС (биллинга); выписок из счетов учета лимитных (сверхлимитных) операций по картам; файл-мастера из клиентской базы данных процессингового центра платежной системы; пластиковой карты.

3.2. Использование конфиденциальной информации о реквизитах подлинных карт и их держателях

Для совершения многих финансовых операций используются не сами карты, а их отдельные *конфиденциальные реквизиты*, вводимые в компьютерное терминальное устройство. Видимо, по этой причине выделенная группа способов подготовки и совершения хищений в понимании является наиболее сложной категорией. В связи с чем отметим следующее.

В соответствии с законодательством Российской Федерации к категории конфиденциальной относится зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать, доступ к которой ограничивается[180]. В рассматриваемом нами случае ее содержание может быть следующих видов.

1) *Сведения, передаваемые путем переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений*[181]. К иным сообщениям относится и обмен информацией между ЭВМ[182]. Соответственно, нарушение тайны этих сообщений влечет за собой уголовную ответственность, предусмотренную ч. 1 ст. 138 УК РФ. Данное преступное деяние имеет место в случае незаконного ознакомления с перепиской, почтовыми и телеграфными сообщениями, прослушивания чужих переговоров, а также ознакомления с конфиденциальной компьютерной информацией, циркулирующей в ЭВМ, системе ЭВМ или их сети.

---

[180] См.: Закон Российской Федерации от 20.02.95 г. № 24-ФЗ «Об информации, информатизации и защите информации». – Ст. 2.

[181] Подробнее см.: Ч. 2 ст. 23 Конституции Российской Федерации.

[182] В соответствии со ст. 2 Закона Российской Федерации «О связи» **электрическая связь** (**электросвязь**) – это всякая передача или прием знаков, сигналов, письменного текста, изображений, звуков по проводной, радио-, оптической и другим электромагнитным системам; **сети электросвязи** – это технологические системы, обеспечивающие один или несколько видов передач: телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений, *включая обмен информацией между ЭВМ*, телевизионное, звуковое и иные виды радио- и проводного вещания.

Нарушение тайны переписки, переговоров и иных сообщений имеет место, когда корреспонденция, в том числе поступившая в виде электронной почты или SMS-сообщений по каналам сотовой радиосвязи, становится достоянием третьих лиц без согласия отправителя и адресата.

Если для совершения данного преступления были использованы специальные технические средства (СТС), предназначенные (разработанные, приспособленные, запрограммированные) для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи[183], то такое деяние должно квалифицироваться по ч. 2 ст. 138 УК РФ. Следует обратить внимание на тот факт, что в качестве указанных СТС, как правило, используются разнообразные программно-аппаратные средства электронно-вычислительной техники.

В случае осуществления неправомерного доступа к охраняемой законом компьютерной информации, содержащейся на пластиковых картах, в памяти терминальных устройств и в системе или сети ЭВМ, обеспечивающих их оборот, а также физических полях, возникающих при работе этого оборудования, содеянное должно квалифицироваться по ст. 272 УК РФ. При этом обязательно необходимо доказать, что деяние повлекло следующие негативные последствия: уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Под доступом к компьютерной информации понимается всякая форма проникновения к ней с использованием средств (вещественных и интеллектуальных) электронно-вычислительной техники, позволяющая манипулировать информацией (уничтожать ее, блокировать, модифицировать, копировать)[184].

Приготовлением к совершению хищения рассматриваемой категории являются несанкционированные: проникновение к пультам

---

[183] Перечень видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации // Постановление Правительства Российской Федерации от 01.07.96 г. № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-разыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации».

[184] См.: Комментарий к Уголовному кодексу Российской Федерации. – 2-е изд., изм. и доп. / Под общ. ред. Ю.И. Скуратова, В.М. Лебедева. – М., 1998. – С. 635.

управления ЭВМ и другими терминальными устройствами (ККМ, банкоматом, бимчекером, сотовым радиотелефоном и суперсмарт-картой), в программу для ЭВМ, базу данных, систему или сеть ЭВМ, обслуживающих операции по пластиковым картам; получение ПИН-кода и других конфиденциальных реквизитов карты; приискание вредоносных программ для ЭВМ и других СТС для негласного получения информации; нейтрализация средств защиты информации, подробно рассмотренных нами ранее.

Доступ к компьютерной информации считается неправомерным, если:

- лицо не имеет права на доступ к данной информации;
- лицо имеет право на доступ к данной информации, однако осуществляет его, помимо установленного порядка, с нарушением правил ее защиты.

Пользователи[185], имеющие допуск к одной информационной системе или к ЭВМ коллективного пользования, обыкновенно ранжируются в зависимости от тех операций, которые им дозволено совершать, – от элементарного просмотра информации на экране электронного терминала до права вносить изменения в используемые системой базы данных и даже в программу, по которой действует система; некоторые файлы доступны лишь для определенной группы пользователей, обладающих индивидуальными открытыми и закрытыми ключами (соответственно картами и ПИН-кодами к ним). Несанкционированное повышение пользователем собственного ранга (например, при использовании реквизитов чужой карты и ПИН-кода) должно рассматриваться как неправомерный доступ к компьютерной информации или приготовление к нему[186]. При этом «нарушение требований защиты информации расценивается как несанкционированный доступ к информации»[187].

2) *Сведения, отнесенные к коммерческой тайне.* К ним относятся только те данные, в отношении которых удовлетворены одновременно три условия, а именно:

- когда они имеют действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;

---

[185] **Пользователь** (потребитель) информации – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею. – См.: Закон Российской Федерации от 20.02.95 г. № 24-ФЗ «Об информации, информатизации и защите информации». – Ст. 2.

[186] См.: Комментарий к Уголовному кодексу Российской Федерации. – С. 635-636.

[187] Концепция правовой информатизации России // Указ Президента Российской Федерации от 28.06.93 г. № 966 «О Концепции правовой информатизации России». – П. 3 разд. IV.

• когда к ним нет свободного доступа на законном основании;

• когда обладатель информации принимает меры к охране их конфиденциальности[188].

В силу ст. 6 Федерального закона «Об информации, информатизации и защиты информации» информационные ресурсы (программы для ЭВМ, базы данных, электронные документы и их массивы, а также пароли доступа к ним и иным информационным продуктам) находятся в собственности физических и юридических лиц и включаются в состав их имущества со всеми вытекающими из этой диспозиции гражданско-правовыми последствиями[189]. Например, из этого следует, что ***компьютерная информация, содержащаяся в памяти SIM-карты, а также иных не банковских пластиковых карт, относится к разряду коммерческой тайны их эмитентов***.

3) *Сведения, являющиеся банковской тайной.* Режим конфиденциальности в отношении их устанавливается ст. 857 ГК РФ «Банковская тайна» и ст. 26 Закона Российской Федерации от 03.02.96 г. № 17 «О банках и банковской деятельности». Это сведения о реквизитах банковского счета и банковского вклада, процедуре доступа к ним, операциях по счету, персональных данных о клиенте и юридическом адресе корреспондентов, а также иные сведения, если это не противоречит настоящему Федеральному закону. Таким образом, *к банковской тайне относятся сведения, содержащиеся* в реквизитах банковской карты; бумажных первичных учетных документах, составленных с их использованием; электронных документах, находящихся в памяти терминальных устройств, на машинных носителях информации, в компьютерной системе или сети ЭВМ (в соответствующих программах для ЭВМ и базах данных) либо передающихся по каналам электросвязи посредством электромагнитных сигналов; ПИН-коде; физических полях, возникающих при работе СВТ, обрабатывающих документы с банковской тайной.

Собирание сведений, составляющих коммерческую или банковскую тайну, путем *похищения* соответствующих *документов*, подкупа, угроз, *а равно иным незаконным способом* в целях их разглашения либо незаконного использования является преступлением (ч. 1 ст. 183 УК РФ). В соответствии с ч. 2 ст. 183 УК РФ преступлением также считаются незаконные разглашение или использование таких сведений без согласия их владельца, совершенные из коры-

---

[188] Подробнее см.: Ч. 1 ст. 139 ГК РФ.

[189] См., например: Ст. 209 и 304, а также гл. 20 ГК РФ.

стной или иной личной заинтересованности и причинившие потерпевшему крупный ущерб.

4) *Сведения, имеющие статус персональных данных*: информация о физических лицах – держателях пластиковых карт – сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность[190]. По поводу данного правового определения следует заметить, что большинство именных пластиковых карт содержат сведения указанной категории (фамилия и имя держателя, его фотография, образец подписи, отпечаток пальца руки, группа крови, отношение к той или иной социальной группе, профессия, должностное положение или род занятий и другие). Эти же сведения содержатся в автоматизированных информационных системах в виде файлов персональных данных (как правило, в клиентских базах данных) – файл-мастеров, которые формируются всеми эмитентами для учета своих клиентов держателей при выдаче им именных карт.

Сведения, имеющие статус персональных данных, определяются назначением именной карты и содержанием ее реквизитов. Так, в соответствии со ст. 6 Закона Российской Федерации от 01.04.96 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования», конфиденциальными являются сведения, содержащиеся в индивидуальном лицевом счете застрахованного лица, а следовательно, и те из них, которые реализованы в виде реквизитов пластиковой карты пенсионного страхования[191]. В то же время, в соответствии со ст. 61 Закона Российской Федерации от 22.07.93 г. № 5487-1 «Основы законодательства Российской Федерации об охране здоровья граждан» (в ред. ФЗ от 20.12. 99 г. № 214-ФЗ) сведения о здоровье конкретных граждан относятся к личной (семейной) тайне и подлежат обязательной защите. Соответственно, если они реализованы в виде медицинской пластиковой карты, то реквизиты последней также являются конфиденциальными. Среди этих карт в настоящее время распространены такие, как: «Полис обязательного медицинского страхования», «Паспорт донора», «Паспорт здоровья», «Больничная

[190] См.: Ст. 11 Закона Российской Федерации от 20.02.95 г. № 24-ФЗ «Об информации, информатизации и защите информации».

[191] Вид и содержание конфиденциальных реквизитов данной карты см.: Пластиковые карты. – 4-е изд., перераб. и доп. – М., 2002. – С. 509-511.

карта», «Карта хронического больного», «Карта результатов лабораторных анализов и диагностических исследований»[192].

С учетом вышеизложенного, возможно выделить следующие способы подготовки и совершения преступлений, основанные на использовании конфиденциальной информации о реквизитах подлинных карт и их держателях.

1. Использование полностью поддельного слипа. Данный способ заключается в том, что мошенниками, входящими в состав организованной преступной группы, изготавливаются поддельные слипы, которые с помощью сообщников – сотрудников мерчанта, эквайрера или эмитента внедряются на определенном этапе в финансовый документооборот. Это дает возможность похищать наличные деньги, товары и иное имущество.

По механизму подделки реквизитов слипа выделяются следующие разновидности рассматриваемого способа.

1.1. Заполнение похищенного либо изъятого с места работы бланка слипа с использованием СВТ и пишущей ручки. Для его реализации преступникам необходимо осуществить несколько тренировок: во-первых, чтобы печатные реквизиты слипа, изготовленные на принтере, точно вошли в соответствующие графы – поля бланка документа; во-вторых, чтобы знаки печати и выполненная от руки подпись держателя карты визуально были схожи с их оригиналами. В этих целях с бланка слипа делаются ксерокопии, которые используются в качестве запечатываемого макета. При этом подделываются следующие реквизиты слипа: реквизиты плательщика – номер карты, срок ее действия, фамилия и имя держателя; реквизиты получателя – название, юридический адрес и идентификационный номер (идентификатор) мерчанта; подпись держателя карты, реквизиты которой были использованы для подделки слипа.

Типичные орудия и следы совершения преступления:

1) слип с признаками печати знаков на принтере соответствующего вида (были подробно рассмотрены нами в третьей главе работы), а также фальсификации подписи держателя;

2) принтер с картриджем;

3) ПЭВМ с программой текстового редактора, содержащая в своей памяти файлы с подделываемыми реквизитами;

4) листы с тренировочными распечатками слипов и подписями;

---

[192] Вид и содержание конфиденциальных реквизитов отечественных и зарубежных карт данной категории подробнее см.: Пластиковые карты. – 4-е изд., перераб. и доп. – С. 445-456.

5) журнал учета выдачи бланков строгой отчетности – слипов (в бухгалтерии мерчанта или эквайрера).

1.2. Заполнение добытого незаконным путем бланка слипа с использованием поддельных клише и пишущей ручки. При заполнении стандартного бланка слипа преступниками могут быть использованы поддельные клише – печатные формы, изготовленные по новым компьютерным технологиям[193]. Эти орудия подделки слипа заранее подготавливаются для совершения преступления: изготавливаются в кустарных условиях с использованием соответствующего оборудования и материалов либо на промышленном оборудовании в специализированных предприятиях. В качестве оборудования используются обычная ПЭВМ со стандартным программным обеспечением и специальный принтер для создания полимерных или каучуковых (резиновых) печатных форм.

Подделка подписи держателя карты в слипе осуществляется обычными способами.

Признаки подделки оттисков клише карты и импринтера в слипе:

- гарнитура оттиска знаков в слипе отличается от гарнитуры знаков клише импринтера, принадлежащего конкретному мерчанту;
- гарнитура оттиска знаков в слипе отличается от гарнитуры клише пластиковой карты, с помощью которой оформлен слип;
- несовпадение изображений одноименных цифр и букв;
- расстояние между оттисками цифр и букв в слипе не совпадает с расстоянием между оттисками аналогичных знаков, сделанными соответственно с клише импринтера и пластиковой карты;
- расстояние между строками оттисков в слипе не совпадает с расстоянием между строками оттисков, сделанных соответственно с клише импринтера и пластиковой карты;
- штрихи отдельных знаков в оттиске на слипе выходят за нижнюю или верхнюю горизонтальную границу строки печати;
- цвет красителя в оттиске на слипе не совпадает с цветом оттиска клише конкретного импринтера.

Документы, в которых могут находиться следы способа: слип; квитанция (счет) об оплате заказа на изготовление печатной формы в специализированном предприятии; бланк с контрольным оттиском изготовленного клише; файл с электронным

[193] Подробнее см.: *Буланова Л.И.* Криминалистическое исследование оттисков печатей и штампов, изготовленных по новым технологиям: Автореф. дис. ... канд. юрид. наук. – М., 1998.

образом клише; макет клише; тренировочные оттиски клише и подписи на бумаге или ксерокопии подделываемого слипа; журнал учета выдачи бланков строгой отчетности – слипов (в бухгалтерии мерчанта или эквайрера).

1.3. Полная подделка слипа с использованием СВТ заключается в сканировании всех или части реквизитов слипа в память персонального компьютера, их редактировании с использованием программ для ЭВМ и распечатывании на цветном принтере.

Типичными средствами совершения преступления являются: слип, оформленный по ранее совершенной (законной) операции; ручной или планшетный сканер; персональный компьютер; соответствующее программное обеспечение – графический и текстовой редактор, программа сканирования и распознавания образов изображений; цветной струйный или лазерный принтер; бумага соответствующего вида; нож для резки фотобумаги; измерительный инструмент. Например, в августе 1995 г. в УБЭП ГУВД г. Москвы поступила информация о том, что в столице действует организованная преступная группа, которая специализируется на подделке слипов с использованием реквизитов действительных банковских карт. После проведения соответствующих оперативно-разыскных мероприятий были установлены члены ОПГ, организовавшие масштабные хищения денежных средств. Преступники различными способами добывали конфиденциальную информацию о всех реквизитах слипов (собирали выброшенные за ненадобностью первые экземпляры слипов по ранее совершенным расчетно-кассовым операциям, приискивали номера карт и фамилии их владельцев и т. д.). С помощью этих сведений и вышеуказанных СВТ изготавливались качественные подделки, содержащие все необходимые печатные и рукописные реквизиты. После этого через своих сообщников – кассиров мерчантов и работников эквайреров документы внедрялись в расчетную банковскую систему. Полученные от криминальных операций деньги наличными изымались из касс тех же мерчантов. Оперативным путем были также установлены несколько известных коммерческих фирм, в помещениях которых изготавливались поддельные слипы.

В результате указанной преступной деятельности со счетов различных коммерческих банков г. Москвы было похищено 2 млрд рублей. Помимо этого, сотрудниками ГУЭП было предотвращено хищение еще свыше 3 млрд рублей. Именно на такую сумму были изъяты поддельные слипы, обнаруженные в ходе проведения обысков у членов ОПГ и в помещениях «полиграфических» фирм.

Документы, в которых необходимо искать следы способа: поддельные слипы; контрольные печатные элементы бланка и реквизитов слипов; макеты слипов и их части; полиграфический брак; пластиковые карты; подлинные оформленные экземпляры слипов и их частей; листы с тренировочными подписями; заявления держателей карт об отказе оплаты товаров и услуг по биллингу (у эмитента); справки из процессинговых центров компаний о номерах пластиковых карт, именах их держателей и эмитентах, выдавших данные карты; сводный список по отказным или возвратным операциям (у эмитента); справки по операциям СКС с указанием их владельцев, реквизиты которых были использованы мошенниками при подделке слипов; кассовые отчеты конкретных мерчантов, из которых были инкассированы поддельные слипы; «Стоп-листы».

2. Незаконное использование специальных технических средств (СТС), предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения конфиденциальной информации о реквизитах пластиковых карт и их держателях. Как показывает анализ отечественной и зарубежной следственной практики, в последнее время преступления очень часто стали совершаться хорошо организованными, мобильными, оснащенными высокотехнологичным оборудованием, специальной техникой и всевозможными приспособлениями преступными группами.

В качестве специальных технических средств подготовки и совершения преступлений часто используются разнообразные разработанные, приспособленные и запрограммированные устройства для негласного получения и регистрации акустической информации; визуального наблюдения и документирования финансовых операций; прослушивания телефонных переговоров; перехвата и регистрации информации с технических каналов электросвязи; получения (модификации, уничтожения, копирования) информации с технических средств ее хранения, обработки и передачи; нарушения работы ЭВМ, системы ЭВМ или их сети; для проникновения и обследования помещений, автомобилей и других объектов; контроля за перемещением транспортных средств, отдельных физических лиц, товаров и других объектов.

Преступления, совершенные с применением указанных технических средств и специальных методов работы с ними, отличаются чрезвычайно высокой общественной опасностью. Это обусловлено как уголовно-правовой квалификацией данных деяний, так и рядом объективных и субъективных факторов криминалистического по-

рядка. В целях улучшения негативной обстановки рассмотрим следующие способы преступных посягательств.

2.1. Активный (контактный) перехват конфиденциальной информации о реквизитах пластиковых карт и их держателях осуществляется путем непосредственного подключения специальных технических средств к машинному носителю карты и памяти банкомата. В данном случае преступник негласно и целенаправленно воздействует на программные и аппаратные средства электронных терминалов, обеспечивающие совершение операций по картам. В зависимости от вида СТС – орудия преступления это возможно следующими путями.

Использование лжебанкомата. В конце апреля 1993 г. в торговом центре «Баклэнд хилс», расположенном в г. Манчестере штата Коннектикут (США), членами ОПГ был установлен фальшивый напольный банкомат, который внешне ничем не отличался от других: он был закомуфлирован под банкоматы, принадлежащие одному крупному и известному банку-эквайреру. Во время своей работы он выдавал стандартные сообщения и поэтому не вызывал у держателей карт каких-либо сомнений в его подлинности. Вместе с тем, выдав несколько долларов по запросу первого клиента, он перестал работать. Держатели вставляли свои карты в приемное считывающее устройство и набирали на клавиатуре ПИН-код. Однако через некоторое время банкомат возвращал их обратно, а на его экране появлялась надпись «Извините, операция прекращена». Клиенты удивлялись и повторяли операцию еще раз, но результат был тот же. За это время банкомат автоматически записывал в свою постоянную память номер карты, банковский идентификационный номер ее эмитента, реквизиты банковского счета и его владельца, ПИН-код доступа к операциям по счету, сумму остатка средств на счете, а также служебную (системную) информацию, раскрывающую формат электронных документов и тип программных приложений.

Для привлечения к своему лжебанкомату большего числа держателей карт – потерпевших преступники вывели из строя все банкоматы, расположенные в торговом центре – месте преступления. В этих целях они покрывали эпоксидным клеем магнитную полосу выброшенной кем-то за ненадобностью недействующей пластиковой карты и поочередно вставляли ее в считывающее устройство каждого банкомата. Высохнув, клей засорил считывающие головки ридеров и заблокировал их входные технологические отверстия. 9 мая 1993 г. после закрытия торгового центра по случаю праздника «День матери» трое преступников, представившись работникам

и охранникам торгового комплекса как сотрудники ремонтной организации, погрузили «испортившийся» банкомат в арендованный грузовик и увезли его «на ремонт».

За время работы лжебанкомата мошенникам удалось получить конфиденциальные реквизиты более чем 300 карт и их держателей. Впоследствии с использованием этой информации были изготовлены поддельные карты для банкоматов. С их помощью в г. Нью-Йорке и городах штата Флорида (США) совершены хищения наличных денежных средств на общую сумму 500 тыс. долларов США.

После длительных поисков сотрудникам ФБР удалось выйти на след преступников и в конечном итоге арестовать их. С исследовательской точки зрения интересен приговор суда: организатор и руководитель преступной группы был приговорен к 4 годам лишения свободы и возмещению причиненного убытка в размере 500 тыс. долларов; один из активных участников ОПГ осужден к 2,5 годам лишения свободы и штрафу в размере 200 тыс. долларов; другие мошенники приговорены к 6 месяцам лишения свободы и штрафу в 25 тыс. долларов[194].

Использование мобильных ПЭВМ малых размеров. Иногда преступникам удается негласно подключить к соответствующим коммуникационным портам электронных терминалов, обеспечивающих проведение операций по пластиковым картам, портативные ПЭВМ – в блокнотном исполнении («ноутбук») и в виде записной книжки («сабноутбук»). Поскольку эти ПЭВМ работают на автономных источниках электропитания – батарейках и аккумуляторах, они могут непрерывно в течение нескольких десятков часов осуществлять запись конфиденциальных реквизитов из памяти терминала. Плоский корпус ПЭВМ позволяет преступникам легко камуфлировать их под окружающую обстановку, например под дополнительную боковую или заднюю панель.

По прошествии определенного периода времени компьютер изымается с места его установки, а накопленная в его постоянной памяти конфиденциальная информация о реквизитах пластиковых карт, их держателях, ПИН-кодах и произведенных операциях используется для совершения хищений. Например, таким способом было подготовлено и совершено хищение денежных средств в Ве-

---

[194] См.: Мошенничество с использованием банкоматов // Материалы международного семинара по борьбе с экономическим мошенничеством и изготовлением фальшивых денег. Вашингтон, округ Колумбия, 27 марта – 7 апреля 1995 г. Секретная служба Соединенных Штатов: отдел расследований. – Вашингтон, 1995.

ликобритании: преступникам удалось скрытно вмонтировать «ноутбук» в автоматизированную бензоколонку на АЗС[195].

Использование СТС, приспособленных из бытовой аппаратуры и изготовленных кустарным способом. В настоящее время в России существует немало одаренных, но безработных людей, которые тратят свой природный интеллектуальный и приобретенный профессиональный талант на криминальные цели. Именно ими придумываются хитроумные и технически изощренные способы получения конфиденциальных реквизитов, необходимых для совершения хищения денежных средств[196]. Отметим лишь два из них.

А. Специально изготовленные клавиатуры – «двойники» и электромагнитные сканеры. Следственной практике известны случаи изготовления специальных технических устройств, состоящих из трех следующих блоков.

1) Специальной клавиатуры с сенсорными клавишами, которая накладывается на стандартную управляющую клавиатуру банкомата. Она не позволяет нажимать на клавиши «родной» клавиатуры и управлять работой банкомата. Вместе с тем набираемый держателем ПИН-код передается в блок управления СТС и сохраняется на флэш-карте.

2) Рамки, прикрепляемой к технологической щели считывателя банкомата для электромагнитного перехвата (сканирования) электронных реквизитов с магнитной полосы карты.

3) Миниатюрного блока управления клавиатурой, сканером и устройством записи перехваченной информации на флэш-карту в виде мини-ЭВМ.

Все составляющие вышеуказанного программно-аппаратного СТС скрытно устанавливаются на избранный преступниками банкомат, камуфлируются под технологические элементы его корпуса и впоследствии также негласно изымаются[197].

Б. Использование цифровой микровидеокамеры и стандартного ридера с доработанной электронной схемой. Этот способ является технологической разновидностью вышерассмотренного. СТС конструктивно собрано из следующих устройств.

---

[195] Подробнее см.: *Батурин Ю.М.* Проблемы компьютерного права. – М., 1991. – С. 79.

[196] Подробнее см.: *Вехов В.Б.* Компьютерные преступления: Способы совершения и раскрытия / Под ред. акад. Б.П. Смагоринского. – М., 1996. – С. 57-104.

[197] См.: Способы мошенничества // Программа обучения сотрудников полиции борьбе с мошенничеством с использованием платежных пластиковых карточек / Авт. и сост: Международная платежная система Visa International Association CEMEA, при поддержке Ассоциации «ВИЗА» в России. – 2001.

1) Обычной цифровой микровидеокамеры – устанавливается таким образом, чтобы зафиксировать ПИН-код, вводимый держателем с клавиатуры банкомата. Поскольку в некоторых банкоматах установлены наружные камеры автоматизированных охранных систем, она, как правило, не привлекает внимания клиентов.

2) Стандартного универсального ридера, электронная схема которого доработана таким образом, что может автоматически накапливать в своей флэш-памяти электронные реквизиты карт, вставляемых в отверстия его считывающих устройств. Ридер устанавливается таким образом, чтобы закрыть своим корпусом приемное отверстие считывателя банкомата.

Цифровые микровидеокамера и считыватель работают непрерывно в течение нескольких часов на миниатюрных автономных источниках питания. Именно такой способ весной 2003 г. использовали члены преступной группы из числа студентов столичных вузов для изготовления поддельных банковских карт и совершения серии хищений наличных денежных средств из банкоматов, установленных на улице Садовое кольцо. Сумма причиненного ими ущерба составила более 700 тыс. долларов США. Данный способ широко освещался отечественными средствами массовой информации[198].

2.2. Пассивный (бесконтактный) перехват конфиденциальных сведений о реквизитах пластиковых карт и их держателях. К этой группе относятся способы, позволяющие осуществлять дистанционное сканирование реквизитов карт, секретных кодов, ключей и шифров доступа, получение которых обеспечивает подготовку и совершение преступлений исследуемой категории. Они основаны на перехвате электромагнитных излучений, отражаемых от реквизитов пластиковых карт, клавиатур управления и изображений на экранах электронных терминалов, а также испускаемых в окружающую среду работающими СВТ и электросвязи. Их криминалистическое содержание состоит в следующем.

Известно, что свойство отражения присуще всей материи. Оно присутствует всегда, когда имеет место взаимодействие двух и более объектов. Так, если в одном объекте происходят изменения, отражающие факт воздействия на него другого объекта, то говорят, что первый объект становится носителем информации о втором. Первый объект называют «следовоспринимающим» или «приемником информации», а второй – «следообразующим» или «источником информации». При этом, когда говорят о процессе передаче

[198] Например, см.: *Федоров А.* Операция «банкомат» // Труд. – 2003. – 24 апр. – С. 21.

информации между этими объектами, то подразумевают систему сведений об их признаках, свойствах, механизме взаимодействия друг с другом и окружающей средой. Конкретные сведения, получаемые приемником от источника информации, называются *сообщениями.* Сообщения передаются при помощи сигналов. *Сигнал* является отображением сообщения и средством переноса информации в пространстве и во времени[199]. Подчеркнем, что *при передаче сообщения от одного объекта к другому одни сигналы могут порождать другие*. Так, звуковой сигнал может вызвать механический (колебания барабанной перепонки в ухе живого существа или мембраны микрофона в техническом устройстве), механический – электрический (в слуховом рецепторе, катушке микрофона, пьезоэлементе), электрический – электромагнитный (в антенне радиопередатчика), механический (сокращение мышцы тела), химический (электролитическую реакцию образования нового вещества) или световой (мигание лампочки, излучение УФ- или ИК-волн), световой – электрический (в фотоэлементе, колбочках – рецепторах сетчатки глаза) или химический (на фотопленке (фотобумаге), фотосинтез у растений). В свою очередь, запаховый сигнал может быть преобразован в электрический (обонятельными рецепторами) и т. д.

Сигналы могут быть взаимосвязаны в пространстве и во времени, например звуковое кино.

Как правило, процесс передачи информации от источника к потребителю – конкретному субъекту или объекту (техническому регистрирующему или управляющему устройству) осуществляется по многоступенчатой схеме с помощью каналов связи. На каждой такой ступени сигнал может быть преобразован в ту или иную форму, а также изменить свою физическую природу (неизменным остается лишь его содержание). Причем такие преобразования осуществляются не хаотично, а по определенным правилам, которые называются *кодом*.

Процесс перевода сообщения в сигнал состоит из следующих операций:

1) *преобразования* – приведения исходного сообщения в форму, удобную для того или иного вида кодирования;

2) *кодирования* – построения элементов сообщения по определенному алгоритму;

---

[199] **Сигнал** – условный знак для передачи какого-либо сообщения, распоряжения, команды и т. п. – См.: Словарь русского языка: В 4-х т. Т. 4 / АН СССР, Ин-т рус. яз.; Под ред. А.П. Евгеньевой. – 3-е изд., стер.– М., 1985–1988. – С. 89.

3) *модуляции* – воздействия на закодированное сообщение с целью превращения его в сигнал;

4) *отправки* – записи сигнала на транспортный (промежуточный) материальный носитель информации (введения сигнала в канал связи).

Процесс превращения сигнала в образ исходного сообщения осуществляется в обратном порядке, а именно:

1) *получения* – регистрации сигнала, его выделения из материального носителя (из канала связи);

2) *демодуляции* – воздействия на сигнал с целью превращения его в закодированное сообщение;

3) *раскодирования* – восстановления элементов сообщения по алгоритму, по которому оно было закодировано;

4) *преобразования* – приведения раскодированного сообщения в форму, доступную для его восприятия получателем (адресатом) – человеком (в человекочитаемую форму) или техническим устройством (машиночитаемую форму).

С точки зрения положения во времени и пространстве сообщения и сигналы делятся на статические и динамические. *Статические* – это сообщения и сигналы, которые отображают устойчивые изменения состояния объекта-носителя, например фотоснимок, ячейка с информацией в памяти ЭВМ, файл данных, магнитная метка, штрих-код, данные на магнитной полосе или интегральной микросхеме памяти и т. д. *Динамические* – отображают непрерывные изменения состояния объекта – носителя либо процесс его перехода из одного устойчивого состояния в другое, например, электромагнитные, упругие или гравитационные колебания.

По своей структуре сообщения и сигналы делятся на непрерывные и дискретные: прерывистые, дробные, состоящие из отдельных частей (порций). *Непрерывным* называется сообщение (сигнал), которое в конечном интервале амплитуд принимает произвольное количество значений. Например, сообщения в аналоговых регистрирующих (измерительных) стрелочных устройствах (часах, барометрах, манометрах и т. д.) или средствах проводной телефонной электросвязи (модуляция несущей частоты под воздействием механических колебаний мембраны микрофона, возбуждаемых речью говорящего и иными звуками). Если сообщение (сигнал) в конечном интервале амплитуд принимает ограниченное количество значений, то оно (он) называется *дискретным*.

Дискретные сигналы как средство передачи информации нашли более широкое применение, чем непрерывные. Это объясняется

тем, что они в меньшей степени подвержены влиянию помех в каналах связи, искажение дискретного сигнала легче обнаружить и восстановить, чем непрерывного. Помимо этого дискретные сигналы легко обрабатываются на СВТ и электросвязи, а также отображаются устройствами цифровой индикации[200].

С учетом вышеизложенного, принимая за основу физическую форму конфиденциального сообщения (сигнала), способы рассматриваемой группы возможно подразделить на следующие виды.

Перехват оптических сигналов (изображений) в видимом диапазоне волн. Осуществляется преступником с помощью различной видеооптической техники (в том числе и специальной): оптических, оптикоэлектронных, телевизионных, тепловизионных, лазерных, фото- и других визуальных средств съема информации. Данным способом преступнику удается незаконно получить графические реквизиты пластиковой карты и ПИН-код в момент проведения их держателем операции с применением стационарного электронного терминала. С криминалистической точки зрения следует различать две разновидности этого способа: *дистанционную* и *контактную*.

А. Дистанционный видеоперехват. Производится с применением различной бытовой и специальной общедоступной видеотехники: бинокля, фотоаппарата с объективом и удлинительными кольцами, портативной видеокамеры, подзорной трубы, оптического охотничьего прицела, прибора ночного видения и т. п. При этом орудие преступления находится непосредственно в руках преступника, который скрытно наблюдает за электронным терминалом на значительном расстоянии и фиксирует на бумаге, фотовидеопленке или машинном носителе информации интересующие его конфиденциальные реквизиты.

Следы преступления по месту нахождения преступника зависят от использованного им способа маскировки себя и видеоаппаратуры, имеющихся специальных знаний негласного наблюдения, наличия в его распоряжении транспортного средства, окружающей среды объекта наблюдения.

Типичные орудия совершения преступления: видеоаппаратура и ее комплектующие, техническая документация на нее; документы, свидетельствующие о приобретении видеотехники (чеки, счета, расписки); методическая литература и видеоматериалы по негласному применению видеоаппаратуры (печатные и рукописные литературные источники, специальные и художествен-

---

[200] Подробнее см.: *Цимбал В.П.* Теория информации и кодирования. – Киев, 1973. – С. 5-7.

ные видеофильмы на видеокассетах, компакт-дисках и в памяти ПЭВМ); фото- и видеодокументы в форме кадров и видеосюжетов, отражающих проведение операций с использованием пластиковых карт потерпевшими (в кассетах – на фото- и видеопленке, на фотографиях, в памяти видеоаппаратуры (включая сотовый радиотелефон с микровидеокамерой), на флэш-картах, компакт-дисках, винчестере ПЭВМ, памяти); печатные и рукописные материалы с реквизитами чужих пластиковых карт и ПИН-кодами.

Б. Контактный видеоперехват. Заключается в установке видеоаппаратуры в непосредственной близости от места расположения электронного терминала либо на нем самом. В этом случае видеозаписывающая и (или) передающая аппаратура камуфлируется под предметы окружающей среды либо внешние технологические элементы терминала. Таким образом, способ предполагает наличие одновременно двух или трех мест происшествия – *место нахождения электронного терминала*, *установки СТС* для негласного получения информации, *пребывания преступника*, осуществляющего визуальный контроль за работой СТС и ходом криминальной операции.

Типичные орудия совершения преступления: бытовая программируемая мини- и микровидеокамера; мини- и микровидеокассета с магнитной лентой; флэш-карта; сотовый радиотелефон с интегрированной микрофото- или видеокамерой.

Помимо вышеуказанных к предыдущему способу, типичными следами преступления также являются: трасологические следы установки и крепления выносной видеоаппаратуры; следы человека на электронном терминале и в непосредственной близости от него.

Перехват электромагнитных сигналов. Современные бытовые, приспособленные и специальные технические средства – СВТ и электросвязи позволяют получать конфиденциальную информацию об операциях, производимых с использованием пластиковых карт, дистанционно, находясь на значительном расстоянии от средств ее обработки, хранения и передачи. Это связано с тем, что любой проводник, по которому передается электрический сигнал, порождает собой дополнительный – паразитный электромагнитный сигнал. Как было указано выше, последний является отражением исходного сигнала и несет в себе такое же информационное сообщение. Используя соответствующие технические устройства, преступник принимает этот сигнал, раскодирует его и прочитывает. При этом, как правило, осуществляется запись перехваченного сигнала в память приемного устройства и на машинные носители информации. В зависимости от формы перехватываемого электро-

магнитного (ЭМ) сигнала выделяются две следующие разновидности данного способа.

А. Перехват ЭМ сигналов стандартной формы из каналов радиосвязи. Большинство современных терминальных устройств при проведении операций по пластиковым картам используют различные каналы радиосвязи. Например, в ИК-диапазоне частот с дальностью до 60 м осуществляются:

а) беспроводная электросвязь ЭВМ электронного терминала с клавиатурой управления, принтером и (или) ридером либо с локальной автоматизированной кассовой сетью;

б) дистанционное считывание с карты штрих-кода ридером терминального устройства;

в) связь микропроцессорной суперсмарт-карты с терминальным устройством;

г) работа местного бимчекера.

На расстоянии 350–450 м от сервера АКС в диапазоне частот от 140 до 902 МГц, с каналом передачи конфиденциальных данных, располагающимся между 30–100 кГц, работают локальные бимчекеры.

Связь банкоматов, бимчекеров дальнего радиуса действия и сотовых радиотелефонов с ЭВМ процессингового центра осуществляется в диапазонах 825-845 МГц стандартов AMPS и D-AMPS, 453-457,5 МГц стандарта NMT, 890-915 МГц – GSM 900, 1,8-1,9 ГГц – GSM 1800 и других[201].

Для перехвата конфиденциальных электронных реквизитов пластиковых карт, электронных документов и ПИН-кодов из вышеприведенных каналов связи преступниками активно используются доступные бытовые и специальные радиоприемные устройства (радиосканеры), открыто продающиеся на радиорынках и с рук отдельными лицами. Например, в сети Фидонет можно встретить информационные сообщения следующего содержания:

Сергей Маревский (Sergey Marevsky), адрес в сети ФИДО – 2:5020/1084.

Домашний телефон: 183-0717. Пейджер: (095) 232-0000 аб. 33262.

Объявление о продаже

«Это Моторола Платинум от Билайна. Такой крутой, с толстой откидывающейся крышкой. Работает везде, где есть Билайн. Сами телефоны без сканера – вводишь код в память и работаешь с этого кода. Входящий и исходящий номера. Межгород тоже будет, а вот международная связь крайне редко. Но зато полная ХАЛЯВА. Память на 100 кодов. На базе 9354. Стоимость – 300$ с аккумулятором и 270$ без него.

---

[201] Подробнее см.: *Леонтьев Б.К.* Фрикинг без секретов. – М., 2001. – С. 503-524.

И также сканеры, которые позволяют использовать как обычный сотовый, так и ловить коды в эфире. Сканеры с дальностью работы на 4 км по городу. На базе 9308. Цена договорная.

Если кого интересует – присылайте телефоны для связи».

Эти СТС также можно изготовить из соответствующих радиоприборов, предлагаемых к продаже в тех же местах. Так, в августе 1998 г. Воронежским областным судом за мошенничество с использованием сотовых радиотелефонных аппаратов к различным срокам тюремного заключения были приговорены 44-летний житель г. Москвы М. и 37-летний житель Воронежа, безработный Л., которые по предварительному сговору причинили имущественный ущерб абонентам, обслуживаемым сотовой телефонной компанией «Вотек Мобайл». М. на совместные с Л. деньги приобрел в Москве несколько сотовых радиотелефонных аппаратов фирмы «Моторола» и соответствующее количество перепрограммируемых интегральных микросхем, содержащих в своей памяти специальные программы для ЭВМ. Он установил их в слоты радиотелефонов, в которые оператором связи подключаются микросхемы SIM-карт. В результате этого аппараты получили возможность работы в режиме автосканирования на коммерческой частоте оператора сотовой электросвязи «Вотек Мобайл», то есть превратились в СТС для негласного перехвата сообщений и конфиденциальных реквизитов идентификации абонентов в этой сети радиосвязи. Затем М. разработал инструкции по записи перехватываемых данных в память установленных микросхем. Указанные орудия совершения преступления М. передал своему сообщнику Л., который применил их в г. Воронеже. Там он, поочередно используя изготовленные М. СТС, подключал их к сети «Вотек Мобайл», перехватывал электронные идентификационные реквизиты абонента, работающего в этот момент в сети, и по указанному в инструкции алгоритму записывал их в память установленной микросхемы. Таким образом, получалась несанкционированная копия SIM-карты. Запрограммированные таким способом сотовые радиотелефоны-«двойники» Л. сбывал в том же городе, а полученные от их продажи денежные средства делил с М. Во время работы такого телефонного аппарата в сети электросвязи радиотелефон законно зарегистрированного абонента блокируется – его использование невозможно. Вместе с этим именно он оплачивает все переговоры, ведущиеся по телефону-«двойнику» (включая и свои собственные)[202].

---

[202] Подробнее см.: *Родионов А.* Компьютерные преступления и организация борьбы с ними // Профессионал.– 1999. – № 5. – С. 16.

Типичные следы преступления: заявление держателя карты (абонента сети электросвязи) об отказе оплаты отдельных произведенных операций (услуг, товаров); отсутствие в электронном журнале (записной книжке сотового радиотелефона) записей о соответствующих операциях, зарегистрированных эмитентом (оператором электросвязи); выписка из биллинга (счета) по каждой «отказной» операции с подробным указанием их реквизитов (даты и времени совершения, идентификационного номера терминала, принадлежности терминала конкретному лицу и его местонахождения, вида операции, суммы операции); электронные данные, содержащиеся в памяти поддельной карты и СТС для негласного получения электронных реквизитов; схемы, инструкции и другая справочная литература по созданию и использованию СТС; составные блоки, части и детали, используемые для создания СТС или приспособления бытового радиотехнического устройства для негласного получения конфиденциальной информации.

Б. Перехват и расшифровывание ЭМ сигналов, распространяющихся по техническим каналам основных и вспомогательных средств и систем обеспечения технологий пластиковых карт в форме паразитных информативных физических полей. Ими являются: побочные ЭМ излучения и наводки (ПЭМИН); паразитные модуляции высокочастотных сигналов, возбуждаемые в различных проводах, которые находятся по месту расположения электронных терминалов и могут выступать в качестве приемной антенны СТС; паразитные информативные токи и напряжения, образуемые за счет эффекта электроакустического преобразования сигналов в сетях электросвязи, электрофикации, электрочасофикации, охранно-пожарной сигнализации, в сетях СВТ, в блоках СВТ и т. п.[203]

Лабораторные опыты показывают, что наиболее мощные и достаточно легко расшифровываемые информативные сигналы исходят от работающих мониторов с электронно-лучевой трубкой (ЭЛТ), принтеров, ридеров, соединительных и электропитающих проводов, а также модемов электронных терминалов. Так, например, ЭЛТ монитора ПЭВМ или банкомата излучает в окружающее пространство ЭМ сигналы, которые могут быть перехвачены на рас-

[203] Подробнее см.: *Андрианов В.И., Бородин В.А., Соколов А.В.* «Шпионские штучки» и устройства для защиты объектов и информации: Справ. пособие. – СПб., 1996. – С. 174.

стоянии до 1000 м[204]. В этих целях преступниками используются обычные дипольная антенна и ТВ-приемник (телевизор), имеющий частично доработанную схему, либо СТС, функционирующие на базе приемников ЭМ сигналов. С помощью указанных орудий преступникам удается на расстоянии до 1 км видеть и записывать на материальный носитель то, что видит на экране банкомата держатель или мониторе ПЭВМ оператор, осуществляющий операцию с использованием пластиковой карты.

По данным отдельных исследователей, современные технические средства позволяют получать и прочитывать сообщения, передаваемые паразитными ЭМ сигналами, на расстоянии до 150 м от работающего принтера и до 500 м от соединительных электронесущих проводов (кабелей, шлейфов)[205].

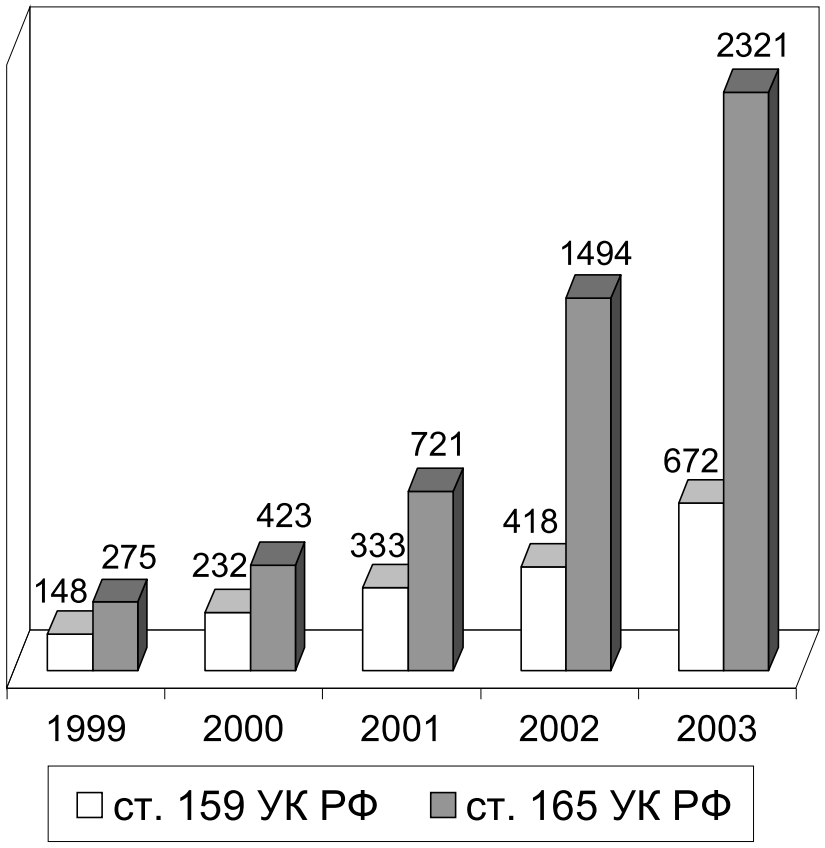
3. Незаконное получение и использование конфиденциальной компьютерной информации о реквизитах пластиковых карт и их держателях в компьютерной сети Интернет. В конце 90-х годов прошлого века и тысячелетия с развитием на территории Российской Федерации и стран, ранее входивших в состав СССР, глобальной компьютерной сети Интернет она превратилась в мощное средство подготовки, совершения и сокрытия преступлений многих видов, в том числе и выделенных нами. Так, по данным Главного информационного центра МВД России, количество имущественных преступлений, совершаемых с использованием Интернет, ежегодно увеличивается в среднем в 1,6 раза. Это наглядно видно из следующей диаграммы.

---

[204] Методику получения указанных экспериментальных данных см.: *Вим ван Эйк*. Электромагнитное излучение видеодисплейных модулей: риск перехвата информации? // Защита информации. Конфидент. – 2001. – № 2. – С. 84-93.

[205] См.: Преступления в сфере компьютерной информации: квалификация и доказывание: Учеб. пособие / Под ред. Ю.В. Гаврилина. – М., 2003. – С. 62.

Динамика роста имущественных преступлений, совершенных с использованием сети Интернет



По мнению специалистов международных платежных систем, высокий уровень мошенничества в Интернете является основным сдерживающим фактором развития электронной коммерции, поскольку держатели платежно-расчетных пластиковых карт, их эмитенты, а также эквайреры и мерчанты боятся широко пользоваться этой телекоммуникационной технологией из-за опасности понести серьезные финансовые потери[206].

Применительно к рассматриваемому виду преступлений целесообразно сгруппировать все известные способы их совершения с использованием сети Интернет и расположить по частоте встречаемости в отечественной следственной практике следующим образом.

3.1. Мошенничество с использованием незаконно добытых электронных реквизитов платежно-расчетных пластиковых карт и их держателей. Эти реквизиты добываются преступниками

[206] См.: *Голдовский И.* Безопасность платежей в Интернете. – СПб., 2001. – С. 63.

всеми возможными способами, в том числе рассмотренными ранее по тексту настоящей работы. В большинстве случаев они используются мошенниками для оплаты товаров и услуг, рекламируемых различными предприятиями, учреждениями и организациями на своих электронных страницах или сайтах в сети Интернет. *Сайт представляет собой специализированную программу для ЭВМ*, дистанционно обеспечивающую ведение диалога между продавцом – поставщиком товаров или услуг и покупателем – держателем пластиковой карты, а также проведение расчетов за выбранный товар. Эта программа содержит несколько управляемых по единой логике электронных страниц с текстовой, графической, иногда звуковой информацией и называется «виртуальным», «электронным» или «интернет-магазином».

Каждая страница, по замыслу ее разработчика, выполняет определенную функцию, например: «витрины магазина» в виде прайс-листа (рекламы) предлагаемого товара (услуги) с его изображением, полным описанием свойств и ценой; регистрационной карточки покупателя (клиента); листа заказа покупаемого товара (услуги); первичного расчетно-учетного документа, юридически подтверждающего факт покупки товара (услуги). Именно для заполнения последнего электронного документа мошенниками и используются чужие реквизиты. В нем преступники указывают свое имя и адрес соответствующего почтового отделения для получения похищенного товара, а оплату за него производит держатель карты, реквизиты которой вносятся в соответствующие графы данного платежного документа. При этом, как правило, достаточно ввести с клавиатуры ПЭВМ вид платежно-расчетной карты, ее номер и срок действия. Например, в 1998 г. Нагатинским межмуниципальным судом ЮАО г. Москвы за совершение мошенничества в крупных размерах на пять лет лишения свободы условно был осужден 17-летний студент одного московского технического вуза Павел Ш. Как следует из материалов уголовного дела, в октябре 1997 г. он, находясь у себя дома, с помощью принадлежащих ему персонального компьютера и модема, имея на основании соответствующего договора законный доступ к сети Интернет, произвел соединение с электронным магазином, принадлежащим американской компании «PC Tech». После чего, выдав себя за держателя кредитной карты № 4254 XXXX XXXX 9331, заказал компьютерное оборудование на общую сумму 5900 долларов США. Через несколько дней Ш. полу-

чил его на складе представителя международной курьерской компании «Федерал Экспресс» в г. Москве[207].

Следы хищения, совершенного указанным способом, можно обнаружить:

1) в заявлении держателя карты об отказе оплаты отдельных произведенных операций (услуг, товаров);

2) в выписке из биллинга (счета) держателя по каждой «отказной» операции с подробным указанием их вида, даты, времени и места совершения, а также расходной суммы;

3) в выписке из электронного журнала (базы данных) регистрации покупателей (клиентов) интернет-магазина, содержащей идентификационные признаки лица, совершившего указанные операции;

4) в выписке из клиентской базы данных магазина, содержащей конфиденциальные реквизиты лица, оплатившего похищенный товар (услугу), а также телефонный номер, электронный адрес (IP) абонента сети Интернет[208] или шифр аппарата электросвязи (электронного терминала), с помощью которого была осуществлена расчетная операция;

5) в справке от оператора электросвязи или провайдера услуг Интернета о принадлежности указанного телефонного номера, IP-адреса или шифра искомого терминала к числу обслуживаемых абонентов, а также местонахождении оконечного оборудования (телефонного аппарата, ПЭВМ и др.);

6) в выписке из счета (лог-файла) абонента по тем соединениям с сетью электросвязи или Интернет, реквизиты которых указаны в учетном документе, предоставленном из интернет-магазина (п. 4), – берется у оператора электросвязи или провайдера;

7) при исследовании информации о реквизитах совершенных криминальных операций, содержащейся в памяти телефонного аппарата или ПЭВМ (протокол выхода в Интернет);

8) при обнаружении похищенного имущества.

---

[207] См.: Уголовное дело № 123688-98 // Архив Нагатинского межмуниципального суда ЮАО г. Москвы.

[208] **Адрес IP** (от англ. «Internet Protocol» – интернет-протокол) – адрес, присваиваемый провайдером услуг Интернет компьютеру своего абонента. Он описывает формат пакета данных, передаваемых по сети. Представляет собой 32-разрядное двоичное число, которое записывается в виде четырех десятичных чисел, разделенных точкой. Каждое такое число изменяется в интервале от 0 до 255, например: 193.124.5.38. Адрес IP служит для идентификации конкретной ЭВМ в сети Интернет. – Подробнее см.: *Фролов А.В., Фролов Г.В.* Всемирная паутина. Ваш спутник в Интернете. – М., 2000. – С. 121.

3.2. Мошенничество при оформлении возврата платежа по операциям, совершенным с использованием незаконно добытых электронных реквизитов платежно-расчетных пластиковых карт и их держателей. Данный способ является технологической разновидностью предыдущего. Его содержание целесообразнее всего раскрыть с помощью следующего яркого примера из отечественной юридической практики, ставшего известным широкой общественности из средств массовой информации.

В середине сентября 1998 г. сотрудники службы безопасности одного из московских коммерческих банков заметили, что на специальный карточный счет некоего В. вместо положенной стипендии стали поступать значительные денежные средства в долларах США. О данном факте было сообщено в правоохранительные органы. При проверке поступившего материала особое подозрение у сотрудников ГУЭП МВД России вызвал тот факт, что деньги после поступления сразу же обналичивались и снимались через сеть банкоматов. В. – студент одного из технических вузов Москвы был задержан для выяснения обстоятельств дела по месту проживания в г. Мытищи. Он сознался в незаконном получении денежных средств по своей дебетовой карте. В результате проведения оперативно-разыскных мероприятий удалось выйти на сокурсника, друга В. – Ф., проживающего в одном доме с задержанным и являющегося одержимым пользователем ПЭВМ и абонентом сети Интернет. Из его показаний стало известно, что руководит их действиями неизвестный, имеющий сетевое имя (кличку) «Спайбулл» (он же «Ансельм»), с которым Ф. («Биохазард») познакомился во время сеанса работы в одном из чатов[209], ни разу с ним не встречался и не собирался встречаться. Именно данный субъект и организовал преступную группу, отработал механизм преступления, распределил роли. Так, В. на свое имя были открыты несколько СКС; Ф., в свою очередь, отвечал за обналичивание денег, поступающих на эти счета, из которых 40 % были его и В., а 60 % – «Спайбулла». Эти деньги передавались организатору хищения в дипломате через камеру хранения. При этом название железнодорожного вокзала, где она находится, номер секции, ячейки и кода доступа сообщались Ф. по сотовому телефону, номер которого был передан ему по Интернету.

---

[209] **Чат** (от англ. «chat» – разговор) – электронная страница в сети Интернет для одновременного обмена текстовыми сообщениями между несколькими пользователями в режиме реального времени.

Установить личность «Спайбулла» не представлялось возможным по причине практически полного отсутствия идентифицирующих его личность материальных следов. Но в этом случае оперативным сотрудникам помогли объективные обстоятельства – кризис банковской системы, когда рубль обесценивался стремительно, в связи с чем банки приостановили выдачу наличной иностранной валюты своим клиентам. Чтобы быстрее конвертировать полученные от очередной преступной транзакции рубли в СКВ «Спайбулл» пошел на риск и назначил Ф. встречу около одного из ночных клубов на Волоколамском шоссе. Там он и был задержан при передаче денег. Таким образом, личность «Спайбулла» была установлена: руководителем преступной группы и организатором хищений на общую сумму свыше 20 тыс. долларов США оказался студент гуманитарного вуза г. Москвы, талантливый скрипач – И.Г.

Готовясь к совершению преступления, на одном из хакерских сайтов сети Интернет им была обнаружена кем-то похищенная база данных одного из американских электронных магазинов, в которой находились конфиденциальные реквизиты пластиковых карт и их держателей – клиентов магазина. Он скопировал ее на свой домашний персональный компьютер. Далее, от имени этих лиц, он стал осуществлять многочисленные покупки товаров в различных интернет-магазинах. Поскольку передача товара покупателю осуществляется не сразу, а по прошествии определенного времени (по почте), он вовремя делал отказ от покупки. В этом случае, по существующим правилам, товар клиенту не отправлялся, а списанные с его счета деньги возвращались обратно. Особенностью технологии возврата денег и воспользовался И.Г. Вместо реквизитов счета, указанного при покупке товара, он указывал в листе возврата данные специальных карточных счетов В., на которые и зачислялись соответствующие денежные средства. Использование данного способа стало возможно по той причине, что банки эквайреры и эмитенты никогда не сверяют реквизиты СКС, с которого осуществляется списание денежных средств, с теми, по которым в случае отказа от операции происходит возврат этих же денег[210].

Помимо документов, указанных к предыдущему способу, следы преступления могут быть обнаружены:

1) в выписке по интересующему СКС с указанием истории приходных и расходных операций, а также особых условий его открытия;

---

[210] См.: *Демченко В.* Жадность хакеров сгубила // Известия. – 1998. – 23 сент. – С. 5.

2) при сопоставлении реквизитов первичных приходных документов с расходными по одинаковым суммам, исходящих от одного мерчанта;

3) в справках от мерчантов, эквайреров и эмитентов по «отказным» операциям с полным указанием их истории;

4) при анализе памяти ПЭВМ и сотового радиотелефона подозреваемого.

3.3. Использование вредоносных программ для ЭВМ. Поскольку при проведении исследуемых операций всегда используются электронные реквизиты пластиковых карт и их держателей, которые обрабатываются с помощью соответствующих программ для ЭВМ, то преступники вынуждены применять такие же средства в своих корыстных целях. Анализ зарубежной и отечественной следственной практики показывает, что в настоящее время в их арсенале имеется большое количество вредоносных компьютерных программ, а также специальных методов модернизации обычного программного обеспечения для совершения преступления. Разработаны специальные тактические рекомендации по их применению в различных условиях и обстановке.

Организованная преступность в начале XXI века и III тысячелетия стала широко использовать новые виды оружия – информационное оружие. Рассмотрим те его виды, которые применяются при совершении исследуемой категории преступных посягательств.

Программы генерации и подбора электронных идентификационных реквизитов пластиковых карт и их держателей. Вся система защиты конфиденциальных электронных данных и документов от несанкционированного доступа к содержащимся в них сведениям и использования их в преступных целях базируется на криптографических средствах. Их основу составляют специальные программы для ЭВМ, работающие по тому или иному алгоритму преобразования данных (DES, RSA и других). Если не вдаваться в подробности, то в общем эти программы оперируют со следующими цифровыми реквизитами: *ПИН-кодом* (простое целое число из 4 – 8 цифр); *номером карты* (до 19 цифр), состоящим из банковского идентификационного номера (BIN) – первые 6 цифр, 7 и 8 цифры – идентификационные номера филиалов и отделений эмитента, следующие 10 цифр – номер идентификации счета держателя, последняя цифра– цифра проверки на четность по контрольному алгоритму Luhn Check Parity, однозначно определяемая всеми остальными цифрами номера карты; *срок действия карты* – номер месяца (две цифры от 01 до 12) и года (последние две цифры года – от 00 до 99); *код доступа к платежной системе* – число,

состоящее из 3-х цифр, которые печатаются методом идент-печати на оборотной стороне карты на планке для подписи держателя после номера карты (в платежной системе «Visa» этот код называется «*CVV2*», а «Europay/MasterCard» – «*CVC2*»)[211].

Рассматриваемые вредоносные программы для ЭВМ работают по принципу простого перебора или подбора неизвестных цифр по тем же криптоалгоритмам. При этом чем больше известных преступнику цифр из указанных реквизитов будет введено в программу, тем быстрее она выдаст правильный вариант, соответствующий оригиналу.

По виду алгоритма различают **«код-грабберы»** – программы для ЭВМ, автоматически подбирающие неизвестные цифры в номере карты либо номер карты из его составляющих, ставших известными мошеннику, и **«генераторы паролей»** – компьютерные программы, которые генерируют реально не существующие, но логически верные идентификационные пары конфиденциальных реквизитов или определяют неизвестный реквизит из известного путем соответствующего вычисления. Например, с 1995 г. преступниками активно используется программа «Мастер кредиток» («CreditMaster»), которая распространяется через кардерские и хакерские сайты сети Интернет. На момент написания настоящей работы эта программа имела уже версию номер «4.0». Программа генерирует правильные номера не существующих платежно-расчетных карт, которые могли быть эммитированы отдельными банками. Для этого в программу заложен тот же самый алгоритм генерации номеров карт, который использует банк-эмитент для выпуска своих карточных продуктов.

Взлом клиентской базы данных интернет-магазина. Этот способ состоит в интеллектуальном взломе программной защиты баз данных электронных магазинов, содержащих всю конфиденциальную информацию о клиентах (держателях) и реквизитах их пластиковых карт. Он осуществляется с использованием вышерассмотренных вредоносных программ для ЭВМ или иными способами[212]. Стоит обратить внимание на то, что в настоящее время существует множество программ-«взломщиков», называемых на профессиональном языке «hacktools» (инструмент взлома) или «crack»-программы. Эти средства позволяют преступникам нейтрализовы-

---

[211] Подробнее см.: *Голдовский И.* Безопасность платежей в Интернете. – СПб., 2001. – С. 65-67.

[212] См., например: *Вехов В.Б.* Компьютерные преступления: Способы совершения и раскрытия / Под ред. акад. Б.П. Смагоринского. – М., 1996. – С. 64-88.

вать (блокировать, модифицировать и т. д.) программные средства защиты от несанкционированного доступа к электронным реквизитам, которые впоследствии используются для совершения хищения. Например, в январе 2000 г. неизвестным лицом, назвавшим себя «19-летний Максим из России», исследуемым способом был осуществлен несанкционированный доступ в клиентскую базу данных американской фирмы «Си-Ди юниверс», торгующей через Интернет музыкальными компакт-дисками с использованием реквизитов платежно-расчетных карт. Преступник незаконно скопировал на свой персональный компьютер электронные реквизиты 300 тыс. пластиковых карт и их держателей, являющихся клиентами этого интернет-магазина. Затем он по электронной почте и факсу направил в фирму сообщения, в которых предложил: «Вы заплатите мне 100 тыс. долларов США по указанному мною счету, я же ликвидирую прорехи в вашей системе электронной защиты от несанкционированного доступа, которую я взломал, и забуду про вашу фирму навсегда. Если вы не согласитесь, то я продам номера кредитных карт ваших клиентов и расскажу про это всем журналистам».

Компания не выполнила требования компьютерного вымогателя и обратилась с официальным заявлением в ФБР. После этого кардер сдержал свое слово. Через Интернет он поведал эту историю корреспондентам газеты «Нью-Йорк таймс» и обнародовал на специально созданном им сайте под названием «Максус кредит кард пайплайн» реквизиты 25 тыс. пластиковых кредитных карт и персональные данные их держателей. По словам «Максима», он специализируется на электронных «кражах» номеров кредитных карт в Интернете уже два года; открыл также с помощью Интернета оффшорный счет, куда переводит похищенные суммы с чужих кредитных карт (с их СКС) и с помощью которых расплачивается за свои реальные покупки, предоставляемые ему услуги, а также снимает деньги наличными через уличные банкоматы; кроме того, он неоднократно продавал эту конфиденциальную информацию другим пользователям Интернет в процессе виртуального общения, в том числе – «на тусовках хакеров».

Специалисты ФБР и компании «Секьюрити Фокус», специализирующейся на защите компьютерной информации в сети Интернет, отметили чрезвычайно высокий профессиональный уровень преступника – помимо вышеуказанных инструментов взлома для вскрытия базы данных интернет-магазина им также были применены специальные методы, известные только сотрудникам соответствующих спецслужб. Мало того, полностью уничтожить созданный преступником сайт удалось лишь спустя две недели после появле-

ния в ней конфиденциальной информации, когда она была уже скопирована несколькими тысячами пользователями сети Интернет. В ходе начавшегося расследования транснационального преступления агентам ФБР удалось лишь установить, что свои сообщения вымогатель посылал из региона Восточной Европы, используя при этом российский IP-адрес. Местонахождение и личность преступника не были установлены, поскольку он искусно скрыл все следы своего пребывания в интернет-магазине и на созданном информационном сайте[213].

О распространенности рассматриваемого способа в криминальной практике свидетельствуют следующие данные. Только в 2000 г. более 40 американских интернет-магазинов подверглись дистанционному нападению со стороны профильных организованных преступных групп, действующих с территории России и Украины. В общей сумме преступникам удалось завладеть более 3,7 млн конфиденциальных электронных реквизитов платежно-расчетных пластиковых карт и персональными данными их держателей. Согласно официальному заявлению представителя ФБР США речь идет о самых масштабных преступных посягательствах, когда-либо совершенных в отношении американских торговых предприятий. Следует добавить, что преступники были установлены и задержаны только один раз: в марте того же года сотрудниками спецслужбы Великобритании арестованы и предаены суду двое подростков, совершивших хищение 26 тыс. записей из клиентской базы данных одного электронного магазина в городе Уэльсе[214].

«Троянский конь» – специальная программа для ЭВМ, предназначенная для негласного получения (сбора, копирования) и передачи ее создателю конфиденциальной компьютерной информации. Чтобы программа начала выполнять заложенный в нее вредоносный алгоритм, она обязательно должна быть запущена в программной среде компьютера потерпевшего. Для этого мошенниками применяются различные тактические уловки. Чаще всего «троянский конь» маскируется под различные информационные продукты, рассылаемые по электронной почте пользователям сети Интернет.

Анализ материалов конкретных уголовных дел позволяет выделить следующие методики обмана потерпевших и принуждения их к запуску рассматриваемого средства совершения преступления на своем компьютере.

---

[213] См.: Ай да Максим из России! // Труд. – 2000. – № 5. – С. 24.
[214] Подробнее см.: *Голдовский И.* Указ. соч. – С. 68.

1. Потерпевший по электронной почте получает письмо с объяснениями в любви от незнакомого адресата. К письму имеется приложение, содержащее точный адрес или фотографию незнакомца (незнакомки). При его открытии автоматически запускается программа «троянского коня». Она негласно перлюстрирует все файлы, содержащиеся в памяти ПЭВМ, отбирая из них конфиденциальные реквизиты платежно-расчетных карт и персональные данные об их держателях, либо перехватывает их в случае ввода с клавиатуры при совершении платежно-расчетной операции. Затем вредоносная программа из незаконно полученной информации формирует сообщение и отсылает его по электронному адресу, указанному в ее алгоритме. После чего она копирует себя и рассылает копии по обнаруженным в памяти ПЭВМ электронным адресам других жертв. При этом оригинал «троянского коня» самоуничтожается, а его копии продолжают описанный цикл на других компьютерах пользователей сети Интернет.

2. В некоторых случаях «троянский конь» маскируется под картинку или фотографию порнографического содержания. При ее открытии – просмотре пользователем на экране ПЭВМ – вредоносная программа автоматически запускается и негласно выполняет вышеуказанные действия. В качестве примера приведем текст электронного письма эротического содержания с приложением в виде порнографической картинки, под которой скрывается программа «троянского коня».

«Привет. Твои деньги мне передали, все в порядке. Поэтому шлю тебе архив с фотками моих девочек, выбери одну из них и я тебе полностью пришлю ее резюме, а также еще более откровенные фото. Твой логин и пароль для входа *vladcher/pw572vc4.* Надеюсь все будет как в прошлый раз.

Введи этот *proxy* (пароль), без него из России никак не зайти к нам (это защита от русских, которые не могут оплачивать наши услуги по кредиткам).

proxy.mcgarem.ru 8080 (расшифровывается как «мисс гарем»).

Всегда к твоим услугам, Кристина»[215].

3. Иногда рассматриваемое средство подготовки преступления приходит к потерпевшему в виде письма от брачного агентства знакомств, рекламы какого-либо товара (услуги), а также под видом бесплатного обновления антивирусной или иной пользовательской программы для ЭВМ.

4. Анализ содержания хакерских сайтов в Интернет показывает, что через них очень часто открыто распространяются «троянские

---

[215] *Казеннов В.Н.* Защита от троянских коней в Windows 9X // Защита информации. Конфидент. – 2000. – № 6. – С. 13.

кони», имеющие различные вредоносные алгоритмы воздействия на программное обеспечение пользователей. При этом открыто объявляется один алгоритм работы программы, а реально (негласно) исполняется другой. Этот прием рассчитан на «лохов» – молодых и неопытных пользователей сети Интернет, которым психологически хочется почувствовать себя «крутыми хакерами». В итоге они сами становятся потерпевшими от того оружия, которое хотели применить против других. Образно говоря, «программная бомба», которую они хотели «забросить» в чужой компьютер, «взрывается» в их собственном, причиняя в дальнейшем значительный материальный ущерб им и их родителям, использующим данную ПЭВМ в качестве электронного терминала для проведения расчетов по пластиковым картам[216].

Сайты-ловушки. Иногда для незаконного захвата (получения) конфиденциальных реквизитов пластиковых карт и их держателей используются специальные программы для ЭВМ, замаскированные под различные сайты сети Интернет. На таком сайте пользователю безвозмездно или за незначительную плату предлагаются различные товары или информационные услуги, для получения которых необходимо зарегистрироваться в клиентской базе данных, указав при этом исчерпывающую информацию о себе и реквизитах своей карты. Чаще всего в целях маскировки преступниками используются сайты следующего содержания: порнографические; содержащие информацию о местах сбыта наркотических средств; имитирующие работу международных брачных агентств; фиктивные торговые предприятия «товары – почтой» или магазины «горящих» туристических путевок. Естественно, после того как клиент оставил свои реквизиты, он не получает заявленного на сайте товара или услуги. В некоторых случаях отказ предоставляется под самым благовидным и естественным предлогом, что не вызывает никаких подозрений у клиента.

4. Негласное внесение изменений в программы, обеспечивающие проведение расчетных операций с использованием пластиковых карт.

Летом 1999 г. в суде города Березняки Пермской области слушалось дело по обвинению бывшего работника отделения АКБ «Сбербанк России» Ч-на и его сообщника безработного Ч-го в хищении 1,5 млрд неденоминированных рублей, принадлежащих названному банку. Суть дела такова.

---

[216] Много информации о таких случаях можно найти на сайте кардеров по адресу http: // www.geocities.com/Silicon Valley/Park/8783/.

Ч-н с лета 1996 г. работал у потерпевшего на должности старшего инженера с функциями администратора безопасности расчетов по пластиковым картам платежной системы «Сберкарт». Имея полный и практически бесконтрольный со стороны администрации и службы безопасности банка доступ к программному обеспечению этой системы, он несанкционированно модифицировал его. Помимо этого, им была разработана и установлена в память управляющей ЭВМ специальная программа, позволяющая делать так называемые безадресные зачисления денежных средств. Запуск программы осуществлялся дистанционно по сети ЭВМ с применением специального пароля доступа. Таким образом, имея ПЭВМ, оборудованную модемом, и являясь абонентом городской телефонной проводной электросвязи либо сотовой радиосвязи, можно было активировать эту программу. После запуска она негласно в автоматическом режиме вносила изменения в таблицу остатков на двух специальных карточных счетах, указанных преступником. СКС были открыты сообщниками Ч-на по похищенному паспорту в разных березняковских отделениях Сбербанка России.

Летом 1997 г. Ч-н неожиданно уволился, заблокировав перед этим пароль доступа к тем областям памяти ЭВМ Сбербанка, где могли быть обнаружены внесенные им в программное обеспечение изменения и внедренная в систему вредоносная программа для ЭВМ.

Реализовать преступный замысел преступникам удалось с квартирного телефона общего знакомого Т., которому было обещано вознаграждение в сумме 5 млн рублей. С помощью вышеуказанных орудий хищения Ч-н дистанционно зачислил на открытые счета 2 млрд рублей, которые его сообщники И. и А. стали обналичивать через банкоматы, установленные в Перми, Санкт-Петербурге и Москве.

По заявлению потерпевшего – представителя березняковского филиала Сбербанка России Пермской области было возбуждено уголовное дело. В ходе расследования был установлен телефонный номер, которым пользовались мошенники для незаконного зачисления денежных средств. При допросе его владельца Т. следствию удалось получить информацию, способствовавшую задержанию Ч-на и Ч-го. При обыске в местах их проживания была обнаружена лишь часть похищенных денег в сумме 45 млн рублей. После допроса подозреваемых стало известно, что остальные деньги находятся у их сообщников И. и А., которые сумели скрыться от следствия и суда.

В итоге Ч-н получил наказание в виде 7 лет лишения свободы с конфискацией имущества, а Ч-й – 6,5 лет.

Следы преступления можно обнаружить:

1) в ходе проведения специальной проверки (ревизии) программного обеспечения ЭВМ, управляющей расчетами по конкретным СКС;

2) в выписке по СКС, содержащей подробную историю приходных и расходных операций;

3) в первичных учетно-расчетных документах, оформленных банкоматами при проведении операций по интересующим СКС;

4) при осмотре фото- и видеодокументов, созданных автоматизированными охранными системами конкретных банкоматов по исследуемым операциям;

5) в электронных журналах средств автоматической фиксации соединений управляющей ЭВМ (сервера сети) с удаленными терминалами по телефонным каналам электросвязи (средств защиты портов от внешнего несанкционированного доступа к конфиденциальной компьютерной информации);

6) в справке от оператора электросвязи или провайдера услуг сети Интернет (в случае использования IP-телефонии) о принадлежности установленного номера конкретному лицу (абоненту) и местонахождении оконечного устройства (месте установки соответствующего терминала – телефонного аппарата или ПЭВМ);

7) в комплекте документов на открытие СКС и получение платежно-расчетных пластиковых карт по нему;

8) в заявлении лица об утрате паспорта, по реквизитам которого был открыт СКС.

5. Создание и использование лжепредприятий торговли и сферы услуг (фирм-«однодневок»). Этот способ совершения преступления достаточно хорошо известен следственной практике. Заключается он в том, что членами организованной преступной группы, специализирующейся на совершении преступлений выделенной категории, легально регистрируется магазин (предприятие сферы услуг), который на договорной основе входит на правах мерчанта в платежную систему. Основная цель создания этого лжепредприятия – хищение денежных средств путем внедрения в платежную систему первичных расчетных документов, составленных с использованием незаконно полученных конфиденциальных реквизитов пластиковых карт и их держателей. В зависимости от количества реквизитов чужих карт, имеющихся в распоряжении преступников, выделяется две разновидности рассматриваемого способа.

5.1. Фиктивный интернет-магазин. Организуется при наличии нескольких десятков реквизитов. Данное предприятие, как правило,

регистрируется на подставное лицо или по похищенным документам и располагается в обычной телефонизированной квартире, которая арендуется с правом распоряжения ее адресом в коммерческих целях. Комнаты маскируются под офисные помещения. После получения необходимого комплекта регистрационных документов и постановки на учет в налоговой инспекции начинается активная фаза совершения хищения. В этих целях выполняется следующий комплекс мероприятий:

1) с провайдером услуг Интернета заключается договор о разработке и обслуживании коммерческого сайта в виде электронного магазина, «торгующего» программным обеспечением или другим информационным продуктом (программами телевизионных передач, подпиской на новости и т. д.), называемым на криминальном жаргоне «воздухом»;

2) в комнате с телефоном устанавливается электронный терминал – ПЭВМ с принтером, модемом и соответствующим программным обеспечением;

3) с банком-эквайрером или эмитентом заключается договор на вступление в платежную систему и проведение операций по пластиковым картам, открываются соответствующие расчетные счета;

4) с эквайрером заключается договор на проведение инкассации расчетных документов, оформленных с использованием пластиковых карт и их реквизитов;

5) арендуется или покупается специальное оборудование и программное обеспечение для составления первичных расчетных документов с использованием реквизитов пластиковых карт.

Стратегия использования данного способа заключается в выполнении максимально возможного числа транзакций на крупные суммы (по несколько тысяч долларов США каждая) с оформлением соответствующих фиктивных документов. В действительности такое предприятие реально ничем не торгует и никаких услуг не оказывает. При этом в обслуживающий банк регулярно направляются авторизационные запросы на проведение операций с использованием пластиковых карт и на инкассацию выставляются соответствующие комплекты документов, на основании которых на счет магазина зачисляются соответствующие денежные суммы. Создается так называемый «информационный шум деятельности» для поддержания маскировки. Виртуальный лжемагазин функционирует до первого возврата эквайрером первичных документов (отказа по их оплате) либо появления в присланном «Стоп-листе» номера карты, использованного мошенниками для оформления расчетных доку-

ментов. Таким образом, фиктивный интернет-магазин функционирует всего несколько недель, после чего исчезает.

5.2. Создание лжепредприятия. Совершение преступления с его помощью может быть реализовано только при наличии у мошенников обширной базы данных, содержащей несколько десятков тысяч реквизитов карт и их держателей. Как правило, она постоянно пополняется новыми сведениями за счет реально производимых расчетных операций и хорошо налаженного канала получения конфиденциальных реквизитов. Для этих целей в преступной группе выделяются специальные лица, отвечающие за данный участок «работы». Их задача состоит в добыче любыми путями реквизитов действующих платежно-расчетных карт.

На первый взгляд, это обычное реально функционирующее предприятие торговли или сферы услуг, которое может иметь свой интернет-магазин и агрессивную рекламу с целью привлечения большого числа клиентов – держателей карт. В некоторых случаях им даже выдают дисконтные карты, малоценные призы, делают большие скидки на товары (услуги) или устанавливают на них очень низкие заведомо убыточные цены.

При реализации данного способа преступники действуют крайне осторожно. Их преступная деятельность рассчитана на длительный срок. Для этого мошенниками избирается тактика «пощипывания счетов», состоящая в совершении криминальных транзакций на незначительные суммы – в размере от 10 до 50 долларов, которые чередуются с действительными, законно совершенными. За счет этого преступники долго остаются незамеченными. Так продолжается до тех пор, пока уровень chargeback (отказов от платежей) карт, реквизиты которых незаконно использовались, не станет критическим, что будет свидетельствовать о факте мошенничества со стороны сотрудников конкретного мерчанта.

Анализ следственной практики показывает, что срок криминальной деятельности таких лжепредприятий составляет от 3 до 7 месяцев. За это время преступникам удается похитить несколько сотен тысяч долларов. Наглядной иллюстрацией этому служит уголовное дело, расследованное следственной частью Следственного комитета при МВД России[217].

Как следует из материалов уголовного дела, в декабре 1999 г. в г. Москве Л., М. и Ж. зарегистрировали торговое предприятие и на

[217] Использовано извлечение из материалов обобщения практики расследования уголовных дел о мошенничествах, совершенных с использованием сети Интернет, подготовленных Следственным комитетом при МВД России в 2002 г.

договорной основе открыли в сети Интернет электронный магазин «Политшоп» по оформлению платной подписки на Дайджест политических новостей стоимостью от 53 до 127 долларов (в зависимости от срока подписки). Далее Л. – частный предприниматель и владелец магазина заключил договор с коммерческим банком (КБ) «П-на» о расчетном обслуживании этого магазина и держателей банковских карт платежной системы «Киберплат».

Следствием было установлено, что Л., М. и Ж. при создании магазина не намеревались заниматься законной предпринимательской деятельностью, так как они преследовали цель хищения денежных средств, поступающих в КБ «П-на» на расчетный счет магазина «Политшоп» от фиктивных расчетно-кассовых операций, оформленных с использованием реквизитов чужих пластиковых карт и их держателей. Осуществляя свои преступные намерения, указанные лица привлекли к деятельности созданной ими организованной преступной группы студентов различных московских вузов К., П., Ш., Д. и Б. В их обязанности входило с помощью персональных ЭВМ через сеть Интернет подключаться к сайту электронного магазина «Политшоп» и вводить реквизиты чужих пластиковых карт Международных платежных систем «Виза» и «Еврокарт/МастерКарт» – совершать фиктивные покупки (подписки на Дайджест) от имени ничего не подозревающих их держателей.

Договорившись между собой о распределении преступных ролей, Л., М. и Ж. осуществляли руководство участниками ОПГ. Так, Л., являясь владельцем зарегистрированного торгового предприятия, выполнял «представительские» функции. Он регулярно встречался с сотрудниками КБ «П-на» и вводил их в заблуждение, убеждая в законности проводимых расчетно-кассовых операций через свой электронный магазин. М. обеспечивал безопасность деятельности участников ОПГ, а также совместно с Л. обналичивал и распределял похищенные деньги между соучастниками. В свою очередь Ж. покупал у неустановленного следствием лица реквизиты чужих банковских карт и их держателей, а затем передавал их К., П., Ш., Д. и Б. для совершения незаконных операций.

В январе 2000 г. Л. и М., обеспокоенные возникшими у руководства КБ «П-на» подозрениями в правомерности совершаемых магазином «Политшоп» сделок, ввели в состав ОПГ гражданина Грузии Б-ю, обладавшего обширными связями в кредитно-банковской сфере. Он обещал Л. и М. уладить возникшие «неприятности». Выполняя принятые на себя обязательства, Б-я неоднократно встречался с представителями данного банка и сумел убедить их в законности операций, осуществляемых через электронный магазин

«Политшоп». При этом Б-я от имени Московского КБ «Зам-й» высказывал ложные обещания о гарантиях возврата денежных средств, зачисленных на счета названного торгового предприятия, в случаях отказа держателей карт от «покупок» («предоставленных им услуг»).

Не удовлетворившись своей ролью в деятельности ОПГ, Б-я в марте 2000 г. добился от Л. и М. заключения нового договора с КБ «П-на», согласно которому денежные средства, накапливаемые от криминальных операций на транзитном счете лжемагазина «Политшоп», переводились не на расчетный счет Л. в ОАО КБ «А.-банк», а в КБ «Зам-й» на счет контролируемого им ООО «Г.-Техно». Тем самым Б-я получил возможность контролировать и самостоятельно распределять между членами ОПГ похищенные деньги, заняв главенствующее положение среди ее участников.

Всего за период с декабря 1999 г. по апрель 2000 г. преступниками были использованы незаконно добытые реквизиты свыше 7 тыс. банковских карт и их держателей, с помощью которых через электронный лжемагазин похищено свыше 23 млн рублей.

Следствием было также установлено, что создавая лжемагазин, преступники изначально рассчитывали на невнимательность держателей банковских карт. Обычно они являются состоятельными людьми и не обращают внимания на списание с их счетов столь незначительной суммы (от 50 до 127 долларов), которая находится среди множества других платежей, осуществленных за месяц (в биллинговой распечатке).

Следы рассмотренных способов совершения хищения следует искать в следующих документах:

1) комплекте регистрационных документов;

2) юридическом деле предприятия в налоговой инспекции;

3) договорах на вступление в платежную систему, открытие расчетных счетов, инкассовое обслуживание;

4) выписке из счетов предприятия по расчетно-кассовым безналичным операциям, осуществленным с использованием реквизитов пластиковых карт; аналитической справке о соотношениях наличных и безналичных доходов мерчанта по кассовым операциям;

5) справках эмитента по возвратным chargeback-операциям, в которых фигурируют реквизиты конкретного мерчанта;

6) справках из процессинговых центров платежных систем о держателях карт, реквизиты которых использовались по возвратным операциям;

7) запросах на имя держателей карт по операциям, совершенным от их имени в конкретном мерчанте на территории России;

8) заявлениях держателей об отказе оплаты операции, произведенной у интересующего следствие мерчанта;

9) первичных расчетно-кассовых документах (слипах, контрольных лентах, электронных расходных реестрах и др.);

10) материалах ревизий и документальных проверок;

11) документах, содержащихся в памяти электронного терминала;

12) заявлениях об утрате паспортов, реквизиты которых фигурируют в регистрационных и иных документах лжемагазина;

13) справке от оператора электросвязи и провайдера услуг Интернет о реквизитах абонентов, соединения с которыми производились в момент совершения всех возвратных операций.

3.3. Использование поддельных карт

С уголовно-правовой точки зрения сам факт изготовления или сбыта поддельных кредитных либо расчетных карт как ценных бумаг и платежных документов является преступлением (соответственно ст. 186 и 187 УК РФ). При этом следует иметь в виду, что их последующее использование в качестве орудия совершения хищения требует дополнительной квалификации. С криминалистических позиций это наиболее часто встречающиеся способы. В случае их применения перед преступником всегда встают следующие основные задачи:

1) получение идентификационных реквизитов подлинных карт и их держателей;

2) определение способа подделки карты, приискание соответствующих орудий и материалов;

3) собственно подделка карты;

4) выбор места совершения хищения – зависит от вида поддельной карты, способа подделки и возможности обеспечения безопасности авторизации ее реквизитов в момент совершения преступного посягательства;

5) получение и использование похищенного имущества.

Очевидная сложность решения этих задач, а также достаточная трудоемкость и финансовая затратность процедуры качественного изготовления поддельной карты обусловливают совершение таких преступлений преимущественно организованными группами с четким разделением ролей, которые соответствуют выделенным позициям. С учетом изложенного, а также принимая во внимание данные, полученные путем анализа различных эмпирических ис-

точников, возможно предложить следующую классификацию рассматриваемых способов преступления.

1. Незаконная персонификация стандартных заготовок или базовых стоков карт на промышленном либо полупромышленном оборудовании является наиболее опасным и трудно выявляемым способом. Он состоит в том, что преступник из числа сотрудников эмитента или организации, осуществляющей техническое обслуживание персонификационного оборудования либо поставку расходных материалов к нему, различными методами добывает заготовки (базовые стоки) карт, которые передает своим сообщникам. Иногда вместе с ними он также предоставляет в распоряжение членов ОПГ конфиденциальную информацию о реквизитах подлинных карт и их держателях. Данные реквизиты достаются преступниками и иными способами, в том числе и теми, которые были рассмотрены ранее.

Как отмечают некоторые исследователи, нередко сотрудники эмитента вступают в преступный сговор с работниками, имеющими доступ к персонификационному оборудованию, либо за взятку получают несанкционированный доступ и сами изготавливают поддельные карты[218].

Исходя из содержания и персональной принадлежности подделываемых реквизитов, наносимых на заготовку (базовый сток), можно выделить две разновидности рассматриваемого способа.

1.1. Использование реквизитов действительных пластиковых карт и их держателей. В этом случае на промышленном или полупромышленном персонификаторе преступниками незаконно изготавливаются дубликаты (неучтенные копии) карт, выдаваемых клиентам, либо создаются карты с реквизитами, которые комбинируются с нескольких реально существующих карт. Например, 13 октября 2000 г. в момент совершения хищения в одном из магазинов гостиницы «Рэдиссон – Славянская» в г. Москве были задержаны нигде не работающие ранее не судимые граждане России Ш. 1965 года рождения (г.р.) и Б. 1969 г.р., оба имеющие высшее образование. При личном обыске у них были обнаружены и изъяты поддельные карты Международных платежных систем «Виза» и «Еврокарт/МастерКарт», с помощью которых они пытались оформить расчетно-кассовые операции по оплате покупаемых товаров на крупную сумму в долларах США. При осмотре автомашины,

---

[218] См.: *Астапкина С.М.* Защита интересов банков и вкладчиков от преступного использования пластиковых платежных средств // Криминальные расчеты: уголовно-правовая охрана инвестиций. – М., 1995. – С. 72.

принадлежащей Ш. и припаркованной недалеко от места происшествия, членами следственно-оперативной группы (СОГ) ГУВД г. Москвы были обнаружены предметы другого хищения: телевизоры и иная дорогостоящая бытовая техника.

При допросе задержанных было установлено, что в 1999 г., когда Ш. и Б. искали себе работу, на одном из хакерских сайтов Интернет они обнаружили объявление о продаже базы данных, содержащей реквизиты чужих платежно-расчетных карт и их держателей, а также персонификационного оборудования и материалов для подделки карт. За 3 тыс. долларов США указанные орудия преступления были приобретены ими у неизвестного лица. Реализуя свои корыстные планы, Ш. и Б. наладили кустарное производство поддельных пластиковых карт и стали совершать с их помощью хищения имущества. По инициативе Ш. в целях безопасности и расширения преступной деятельности в группу был введен ранее не судимый безработный гражданин Украины Л. 1961 г.р., также имеющий высшее образование. На него возлагались обязанности по хищению товаров из магазинов автозаправочных станций компании «Бритиш Петролеум», расположенных в том же городе. Для этого Л. снабжался поддельными пластиковыми картами, которые изготавливали Ш. и Б. Затем в организованную преступную группу был привлечен знакомый Л. – ранее не судимый безработный гражданин Украины Б-о 1955 г.р., имеющий высшее образование. Его роль заключалась в совершении с применением поддельных пластиковых карт хищений наличных денежных средств из банкоматов. При изготовлении этих орудий преступлений мошенниками был использован способ «белый пластик» («чистая пластиковая карта»), который будет рассмотрен далее по тексту работы.

По показаниям подозреваемых Ш. и Б. с поличным были задержаны их подельники Л. и Б-о.

При проведении технико-криминалистической экспертизы пластиковых карт, изъятых у мошенников, экспертами был отмечен высокий технический уровень их подделки.

Примечателен тот факт, что членами этой ОПГ с использованием поддельных пластиковых карт было совершено около 10000 хищений на сумму несколько миллионов долларов США.

С научной точки зрения интерес представляет то обстоятельство, что ранее в 1995 г. аналогичным способом в г. Москве совершались хищения наличных денежных средств из обменных пунктов некоторых коммерческих банков. Эти хищения были организованы и осуществлены членами специализированной преступной группы, насчитывавшей в своем составе 14 человек. Все они были ранее

не судимы, имели высшее образование и являлись безработными. «На работу» они «нанимались» через соответствующие объявления газеты «Из рук в руки». Общий ущерб тогда составил 550 тыс. долларов США.

По данным Международной уголовной полиции Интерпол, указанным способом в Венгрии из банкоматов, расположенных в различных районах города Будапешта, членами организованной преступной группы в количестве 150 человек одновременно в течение нескольких минут было осуществлено хищение 1,5 млн форинтов. В ходе криминальной операции преступниками использовались 1,5 тыс. заранее подготовленных поддельных пластиковых карт[219].

Основные вещественные доказательства: поддельные пластиковые карты; первичные расчетные документы, которые были составлены с их использованием; похищенное имущество; фото- и видеодокументы из автоматизированных систем охраны терминалов, зафиксировавших факт проведения криминальной операции; оборудование и материалы, использованные для подделки (незаконного изготовления) пластиковых карт.

1.2. Использование реквизитов несуществующих (фантомных) пластиковых карт. Данный способ основан на использовании преступниками «генератора паролей» (вредоносной программы для ЭВМ). Зная номер действительной карты, они вычисляют из него ПИН-код либо генерируют полную идентификационную пару реквизитов: ПИН-код и соответствующий ему номер карты. Эти программы приобретаются преступниками через объявления об их продаже, размещаемые на «электронных досках», либо приискиваются на хакерских сайтах в сети Интернет. Полученный номер наносится на заготовку методом эмбоссирования или идент-печати и записывается в память карты. Таким образом, появляется фантомная пластиковая карта, полностью отвечающая всем техническим и идентификационным требованиям подлинной, с той лишь разницей, что ее номер и ПИН-код не зарегистрированы ни одним эмитентом. Совершить преступление с помощью такой поддельной карты возможно лишь через электронные терминалы, работающие в режиме «off line», когда операции авторизации и финансовых транзакций совершаются непосредственно в электронном терминале без связи с процессинговым центром[220].

---

[219] Подробнее см.: Организованная преступность и частные инвестиции: Учеб. пособие / Под ред. В.И. Попова, А.С. Овчинского. – М., 1998. – С. 335.

[220] См.: Там же. – С. 364-365.

2. Термопеределка. В зарубежной юридической практике способ называется «работа утюгом». По мнению ряда исследователей, он получил свое широкое распространение уже с начала 80-х годов прошлого века[221]. В криминальной практике встречаются две его разновидности.

2.1. Термоперенос магнитных меток. Известно, что нагрев магнитного материала понижает его коэрцитивность – делает его магнитомягким. Следовательно, пока магнитный машинный носитель находится в разогретом состоянии, то достаточно сравнительно небольшого внешнего электромагнитного или магнитного воздействия, чтобы записать на него то или иное сообщение. Одновременно с этим при повышении температуры возрастает напряженность магнитных полей, создаваемых магнитными метками, с помощью которых информация записана на соответствующий машинный носитель. Данными физическими свойствами пользуются преступники для получения незаконной копии реквизитов, содержащихся на магнитной полосе карты. Для этих целей ими используется действительная карта с магнитной полосой (оригинал) и заготовка, на магнитной полосе которой не содержится никакая информация (будущая копия). Карты накладываются лицевыми сторонами друг на друга так, чтобы их магнитные полосы совпали. Затем через обычный лист бумаги они проглаживаются горячим утюгом. В итоге на пустой магнитной полосе остается отпечаток магнитных меток, с помощью которых закодировано сообщение на оригинале. После остывания карты сохраняют свои свойства: оригинал – имевшиеся до нагрева; копия – приобретенные во время нагрева.

Анализ отечественной и зарубежной следственной практики показывает, что заготовка приискивается тремя следующими основными способами:

1) преступники собирают использованные (размагниченные) карты, изготовленные на заводском оборудовании эмитента, например, телефонные и проездные карты с фиксированной покупательной способностью, массово выбрасываемые в урны на станциях метро;

2) заготовки изготавливают кустарным способом из подручных бытовых материалов. Так, при помощи ножниц по стандартным размерам из тонкого картона или пластика вырезается подложка карты, а из магнитной ленты разобранных видео- или аудиокассет – ее маг-

[221] Например, см.: *Астапкина С.М.* Указ. соч. – С. 77.

нитная полоса. Полоса наклеивается на подложку клеем ПВА[222]. Для копирования графического изображения с подложки карты-оригинала на заготовку преступники используют современные компьютерные технологии, которые были подробно рассмотрены ранее при описании способов подделки слипов.

В некоторых случаях мошенники не утруждают себя воссозданием каких-либо графических, текстовых и иных реквизитов – ими подделываются только подложка и машинный носитель карты (магнитная полоса, микросхема, штрих-код и т. д.). Такой способ в международной юридической практике получил название «белый пластик» или «чистая карта»;

3) заготовки вырезают из использованных карт, имеющих нестандартные размеры подложки и магнитной полосы, например, проездных билетов французской железной дороги или российского Аэрофлота[223].

2.2. Термопеределка эмбоссированных реквизитов подлинной карты. Способ основан на полиморфических особенностях пластика принимать под воздействием тепла исходно гладкую поверхность, существовавшую до заводского эмбоссирования реквизитов, а после остывания – сохранять новые, нанесенные преступником. Алгоритм подделки складывается из следующих этапов:

1) перед тепловой обработкой карты с эмбоссированных реквизитов химическим или механическим путем удаляется (соскабливается) краситель. Данные действия осуществляются преступником для того, чтобы во время разогрева пластика частицы краски не попали в структуру подложки. В противном случае визуально будут просматриваться контуры и фрагменты исходных (переделанных) реквизитов;

2) участки подложки, содержащие эмбоссированные реквизиты, нагревают с помощью различных бытовых приборов и инструментов: утюга, паяльника, горелки, зажигалки, тостера, ростера и др.;

3) после получения свойств текучести пластика поверхность карты механически выравнивают (прессуют), стирая исходные выпуклые реквизиты. Для этого применяют слесарные тиски, прессы, струбцины, металлические пластины от фотоглянцевателей, молотки и другие орудия;

4) до момента частичного или полного остывания пластика на его поверхность наносят новые реквизиты. Буквы и цифры выдав-

---

[222] Подробнее см.: *Леонтьев Б.К.* Фрикинг без секретов. – М., 2001. – С. 82-84.

[223] Подробнее см.: *Гелль П.* Магнитные карты и ПК / Пер. с фр. – М., 2001. – С. 109-111.

ливаются из мягкого пластика с помощью различных бытовых и слесарных инструментов, например, металлическими: вязальной спицей, отверткой, гвоздем, пишущей головкой шариковой авторучки, проволокой, заколками для волос («невидимками»). В случае массовой подделки могут также использоваться специально изготовленные металлические печатные формы – печати и литеры от механических печатных машинок либо промышленные (полупромышленные) эмбоссеры;

5) после остывания полученные выпуклые поверхности окрашиваются с использованием разнообразных лакокрасочных материалов (например, лака для ногтей), инструментов и приспособлений (кисточкой от руки, по трафарету, краскопультом, баллончиком с краской и т.д.);

6) поврежденные голографические защитные знаки, метки и эмблемы, заламинированные в подложку карты, как правило, закрываются мошенниками поверхностными наклейками соответствующего вида и содержания.

Типичными следами термопеределки эмбоссированных реквизитов карты являются:

1) *следы термического воздействия* – волнообразные наплывы пластика на поверхности подложки, неровные края подложки, непостоянная толщина подложки, изменение цветовой гаммы подложки и нанесенного на нее изображения в местах теплового воздействия, частичная или полная деформация подложки, а также сквозные отверстия, проплавленные в подложке;

2) *следы первоначальных (измененных) реквизитов* – слабовыраженные рельефные контуры цифр и букв, вплавленных в подложку; наличие вне контуров эмбоссированных знаков точек – «марашек» и отдельных штрихов красителя;

3) *следы орудий и инструментов подделки* – расположение эмбоссированных реквизитов выше или ниже места их стандартной печати, наличие вмятин на выпуклых реквизитах или подложке, непостоянная базовая глубина вдавливания знаков в подложку с оборотной стороны, непостоянный рельеф знаков на лицевой стороне, смещение отдельных букв и цифр относительно строки их написания, различный угол наклона знаков, нестандартный тип шрифта, различные размеры одноименных букв и цифр, неравные интервалы между одноименными знаками, разный цвет красителя в штрихах.

3. Подделка конфиденциальных электронных реквизитов и их машинных носителей. Подделку карты данным способом может осуществить лишь тот, кто владеет знаниями в области ра-

диотехники и компьютерных технологий. При этом перепрограммирование конфиденциальных данных, содержащихся в интегральной микросхеме памяти карты, намного сложнее, чем запись электронных реквизитов на магнитную полосу. За рубежом данным способом могут воспользоваться только отдельные, хорошо законспирированные субъекты, входящие в состав специализированных организованных преступных групп и сообществ. Напротив, в нашей стране, как показывает анализ следственной и судебной практики, этот способ широко распространен в среде молодых людей, как правило студентов, в возрасте от 18 до 28 лет. Так, некоторые студенты московских вузов «зарабатывают себе на жизнь» тем, что продают поддельные обезличенные платежно-расчетные карты с фиксированной покупательной способностью – таксофонные карты и проездные билеты на метро. В качестве исходного материала – заготовки, как правило, выступают использованные и выброшенные за ненадобностью недействительные карты. Они имеют все необходимые стандартные реквизиты за исключением одного – электронных данных, стертых считывателями терминалов во время применения карт по назначению. Вместе с этим могут использоваться и заготовки, полученные иными способами. При помощи легально приобретенных орудий – специальной литературы, персонального компьютера, соответствующего программного обеспечения, полученного из Интернет, периферийного оборудования и стандартных комплектующих мошенники конструируют специальные технические устройства, позволяющие перепрограммировать микропроцессоры и восстанавливать стертую компьютерную информацию на магнитных полосах карт соответствующих видов[224]. Например, в сети Фидонет можно встретить информационные сообщения следующего содержания:

Алексей А. Новожилов (Alexey A. Novojilov), адрес в сети ФИДО – 2:5020/118.11 и 2:5020/4000.

*Телефон, на котором установлена почтовая станция ФИДО: 939-2231.

E-mail: alexn@chem.msu.ru. Пейджер: (095) 232-0000 аб. 11223.*

Объявление о продаже

«Продаю хакнутые телефонные карточки, хакнутые карточки для метро и оборудование для их подделки».

В зависимости от вида машинного носителя и формата электронных реквизитов выделяются следующие разновидности рассматриваемого способа преступления.

---

[224] См.: *Милкус А., Мызалин В.* Если денег дома нет – потрясите Интернет // Комсомольская правда. – 1998.– 18 дек. – С. 18.

3.1. Незаконное электромагнитное копирование конфиденциальных электронных реквизитов карт с магнитной полосой. В качестве оригинала (модели), с которого производится создание незаконных копий конфиденциальных электронных реквизитов (поддельных карт), используется действительная платежно-расчетная карта с магнитной полосой, приобретаемая обычным порядком в торговых точках эмитента. Для электромагнитного перекопирования информации с магнитной полосы действительной карты на полосу недействительной (использованной – «чистой») карты преступниками применяются специальные технические устройства кустарного и заводского изготовления. Схемы и методики их изготовления и применения можно найти в открытой литературе[225].

С помощью рассмотренного способа преступникам удается за короткий промежуток времени изготавливать значительное количество поддельных карт. Например, в октябре 2000 г. в ходе проведения оперативно-разыскных мероприятий на одном из железнодорожных вокзалов г. Москвы был задержан 28-летний безработный житель Воронежа К., имеющий высшее образование по специальности «учитель истории». При досмотре его кожаной сумки был обнаружен целлофановый пакетик с героином, а также несколько сотен поддельных платежно-расчетных карт – билетов и абонементов на проезд в московском метрополитене. В ходе расследования уголовного дела было установлено следующее.

На одном из сайтов сети Интернет К. прочитал сообщение о том, что никому еще не удалось подделать электронные реквизиты карт для проезда в московском метро, которые австралийская фирма защитила от подделки специальным скрытым некопируемым кодом. К. позволил себе усомниться в надежности этой защиты. Он приобрел в кассах метрополитена несколько действительных карт различного достоинства (на одну, две и т. д. поездок) и подобрал из мусорных баков соответствующие им использованные (недействительные) карты. С помощью ПЭВМ, ридера и программного обеспечения к нему, приобретенных на Митинском радиорынке (в Москве), К. произвел исследование данных, содержащихся на магнитных полосах. Через месяц им был программно выделен защитный код и разработан алгоритм по его копированию. После нескольких удачных тренировок К. научился восстанавливать все электронные реквизиты, утрачиваемые картами во время их использования по назначению. Как показал следственный экспери-

[225] Подробнее см.: *Гелль П.* Магнитные карты и ПК / Пер. с фр. – М., 2001. – С. 100-108.

мент, с помощью указанных орудий преступления К. тратил на подделку одной карты в среднем от 30 до 50 секунд.

После отладки технологии К. стал массово собирать недействительные карты и превращать их в действительные путем копирования электронных реквизитов. Поддельные карты он оптом и в розницу сбывал на железнодорожных вокзалах и станциях метро в г. Москве по 1 руб. за карту на одну поездку и по 8 руб. – на пять. Вырученные от продажи деньги К. тратил на покупку наркотиков для личного потребления.

В приведенном примере выделим следующее обстоятельство. Из допроса К. в качестве подозреваемого стало известно, что при подделке недействительных карт им неоднократно встречались те, которые уже были кем-то ранее подделаны и использованы по назначению[226].

3.2. Подделка интегральной микросхемы памяти. В зависимости от вида интегральной микросхемы, используемой в качестве машинного носителя электронных реквизитов карты, в криминальной практике распространены следующие разновидности данного способа.

А. Замена интегральной микросхемы памяти. Осуществляется в тех случаях, когда технически невозможно ее перепрограммировать – восстановить ранее содержавшиеся на ней электронные реквизиты. Для этого старая неработающая микросхема с помощью скальпеля, канцелярского ножа, лезвия бритвы или стандартного пресса-перфоратора[227] вырезается из подложки карты с частью пластика, в который она имплантирована. В образовавшееся сквозное отверстие вклеивается или вплавляется перепрограммируемая микросхема памяти, имеющая такую же топологию, что и удаленная – не работающая. С помощью подключенного к ПЭВМ специального технического устройства – программатора и соответствующего программного обеспечения, полученного из Интернета, в память микросхемы записываются все необходимые электронные реквизиты, формат и содержание которых берется с карты-оригинала. По мере совершения операций и стирания из памяти поддельной карты электронных реквизитов, они периодически перезаписываются (восстанавливают-

---

[226] См.: *Старухин А.* Московское метро грабили в Воронеже // Трибуна. – 2000. – № 193. – С. 1.

[227] Используется техническими работниками операторов электросвязи при подключении абонентского аппарата (сотового радиотелефона) к своей сети. С помощью такого перфоратора из подложки SIM-карты вырезается модуль с микросхемой, которая подключается к контактам коммутационного порта (слота) сотового радиотелефона (трубки).

ся) мошенником с помощью тех же орудий преступления. Таким образом, например, получается платежно-расчетная карта, имеющая неиссякаемый денежный ресурс.

Б. Перезапись конфиденциальных электронных реквизитов. Совершение подделки данным способом возможно в отношении карт, имеющих перепрограммируемую микросхему, которая была имплантирована в подложку в момент изготовления карты на заводском оборудовании. В этом случае задача преступника упрощается: ему лишь необходимо с использованием вышеуказанных программно-аппаратных средств совершения преступления записать новые электронные реквизиты или модифицировать старые, записанные эмитентом при персонализации карты на имя конкретного держателя.

Оперативно-следственная практика показывает, что этим способом преимущественно подделываются карты, эмитируемые операторами электросвязи (SIM-карты, телефонные и таксофонные карты).

В. Электромеханическое блокирование коммутационных контактов. Как было указано ранее, интегральная микросхема фактически представляет собой электрическую схему. При этом отдельные виды терминальных устройств позволяют производить платежно-расчетные операции с применением карт до тех пор, пока последний логический элемент этой схемы не будет физически уничтожен таким образом, что уже не сможет пропускать через себя управляющий электрический импульс – сигнал. Иными словами, пока через соответствующие коммутационные контакты микросхемы протекает ток, терминальное устройство производит операции, но как только ток перестает циркулировать по микросхеме – операции прекращаются и карта считается недействительной. Используя этот принцип, мошенники замыкают между собой те или иные контакты микросхемы и получают «вечную» карту. В этом случае электрический ток начинает проходить напрямую по замкнутым коммутационным контактам микросхемы, минуя ее электрическую схему. Контакты замыкаются обычной металлической фольгой либо припаиваются друг к другу[228].

В первом случае орудиями преступления будут – прямоугольные фрагменты алюминиевой фольги, ножницы, скальпель (лезвие бритвы или канцелярский нож) и прозрачная липкая

[228] Методику подделки пластиковых карт и совершения с их помощью хищений см.: *Леонтьев Б.К.* Фрикинг без секретов. – М., 2001. – С. 79.

лента – скотч; во втором – электрический маломощный паяльник, олово (припой), канифоль и флюс[229].

Г. Использование имитатора работы микросхемы памяти пластиковой карты. Зная принципы функционирования считывающего устройства электронного терминала, мошенник изготавливает специальное техническое средство, имитирующее работу интегральной микросхемы пластиковой карты. Это СТС относится к классу Специальных технических средств для негласного получения (изменения, блокирования, уничтожения) информации с технических средств ее хранения, обработки и передачи[230]. Оно состоит из следующих компонентов.

1. Электротехническое приспособление, имитирующее контакты микросхемы. Оно предназначено для подключения управляющего модуля СТС – мини-ЭВМ к коммутационному порту считывателя электронного терминала. Данное приспособление изготавливают двумя способами:

а) по технологиям создания электрических печатных плат, например, путем травления покрытого медной фольгой (фольгированного) гетинакса в медном купоросе в кустарных условиях;

б) путем удаления тела интегральной микросхемы из подложки стандартной пластиковой карты соответствующего вида с одновременным сохранением ее коммутационных контактов.

2. Электрические проводники, соединяющие указанное в п. 1 приспособление с программно-аппаратным модулем СТС. В этих целях преступниками используется изготовленный заводским способом тонкопленочный токопроводящий шлейф, состоящий из нескольких электрических проводников (медных жил). Такие шлейфы применяются при изготовлении принтеров: они соединяют печатающие элементы печатной головки с модулем, управляющим их работой.

3. Программно-аппаратный модуль, имитирующий электронную схему работы интегральной микросхемы пластиковой карты. Фактически он представляет собой мини-ЭВМ, работающую под управлением специальной программы и имеющую миниатюрную

---

[229] **Флюс** – специальное химическое вещество, как правило, находящееся в жидком состоянии, применяемое при пайке или сварке металлов для удаления окислов с соединяемых поверхностей.

[230] См.: Перечень видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности // Постановление Правительства Российской Федерации от 01.07.96 г. № 770.

клавиатуру. Размеры модуля сопоставимы с электронным органайзером (записной книжкой или переводчиком).

4. Блок питания – миниатюрные аккумуляторы, используемые в качестве источников электропитания для бытовых электронных приборов и устройств.

Так, в октябре 2001 г. сотрудниками Управления ФСБ России по Ростовской области был задержан студен одного из российских вузов – гражданин Республики Судан Э.Р.О.Ф. Эль Мула, который неоднократно получал неоплачиваемые услуги международной телефонной связи путем неправомерного доступа к охраняемой законом компьютерной информации, повлекшего нарушение работы ЭВМ, а также уничтожение и блокирование такой информации. Как было установлено следствием, в период с августа по октябрь 2001 г. Мула систематически осуществлял длительные неоплачиваемые телефонные переговоры со своими родственниками и знакомыми – абонентами, расположенными на территории Судана. Для этого им использовалось специальное программно-техническое устройство, имитирующее работу интегральной микросхемы таксофонной карты. По заключению судебной компьютерно-технической экспертизы, это устройство – имитатор – нарушало работу ЭВМ таксофонного терминала для ведения междугородных и международных телефонных переговоров. При этом во время разговора информация о его длительности и тарификации автоматически уничтожалась и в процессинговый центр компании «Кубаньтаксофон» – филиала оператора электросвязи ОАО «Южная телекоммуникационная компания» для учета не поступала. Своими действиями Мула причинил ущерб на общую сумму 44 077 руб.[231]

3.4. Использование несовершенства программно-аппаратного обеспечения технологии обращения пластиковых карт

В связи с тем что программы для ЭВМ, обеспечивающие работу персонификационного оборудования, электронных терминалов, их систем и сетей, разрабатываются по разным стандартам различными фирмами-изготовителями, они могут быть частично несовместимы между собой. Несовместимость проявляется в процессе эксплуатации данных средств электронно-вычислительной техники

---

[231] См.: *Щелкунов В.Г.* Виды компьютерных преступлений // Рос. следователь. – 2003. – № 1. – С. 20.

в виде различных сбоев, отказов в работе и логических ошибок, влияющих на конечный результат вычислительных операций. Этими ошибками в вычислениях активно пользуются мошенники.

Так, по данным Следственного комитета при МВД России, в октябре 1994 г. следователем СУ ГУВД г. Москвы по заявлению первого вице-президента Акционерного коммерческого банка «С-ый» было возбуждено уголовное дело в отношении группы лиц, которые вступили в преступный сговор на хищение денежных средств, принадлежащих указанному банку. В ходе предварительного следствия было установлено следующее.

Л., являясь клиентом банка, в июле 1994 г. обратил внимание на ошибку в работе программного обеспечения банкоматов, обслуживаемых потерпевшим. Сбой в вычислительных операциях происходил из-за частичной несовместимости программы автоматизации банковских операций «Пан» немецкой фирмы «Артист» и программы обслуживания пластиковых карт «Аризона» американской фирмы «Аметист системз». Ошибка состояла в том, что в программе «Пан» любая валюта представлялась с двумя дополнительными знаками, рассчитанными на более мелкие единицы основной валюты (копейки, центы, пфенинги и т. д.), а программа «Аризона» при операциях с валютами, не имеющими более мелкого деления, считывала последний знак как единицу основной валюты. В результате чего при снятии через банкомат наличных средств со специального карточного счета, открытого в валютах, не имеющих деления (итальянские лиры, японские йены и др.), остаток на счете держателя определялся ЭВМ неправильно – в 100 раз большим, чем он был в действительности. Таким образом, банкомат позволял снять со счета наличными суммы, стократно превышающие размер суммы вклада, открытого в АКБ «С-ый» в указанных валютах. Это обстоятельство и было использовано Л., который вступил в преступный сговор со своей знакомой Д. для совершения хищений денежных средств.

22 июля 1994 г. Л., не посвящая в свои преступные планы свою мать и заполнив от ее имени часть документов, открыл на нее в банке «С-ый» три счета: в японских йенах, английских фунтах стерлингов и немецких марках. При этом по двум последним счетам специальный карточный счет в йенах был оформлен как дополнительный, поскольку в соответствии с Договором об обслуживании СКС по одной банковской карте в сутки можно было получить из банкомата наличными лишь 500 тыс. рублей. По доверенности Л. получил по открытым счетам соответственно три пластиковые карты на имя матери и ПИН-коды доступа к ним. После этого через

кассу банка Л. внес на указанные счета денежные средства в рублях, сконвертировав их в йены по действовавшему курсу. Затем в течение недели он периодически пополнял сумму основного вклада в йенах, конвертировал деньги с йен в рубли и использовал для наращивания похищаемой суммы основного и двух дополнительных счетов. В конце этой криминальной операции через банкоматы деньги были сняты Л. совместно с Д. в несколько приемов и поделены.

Расширяя свою преступную деятельность, Л. аналогичным способом «в темную» открыл четыре счета на своего знакомого М.: в йенах, французских франках, финских марках и итальянских лирах. По трем последним счетам в качестве дополнительного был оформлен СКС в йенах. 29 июля 1994 г. Л. получил от М. 4 пластиковые карты и ПИН-коды к ним. Таким же порядком была проведена операция и со случайным знакомым Л. – Ш.: по его паспорту были открыты 4 счета для совершения операций с использованием банковских карт, но уже с тремя другими валютами, неизменной оставалась лишь японская йена.

4 августа того же года преступники, используя найденный паспорт на имя гр. З. и вклеив в него фотографию Д., открыли по нему еще 4 счета, получив по ним соответствующие орудия хищения – пластиковые карты и ПИН-коды.

Своими преступными действиями Л. и Д. причинили потерпевшему АКБ «С-ый» ущерб на общую сумму около 500 млн неденоминированных рублей.

Следует обратить внимание на тот факт, что хищения, совершаемые вышерассмотренным способом, можно выявить только путем проведения специальных исследований, осуществляемых контрольно-ревизионными органами совместно со службами защиты конфиденциальной компьютерной информации.

Подводя некоторую черту в исследовании темы настоящей работы, представляется возможным акцентировать внимание на следующем. Преступления, совершенные с использованием пластиковых карт и их реквизитов, с позиций криминалистической науки целесообразнее условно выделить в отдельную группу преступных посягательств, имеющих отличительные признаки. Это отличие проявляется: в их повышенной социальной опасности и достаточно широкой распространенности; специфичности предметов и орудий посягательств; наличии определенного круга потерпевших; характерных способах подготовки, совершения и сокрытия преступлений, обусловленных технологиями оборота нового вида документов – пластиковых карт; использовании при их совершении средств

электронно-вычислительной техники; специфичной локализацией материальных следов на месте происшествия; возрастных и профессиональных особенностях личности преступников; совершении значительного числа преступлений группами лиц по предварительному сговору и в составе организованных преступных групп и сообществ.

С учетом вышеизложенного очевидно, что эффективность криминалистической характеристики как выработанного наукой инструмента формирования частной методики тем выше, чем конкретнее и точнее выделены все существенные для расследования данного вида преступлений обстоятельства. Поэтому основное назначение криминалистической характеристики преступлений выделенной категории видится в возможности реального ее использования в следственной практике. Знание следователем и оперативным сотрудником корреляционных связей между ее основными элементами позволит уже на первоначальном этапе работы по делу с учетом исходной криминалистически значимой информации более точно оценить те или иные следственные ситуации, выдвинуть обоснованные версии, успешно спланировать свою работу, более точно определить направления розыска преступника и расследования преступления, вид и характер следственных действий, оперативно-разыскных и организационно-тактических мероприятий, которые будут подробно рассмотрены в последующих главах данной работы.