**МОСКОВСКАЯ АКАДЕМИЯ ЭКОНОМИКИ И ПРАВА**

**РЯЗАНСКИЙ ФИЛИАЛ**

**КОНТРОЛЬНАЯ РАБОТА ПО ДИСЦИПЛИНЕ**

**«ПРЕСТУПЛЕНИЯ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ»**

**Тема: Криминалистическая классификация преступлений в сфере компьютерной информации.**

**Рязань 2004 г.**

**План**

1. Криминалистическая классификация преступлений в сфере компьютерной информации. 3

2. «Пластиковая» преступность 18

Литература 22

# 1. Криминалистическая классификация преступлений в сфере компьютерной информации.

«Минимальный список нарушений» содержит восемь основных видов компьютерных преступлений:

* компьютерное мошенничество;
* подделка компьютерной информации;
* повреждение данных ЭВМ или программ ЭВМ;
* компьютерный саботаж;
* несанкционированный доступ;
* несанкционированный перехват данных;
* несанкционированное использование защищенных компьютерных программ;
* несанкционированное воспроизведение схем.

«Необязательный список» включает в себя четыре вида компьютерных преступлений:

* изменение данных ЭВМ или программ ЭВМ;
* компьютерный шпионаж;
* неразрешенное использование ЭВМ;
* неразрешенное использование защищенной программы ЭВМ.

Одной из наиболее распространенных классификаций преступлений в сфере компьютерной информации является *кодификатор рабочей группы Интерпола*, который был положен в основу автоматизированной информационно-поисковой системы, созданной в начале 90-х годов. В соответствии с этим кодификатором все компьютерные преступления классифицированы следующим образом:

**QA – Несанкционированный доступ и перехват:**

QAH – компьютерный абордаж;

QAI – перехват;

QAT – кража времени;

QAZ - прочие виды несанкционированного доступа и перехвата.

**QD – изменение компьютерных данных:**

QDL – логическая бомба;

QDT – троянский конь;

QDV – компьютерный вирус;

QDW – компьютерный червь;

QDZ – прочие виды изменения данных.

**QF – Компьютерное мошенничество:**

QFC – мошенничество с банкоматами;

QFF – компьютерная подделка;

QFG – мошенничество с игровыми автоматами;

QFM –манипуляции с программами ввода/вывода;

QFP – мошенничество с платежными средствами;

QFT – телефонное мошенничество;

QFZ – прочие компьютерные мошенничества.

**QR – Незаконное копирование:**

QRG – компьютерные игры;

QRS – прочее программное обеспечение;

QRT – топология полупроводниковых устройств;

QRZ – прочее незаконное копирование.

**QS – Компьютерный саботаж:**

QSH – с аппаратным обеспечением;

QSS – с программным обеспечением

QSZ – прочие виды саботажа.

**QZ – Прочие компьютерные преступления:**

QZB – с использованием компьютерных досок объявлений;

QZE – хищение информации, составляющей коммерческую тайну;

QZS – передача информации, подлежащая судебному рассмотрению;

QZZ – прочие компьютерные преступления.

Одним из достоинств, предложенного кодификатора, является введение литеры «Z», отражающей прочие виды преступлений и позволяющей совершенствовать и дополнять используемую классификацию.

Однако все приведенные выше кодификаторы и системы классификации страдают одним общим недостатком – в них происходит смешение уголовно-правовых начал и технических особенностей автоматизированной обработки информации, что приводит к неоднозначности толкования и существенным проблемам при формулировании частных целей и задач расследования преступлений в сфере компьютерной информации.

В связи с этим для расследования преступлений возрастает значение криминалистической классификации, которая (в общем случае) проводится по способу, обстановке, орудиям и месту совершения преступления, его последствиям, непосредственным предметам посягательства, условиям их охраны от преступных посягательств, личности субъекта преступления, личности потерпевших, способов сокрытия следов преступления и лица его совершившего. Построение криминалистической классификации преступлений в сфере компьютерной информации должно быть основано на анализе объекта преступного посягательства – компьютерной информации как сложного многоуровневого объекта.

Проведенный анализ сущности информации, обрабатываемой (используемой) в большинстве автоматизированных систем, а также форм ее представления (существования) показал, что компьютерная информация как объект преступного посягательства представляет собой достаточно сложную иерархическую структуру с тремя основными уровнями представления – физическим, логическим и семантическим.

1. *Физический уровень* – уровень материальных носителей информации, где информация представлена в виде конкретных характеристик вещества (намагниченность домена – для магнитных дисков, угол и дальность плоскости отражения лазерного луча – для лазерных компакт-дисков) или электромагнитного поля (амплитуда, фаза, частота).

Учитывая, что практически все использующиеся в настоящее время ЭВМ являются цифровыми и используют двоичную систему счисления, большие объемы информации могут быть представлены в виде последовательности или поля из элементарных информационных единиц («0» и «1»).

2. *Логический уровень* – уровень представления более сложных информационных структур (от байта до файла) на основе элементарных компонент физического уровня. Данный уровень включает две группы правил объединения – *общие* и *специальные*.

*Общие правила* диктуются физическими основами устройства и техническими особенностями используемых средств обработки информации и не могут быть быстро и произвольно изменены. В качестве примера общих правил объединения множества элементарных информационных единиц в более крупные информационные структуры может служить количество и порядок нанесения информационных дорожек на магнитном носителе, размер кластера и т. п. *Специальные правила* объединения устанавливаются заказчиками или разработчиками автоматизированных информационных систем и могут быть достаточно просто изменены.

В качестве примера специальных правил объединения информации могут быть приведены способы объединения информационных полей в записи базы данных, записей и запросов в банках данных. Поскольку специальные правила объединения не обусловлены техническими особенностями аппаратных средств, то они могут быть быстро изменены (даже в рамках выполнения одной программы) или же просто проигнорированы. Например, записи баз данных могут быть прочтены не как последовательность записей установленного формата (то есть файл последовательного доступа), а как файл прямого доступа, состоящий из отдельных байтов или даже битов.

*Семантический уровень* – уровень смыслового представления информации. На данном уровне можно говорить о содержательной части компьютерной информации, представленной двумя предыдущими видами.

Названные уровни компьютерной представления информации тесно взаимосвязаны между собой и образуют единую систему. Такое представление компьютерной информации позволяет решить основные проблемы уголовно-правовой квалификации деяний в сфере компьютерной информации и основные криминалистические проблемы.

Так, наличие третьего уровня представления (семантического) позволяет разграничить (в уголовно-правовом смысле) преступления в сфере компьютерной информации от иных информационных преступлений, совершаемых с использованием средств вычислительной техники и новых информационных технологий (разглашение тайны усыновления в результате доступа к базе данных органов ЗАГС, шпионаж и т.п.).

С точки зрения криминалистики представление компьютерной информации в виде сложного многоуровневого объекта позволяет понять суть происходящих явлений при совершении преступления в сфере компьютерной информации. Получить осознаваемую информацию (готовую к восприятию человеком), то есть представленную на третьем, семантическом уровне, невозможно, не преодолев два нижних уровня ее представления. Таким образом, если следователь установил факт того, что преступник добыл информацию из автоматизированной системы и каким-либо образом осознанно воспользовался ею, значит у него были средства (орудия) совершения действий на первом (физическом) и втором (логическом) уровнях ее представления, он владел навыками их использования и специальными познаниями для их настройки и подключения.

Отсутствие или невозможность выявления хотя бы одного из элементов деятельности подозреваемого в совершении преступления в сфере компьютерной информации на более низком уровне представления информации заставляет серьезно сомневаться в возможности совершения им самостоятельных действий на более высоком уровне ее представления и говорит о наличии у него сообщника или невольного пособника.

Представление информации в виде трехуровневой системы позволяет определить исчерпывающий перечень действий на каждом из них и представить любое деяние, описываемое в терминах уголовного законодательства и наук информационного цикла как совокупность элементарных действий соответствующего уровня.

На физическом уровне представления информации технически возможно выполнение всего лишь трех действий – чтения, записи и разрушения. При этом под разрушением понимается такое воздействие на носитель информации, при котором стандартными средствами чтения невозможно получить какое-либо определенное значение, то есть нет ни «0», ни «1». Разрушение информации может быть произведено воздействием мощного внешнего магнитного поля на магнитный носитель информации. Таким образом, традиционно используемые в законодательстве понятия могут быть представлены через последовательность или сочетание названных трех элементарных действий.

Например, «копирование информации» представляет собой строгую последовательность операции чтения и записи порций информации. «Уничтожение информации», в свою очередь, представляет собой или разрушение информации или запись новой информации на то место носителя, где размещалась уничтожаемая информация.

В существующих вычислительных системах удаление или уничтожение информации как раз и происходит путем записи новой информации поверх уничтожаемой. Говоря о понятии «уничтожение информации», необходимо отметить наличие существенной разницы между действием пользователя автоматизированной системы по уничтожению (удалению) информации (имеющим существенное значение для уголовно-правовой квалификации деяния) и криминалистически значимым (имеющим существенное значение с точки зрения возможности обнаружения и изъятия следов существования информации), то есть действительным удалением информации.

Пользователь автоматизированной системы, совершив удаление информационного файла (запустив стандартную команду операционной системы *delete*), выполнил все необходимые действия для его уголовно-правовой квалификации как «удаление информации», в то время как в реальности был изменен только первый символ имени удаляемого информационного файла в области FAT магнитного носителя, а весь информационный массив остался неизменным. Внесенная пометка в первом символе имени файла означает, что операционная система может использовать места, в которых находились кластеры удаленного информационного файла, для записи другой информации. В связи с этим для осуществления криминалистически значимого удаления информации необходимо не только выполнить стандартные действия, но и записать новую информацию на место размещения удаляемой.

Более сложную комбинацию элементарных действий представляют собой действия по модификации и блокированию информации. Говоря о модификации, следует подчеркнуть, что это есть действие по изменению значения информации в желаемом (заданном) направлении. Важнейшим элементом в определении понятия «модификация» является направленность изменения информации. Если нет направленности в выполняемых действиях, то это уже не модификация, а уничтожение информации. Модификация означает, что информация не должна быть уничтожена не только на логическом, но и на физическом уровне. Модификацией будет являться заданное изменение лишь нескольких символов в смысловой фразе.

Понятие «блокирование информации» во многом совпадает с понятием «модификация информации» и отличается лишь тем, что модификации подвергается не смысловая, а управляющая информация. Например, для блокирования доступа легального пользователя к базам данных необходимо изменить значение кода доступа этого пользователя в системных файлах администратора безопасности, сохранив содержание самой базы данных.

Анализ известных случаев преступлений в сфере компьютерной информации, а также анализ особенностей развития современных информационных технологий и условий их применения в различных сферах человеческой деятельности позволяет предложить следующую систему их криминалистической классификации.

1. Неправомерное завладение информацией как совокупностью сведений документов (нарушение исключительного права владения).

 1.1 Неправомерное завладение информацией как совокупностью сведений, документов (нарушение исключительного права владения).

 1.2 Неправомерное завладение информацией как товаром.

 1.3 Неправомерное завладение информацией как идеей (алгоритм, методом решения задачи)

2. Неправомерная модификация информации.

 2.1 Неправомерная модификация информации как товара с целью воспользоваться ее полезными свойствами (снятие защиты).

 2.2 Неправомерная модификация информации как идеи, алгоритма и выдача за свою (подправка алгоритма).

 2.3 Неправомерная модификация информации как совокупности фактов, сведений (записи на счетах в банке).

3. Разрушение информации.

 3.1 Разрушение информации как товара.

 3.2 Уничтожение информации.

4. Действие или бездействие по созданию (генерации) информации с заданными свойствами.

 4.1 Распространение по телекоммуникационным каналам информационно-вычислительных сетей информации, наносящей ущерб государству, обществу и личности.

 4.2 Разработка и распространение компьютерных вирус и прочих вредоносных программ для ЭВМ.

 4.3 Преступная халатность при разработке (эксплуатации) программного обеспечения, алгоритма в нарушение установленных технических норм и правил.

5. Действия, направленные на создание препятствий пользования информацией законным пользователям.

 5.1 Неправомерное использование ресурсов автоматизированных систем (памяти, машинного времени и т.п.)

 5.2 Информационное «подавление» узлов телекоммуникационных систем (создание потока ложных вызовов).

Приведенная классификация содержит специальные индексы, которые мы будем использовать в дельнейшем при рассмотрении типовых начальных следственных ситуаций и изложении приемов расследования данного вида преступлений, а также включает достаточно много новых (чисто технических) и «непонятных» для практических работников правоохранительных органов терминов и понятий.

В этой связи необходимо дать краткую характеристику содержания каждого из приведенных видов преступлений.

**Неправомерное завладение информацией как совокупностью сведений документов (нарушение исключительного права владения).** Это наиболее часто встречающийся класс простейших преступных деяний, к которым относятся, как правило, без должного внимания. Примером данного вида деяний является неправомерное ознакомление служащего банка с записью в базе данных размера вклада того или иного клиента, его адресе, видах сделок и т.п.

С криминалистической точки зрения это наиболее простое действие, для осуществления которого не обязательна длительная подготовка, высокая квалификация и разработка специальных приспособлений. Преступник может воспользоваться штатным набором средств аппаратного и программного обеспечения автоматизированной системы, в которой осуществляются данные действия. Результаты данного действия могут быть записаны на машинный носитель информации (магнитный или лазерный диск, магнитную ленту и т.п.), бумагу или просто остаться в памяти человека.

**Неправомерное завладение информацией как товаром.** Это наиболее распространенный вид преступных, но не считающихся таковыми в современном российском обществе деяний, который заключается в копировании программ для ЭВМ или целой информационной системы (банка данных, электронного архива и пр.) без согласия (разрешения) владельца или собственника. Данный вид деяний очень широко распространен в нашей стране и, к сожалению, часто является практически единственной возможностью получения современного программного обеспечения.

Примером такого преступления может быть переписывание программы расчета заработной платы, ведения главной книги бухгалтера, автоматизированного банка данных с адресами предприятий и др. При этом цель преступления – воспользоваться нужными свойствами неправомерно полученной информации (программы, базы данных): выполнить расчеты с использованием программы, получить справки или отчеты из базы данных.

С криминалистической точки зрения это уже более сложное деяние, для которого обязательно использование машинного носителя информации, так как современные программные продукты занимают весьма значительные объемы памяти. Для достижения целей данного вида действий часто бывает недостаточно завладения только файлами программного продукта, так как для нормального его функционирования необходимо наличие определенных компонентов общего (драйверов периферийных устройств. Наличия музыкальной карты и др.) или общесистемного программно-математического обеспечения (системы управления базами данных, электронной таблицы и др.)

**Неправомерное завладение информацией как идеей, алгоритмом (методом преобразования информации).** Данный вид преступления заключается в ознакомлении с использующимся методом расчета каких-либо оценок, алгоритмом принятия решений в экспертной системе или другой автоматизированной системе принятия решений. Примером такого деяния может быть ознакомление с методом расчета вероятности преодоления противоракетной обороны средствами воздушно-космического нападения вероятного противника, ознакомление с использующимся типом (механизмом) системы защиты информации в электронной системе платежей банка.

С криминалистической точки зрения это достаточно сложное действие, так как оно предусматривает не только доступ к информации как к совокупности фактов или сведений, но и последующие этапы, связанные с анализом структуры используемых данных. Выяснением их смыслового значения, последовательности их применения для получения требуемого результата. Для реализации этого действия необходимо наличие специальных средств анализа программного обеспечения (отладчики, дизассемблеры, интерпретаторы), высокой квалификации исполнителей (или хотя бы одного из них). Как правило, такие действия не могут быть проведены в одиночку, так как, во-первых, очень редко бывает, чтобы в одном человеке были воплощены все необходимые навыки и умения, необходимые для его совершения, и, во-вторых, чтобы он же имел возможность воспользоваться материальной выгодой от использования результатов неправомерного завладения информацией как идеей (алгоритмом).

Такого рода преступные деяния образуют фабулу промышленного шпионажа, когда крупные фирмы организуют специальные разведывательные операции, проводимые в течение значительного промежутка времени, по единому замыслу, с привлечением многих исполнителей и направленные на добывание промышленных секретов своих конкурентов.

**Неправомерная модификация информации как товара.** Данный вид деятельности, так же как и неправомерное завладение информацией как товаром, является наиболее распространенным преступлением (на наш взгляд, именно преступлением). Многие фирмы – производителя программного обеспечения. Стараясь защитить себя от компьютерного пиратства. Разрабатывают и используют различные методы защиты от копирования и анализа своих разработок. Однако экономические условия, в которых функционирует наша экономика, а также принципиальная невозможность создания абсолютных средств защиты информации приводят к тому, что программное обеспечение или базу данных, полученную однажды законным (или «полузаконным» путем), вносится модификация, позволяющая делать неограниченное количество копий и использовать полезные свойства информации как товара без каких-либо ограничений (временных или по числу раз запуска), наложенных разработчиком.

**Неправомерная модификация информации как идеи.** Данный вид преступного деяния встречается гораздо реже и заключается не только в получении какого-либо программного обеспечения, но и его обязательный предварительный анализ. Примером такого рода действий могут служить широко известные случаи преступления в банковской сфере, когда в алгоритмы выполнения действий с записями на счетах, взимания процентов и пр. вносились незапланированные модификации, при которых с каждой операции на заранее подготовленный счет делались отчисления (так называемые атаки «салями»). Практически все известные на сегодняшний день преступления такого рода совершены разработчиками программного обеспечения и чаще всего теми же, которые его эксплуатируют.

Характерной криминалистической чертой данного преступления является, во-первых, то, что направление деятельности (научно-техническая разработка), в которое планируется внедрить чужую идею (алгоритм), должно иметь весьма ощутимую экономическую или другую ценность. Во-вторых, исполнители должны обладать большим багажом специальных познаний в данной области. В-третьих, для совершения данного преступления необходимо наличие специального технического и программного обеспечения.

**Неправомерная модификация информации как совокупности** **фактов.** Данный вид преступлений особенно широкое распространение получил в автоматизированных банковских системах, так как именно в них записи в полях баз данных отражают определенные денежные суммы или другие сведения, которые имеют конкретное денежное или иное экономическое выражение.

**Разрушение информации как товара.** Данный вид преступления заключается в том, что законный владелец информации не может воспользоваться программным обеспечением или базой данных как товаром, его полезным свойством.

**Распространение по телекоммуникационным каналам информационно-вычислительных сетей информации, наносящей ущерб государству, обществу или личности.** Данный вид преступлений имеет самостоятельное значение лишь с криминалистической точки зрения, т. е. точки зрения способов выявления субъекта преступления, особенностей совершения преступления, в то время как с уголовно-правовой может быть полностью охарактеризовано с помощью других (некомпьютерных) составов преступлений, но и с использованием компьютера. Примером такого рода преступных деяний может быть создание и распространение компьютерных игр порнографического характера с известными персонажами, использование компьютерных сетей для передачи и распространения материалов, содержащих призывы к насильственному изменению конституционного строя, и пр.

**Разработка и распространение компьютерных вирусов.** Этот вид деяний является очень распространенным в настоящее время и может соперничать по количеству зарегистрированных фактов разве что только с неправомерным завладением информацией как товаром.

**Преступная халатность при разработке программного обеспечения, алгоритма в нарушение установленных технических норм и правил.** Развитие вычислительной техники и информатики привело к тому, что автоматизированные системы управления находят свое применение практически во всех отраслях техники и экономики. Не являются исключением и вооружение, объекты атомной энергетики, непрерывные химические производства, системы управления воздушным движением, а также другие объекты, аварии и неисправности которых могут причинить огромный ущерб и вызвать непоправимые последствия. В связи с этим уже в настоящее время у нас в стране и за рубежом разработаны стандарты, инструкции и рекомендации, определяющие порядок разработки, испытания, эксплуатации и сопровождения программных средств критического приложения.

Таким образом, под составом преступления, предусмотренного в п. 4.3 классификации, следует понимать нарушение этих установленных правил, которые повлекли за собой тяжкие последствия.

**Неправомерное использование ресурсов автоматизированных систем.** Развитие вычислительной техники, появление сетей ЭВМ привело к возможности ее коллективного использования различными субъектами. При этом потребители запрашивают и оплачивают определенный вычислительный ресурс (объем внешней и оперативной памяти, время работы процессора). При этом под составом преступного деяния следует понимать скрытный неправомерный захват вычислительного ресурса коллективного пользования каким либо субъектом с намерениями минимизации либо полного исключения своих затрат за его использование.

**Информационное «подавление» узлов телекоммуникационных систем.** Появление доступных информационных систем коллективного пользования, построенных на основе стандартных телефонных каналов взаимосвязанной системы связи России (Internet, Relcom), позволило решать задачи информационного обеспечения самых широких кругов потребителей. В частности, с использованием этой информационной технологии разрабатывались системы электронных торгов на биржах, передачи ценовой информации, проведения электронных платежей.

Большую роль в этом играет оперативность получения информации с использованием систем такого рода. Например, наличие принадлежащих одной и той же фирме торговых мест на биржах городов из разных часовых поясов позволяет при использовании модемной связи получить все основные параметры интересующих сделок на торгах и сыграть на разнице цен. Временной интервал, при котором необходимо получить информацию, то есть период, когда она имеет ценность, равняется разнице в часовых поясах.

Использование стандартных телефонных коммутируемых каналов для обеспечения электронных торгов, сделало их достаточно уязвимыми для так называемого «информационного подавления», когда по заданному телефонному номеру осуществляется постоянный «автодозвон» с нескольких источников, создавая тем самым поток ложных вызовов, при котором истинный абонент не может установить желаемое телефонное соединение.[[1]](#footnote-1)

# 2. «Пластиковая» преступность

По мнению специалистов, компьютер становится самым многообещающим орудием преступления. В развитых странах практически все денежные операции производятся через компьютерные системы и сети. Широкое распространение получили кредитные карточки, заменяющие обычные деньги. Их поделка, воровство с помощью ЭВМ приняли характер подлинного бедствия в США, Италии и других странах. Компании, особенно банки, стремятся скрыть факты компьютерного воровства, поскольку опасаются падения доверия вкладчиков, акционеров, партнеров. Поэтому в официальной статистике масштабы потерь почти не регистрируются. Да и жертвы часто не подозревают, что их обокрали. Эксперты полагают, что в США с помощью ЭВМ из банков похищают вчетверо больше, чем при вооруженных ограблениях. За последние 10 лет ежегодные потери возросли более чем в 20 раз и составляют десятки миллиардов долларов.

В апреле 2003 года трое молодых людей с помощью хитроумного устройства похитили из московских банкоматов более $700 тыс. Небольшое устройство - уникальное изобретение трех студентов московских технических вузов, их гордость и источник дохода. Причем дохода довольно значительного: с января они заработали 700 тысяч долларов.

Устройство позволяло им снимать с чужих кредитных карточек все деньги. Оно прикрепляется к щели, куда вставляется кредитка, надежно крепится к банкомату и, поскольку покрашено в его цвет, практически не привлекает к себе внимания. Зато считывает с карточки все данные, когда человек пытается снять со счета деньги. А крепившаяся рядом видеокамера записывала вводимый владельцем кредитки пин-код. После этого 3 студента имели практически неограниченный доступ к чужому банковскому счету. С помощью оборудования, купленного специально для этого, делался дубликат карточки, и обычно в этом же банкомате все средства со счета снимались. Только по предварительным данным от этого пострадало около 200 человек.

Работали студенты в центре Москвы. У тех банкоматов, через которые проходит много людей - на Садовом кольце и на Тверской улице. Чтобы задержать их, милиции пришлось проводить целую спецоперацию.

Филипп Золотницкий, начальник пресс-службы УБЭП ГУВД г.Москвы: "Пришлось привлекать к работе около 300 наших сотрудников, а те банкоматы, которые не были охвачены, мы просто отключили".

Но даже в милиции об этих студентах говорят с некоторой долей восхищения. Такое в мире не удавалось вообще никому. Принцип подобного устройства известен давно, но сделать его миниатюрным и пригодным к работе получилось только у них. Более того, эксперты не смогли сразу понять, как оно крепиться к банкомату и поэтому аппарат пришлось разбирать прямо на месте.

Студенты же максимально использовали уникальность этого устройства, один его экземпляр они продали французским арабам, занимающимся мошенничествами с кредитками. И им же продавали данные, полученные с карточек в Москве. Поэтому, хотя изобретателей и поймали, деньги со счетов все равно могут продолжать пропадать.

Как бы то ни было, но держателям карт, можно сказать, повезло. Во-первых, потому, что преступление раскрыто, во-вторых, потому, что большая часть украденных денег жива. Как сообщили «Газете.Ru» в УБЭП, 55% из снятых мошенниками $700 тыс. они потратить не успели. Так что половина украденных денег пострадавшим будет возвращена. Какие банки, и в каком количестве невольно оказались участниками преступления, не раскрывается в интересах следствия.

А вообще, «карточные» кражи тем и страшны, что много пострадавших и участников преступления, так что вернуть деньги удается далеко не всегда.

Каждый владелец пластиковой карты сто раз слышал о том, что пин-код надо хранить в целости и сохранности, номер никогда и никому не давать и не показывать, а сам «пластик» беречь как зеницу ока.

Как выясняется, даже простое снятие наличных денег в банкомате может закончиться плачевно. Поэтому лучше заранее узнать о возможных уловках аферистов, чем в один прекрасный день из-за незнания их расстаться со своими деньгами. Назовем самые распространенные способы мошенничества с картами.

1. Зачастую мошенники используют устройства, которые, будучи установлены на банкомате, помогают им получить сведения о карточке. В свое время в Москве отметилась группа мошенников, которая устанавливала на клавиатуры специальные насадки, которые внешне повторяли оригинальные кнопки. Владелец карты снимал деньги со счета без всяких проблем, но при этом поддельная клавиатура запоминала все нажатые клавиши, в том числе и пин-код.

Совет: прежде чем снять деньги со счета, внимательно изучите клавиатуру незнакомого банкомата.

2. Другое устройство, англичане называют его lebanese loops. Это пластиковые конверты, размер которых немного больше размера карточки - их закладывают в щель банкомата. Хозяин кредитки пытается снять деньги, но банкомат не может прочитать данные с магнитной полосы. К тому же из-за конструкции конверта вернуть карту не получается. В это время подходит злоумышленник и говорит, что буквально день назад с ним случилось то же самое! Чтобы вернуть карту, надо просто ввести пин-код и нажать два раза на Cancel. Владелец карточки пробует, и, конечно же, ничего не получается. Он решает, что карточка осталась в банкомате, и уходит, дабы связаться с банком. Мошенник же спокойно достает кредитку вместе с конвертом при помощи нехитрых подручных средств. Пин-код он уже знает - владелец (теперь уже бывший) «пластика» сам его ввел в присутствии афериста. Вору остается только снять деньги со счета.

3. Технически сложно, но можно перехватить данные, которые банкомат отправляет в банк, дабы удостовериться в наличии запрашиваемой суммы денег на счету. Для этого мошенникам надо подключиться к соответствующему кабелю, при этом, не разрывая его, и считать необходимые данные. Учитывая, что в Интернете соответствующие инструкции легко обнаруживаются в свободном доступе, а технический прогресс не стоит на месте, можно утверждать: такой вариант будет встречаться все чаще.

4. Для того чтобы узнать пин-код, некоторые аферисты оставляют неподалеку миниатюрную видеокамеру. Сами же они в это время находятся в ближайшем автомобиле с ноутбуком, на экране которого видны вводимые владельцем карты цифры.

Совет: вводя пин-код, прикрывайте клавиатуру свободной рукой.

5. Дорогостоящий, но верный способ. Бывают случаи, когда мошенники ставят в людном месте свой собственный «банкомат». Он, правда, почему-то не работает (да кого этим удивишь?), естественно, никаких денег не выдает - зато успешно считывает с карточки все необходимые данные. А потом выясняется, что вы вчера уже сняли все деньги со счета и почему-то не хотите этого вспомнить!

6. В свое время мошенники из ОАЭ устанавливали в отверстия для кредиток специальные устройства, которые запоминали все данные о вставленной в банкомат карте. Злоумышленникам оставалось только подсмотреть пин-код, либо вышеописанными способами - первым и четвертым, либо банально подглядывая из-за плеча.

7. Здесь уже ничто не зависит от вашей внимательности, осторожности или предусмотрительности. Просто бывает, что в сговор с мошенниками вступают те люди, которым добраться до ваших кредиток и так очень просто, служащие банков, например. Это случается очень редко, но от таких случаев не застрахован никто.

# Литература

1. Уголовный кодекс Российской Федерации. М., 2001.

2. Королев Д.Г. Информация и право: Учебное пособие. – Рязань: Рязанский факультет Московского института МВД Россию 2000.

3. «Пластиковая» преступность // http: www.crime-research.org.

1. Королев Д.Г. Информация и право: Учебное пособие. – Рязань: Рязанский Факультет Московского института МВД Россию 2000. С. 41 - 55. [↑](#footnote-ref-1)