УДК 343.7

УГОЛОВНО-ПРАВОВЫЕ СРЕДСТВА ПРОТИВОДЕЙСТВИЯ ХИЩЕНИЯМ ДЕНЕЖНЫХ СРЕДСТВ, НАХОДЯЩИХСЯ НА БАНКОВСКИХ СЧЕТАХ ГРАЖДАН

А. А. Лихолетов

Волгоградская академия МВД России

Поступила в редакцию 24 февраля 2015 г.

Аннотация: *статья посвящена анализу современного состояния хищений денежных средств, находящихся на банковских счетах граждан. Указанные общественно опасные деяния получили широкое распространение в связи с масштабным внедрением в обиход пластиковых карт и возможностью незаконного обогащения в значительных объемах. Отдельным условием роста таких преступлений является отсутствие эффективных уголовно-правовых мер противодействия им.*
Ключевые слова: *банковские счета, пластиковые карты, преступление, скимминговое оборудование, скиммер, техническое устройство, хищение.*

Abstract: *this article analyzes the current state of embezzlement of funds held in bank accounts of citizens. These socially dangerous acts are widely used in connection with the large scale introduction into use of plastic cards and the possibility of illicit enrichment in large volumes. Separate condition for the growth of such crimes is a lack of effective criminal law measures to counter them.*
Key words: *bank accounts, credit cards, crime, skimming equipment, skimmer, technical devices, theft.*

Появление и распространение некоторых видов преступлений нередко коррелируется с развитием отдельных направлений научно-технического прогресса. К таковым можно отнести и постоянно возрастающее количество хищений денежных средств, находящихся на банковских счетах граждан, с использованием специальных технических устройств, позволяющих считывать данные о ПИН-кодах и иных реквизитах пластиковых карт (скимминговое оборудования).

Так, по сведениям, предоставленным заместителем министра внутренних дел России И. Н. Зубовым, ежегодно число регистрируемых преступлений данного вида растет в среднем на 10 %[1]. Однако следует отметить, что подобные преступления обладают повышенным уровнем латентности, в связи с этим только часть их выявляется сотрудниками правоохранительных органов.

Алгоритм совершения рассматриваемых преступлений в общих чертах можно представить следующим образом[2].

[1] Госдума вводит уголовную ответственность за скимминг-хищение средств с банковских карт. URL: http://itar-tass.com/obschestvo/1583620

[2] При подготовке данной статьи автор сплошным методом изучил 23 приговора и иные судебные акты по рассматриваемым уголовным делам, размещенным на сайтах «Росправосудие», «Судебные решения.рф», «Sudact.ru».

1. На стадии приготовления лицами приобретается комплект специальных технических устройств, в состав которого входят: скиммер (устройство в виде накладки, внешне напоминающее стандартное оборудование банкомата, устанавливаемое перед картоприемником банкомата); накладка, имитирующая клавиатуру банкомата, а также накладка в виде пластиковой планки с вмонтированной с внутренней стороны микровидеокамерой и собственным цифровым носителем либо передатчиком (для видеофиксации и снятия информации о ПИН-кодах к пластиковым картам); энкодер (устройство, позволяющее с помощью компьютерной техники и специального программного обеспечения переносить информацию о пластиковой карте, считанную скиммером, на карту-клон); комплект «белого пластика» (заготовок пластиковых карт, на которые со скиммеров переносится информация, необходимая для получения денежных средств через банкомат).

Приобретение указанного комплекта не вызывает особых сложностей. Наиболее распространенным является покупка через объявления, размещенные в сети Интернет, путем регистрации на специализированных сайтах.

Так, при рассмотрении уголовного дела по обвинению Г. в совершении преступлений, предусмотренных ч. 1 ст. 158, ч. 2 ст. 272, ч. 3 ст. 183, ч. 1 ст. 158, ч. 2 ст. 272, ч. 3 ст. 183, ч. 3 ст. 30, ч. 1 ст. 158 УК РФ Сарапульским городским судом Удмуртской Республики, установлено, что Г. в период с 09.06.2013 г. по 15.10.2013 г., находясь по месту жительства, зарегистрировался на сайте «XXX» и в целях подготовки к совершению преступлений изучил информацию о техническом процессе «скимминга». После чего, продолжая свои преступные действия, Г. на указанном сайте нашел объявление о продаже скиммингового оборудования» пользователем сайта. Затем Г. сообщил неустановленному пользователю сайта о своем намерении пробрести «скиммингговое оборудование» по цене и на условиях продавца: перечисление Г. денежных средств в сумме 2000 долларов США на лицевой счет неустановленного следствием лица. 28.09.2013 г. Г. перечислил денежные средства в требуемой сумме на лицевой счет, указанный ему пользователем сайта, который в свою очередь направил Г. информацию об отправке груза, дате и месте его получения в офисе логистической компании[3].

2. Далее определяется банкомат, на который планируется установка скиммингового оборудования. В большинстве случаев скиммеры устанавливаются на банкоматы, расположенные в малолюдных местах, в ночное время суток.

3. Затем на банкомат, расположенный в определенном месте, устанавливается скиммер, накладка на клавиатуру и средства видеофиксации (для получения сведений о ПИН-кодах держателей карт). Если банкомат расположен в отдельном закрытом помещении (офис банка),

[3] Приговор Сарапульского городского суда Удмуртской Республики от 5 августа 2014 г. № 1-139/14 1-139/2014. URL: http://sudact.ru/regular/doc

доступ в которое осуществляется с помощью пластиковой карты круглосуточно, считывающее устройство устанавливают на картоприемник, расположенный на входной двери.

4. После снятия оборудования с банкомата полученные данные с магнитной полосы кредитных карт законных держателей копируются с носителя, вмонтированного в скимминговое оборудование, на персональный компьютер. В случае, если скимминговое оборудование оснащено передатчиком, информация с него передается по радиоканалу в момент использования.

5. Полученная информация в дальнейшем используется для обналичивания денежных средств, находящихся на счетах граждан. При этом способы обналичивания могут быть различными: покупка товаров на сайтах в сети Интернет (похищенные данные с пластиковых карт вносятся на страницы интернет-магазинов); перевод денежных средств на «электронные кошельки»; перечисление денег на расчетные счета подконтрольных фирм-однодневок; создание дубликатов пластиковых карт, информация о которых получена с помощью скиммера (так называемый «белый пластик»). При этом для осуществления операций по карте вводится ПИН-код владельца, снятый на видеокамеру или полученный при помощи накладки, имитирующей клавиатуру.

На практике преступления, связанные с использованием скимминговое оборудования, квалифицируются как кража по совокупности со ст. 183 и (или) ст. 272 УК РФ.

Федеральным законом от 29 ноября 2012 г. № 207-ФЗ Уголовный кодекс России дополнен ст. 159.3, предусматривающей ответственность за хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации.

Уголовная ответственность по этой статье наступает только в тех случаях, когда лицо путем обмана или злоупотребления доверием ввело в заблуждение уполномоченного работника кредитной, торговой или иной организации[4].

Таким образом, хищение денежных средств с банковских счетов держателей пластиковых карт с помощью скимминговое оборудования не может квалифицироваться по ст. 159.3 УК РФ.

Более того, следует отметить, что в настоящее время сложилась неопределенность относительно существования специальных составов мошенничества (ст. 159.1–159.6 УК РФ), обусловленная признанием Конституционным Судом РФ отдельных положений ст. 159.4 УК РФ, не соответствующими Конституции РФ с указанием федеральному законодателю на необходимость внесения соответствующих изменений в

[4] Комментарий к Уголовному кодексу Российской Федерации : науч.-практ. (постатейный) / Н. И. Ветров [и др.] ; под ред. С. В. Дьякова, Н. Г. Кадникова. 2-е изд., перераб. и доп. М., 2013. С. 378.

Уголовный кодекс России в шестимесячный срок со дня провозглашения указанного постановления. По истечении указанного срока и при отсутствии изменений ст. 159.4 УК РФ будет признана утратившей силу[5].

Следует отметить, что проблемы несогласованности санкций, а также границ крупного и особо крупного размеров ущерба в ст. 159.4 УК РФ по сравнению с основным составом (ст. 159 УК РФ), отмеченные Конституционным Судом России, характерны и для мошенничества с использованием платежных карт.

На несовершенство специальных составов мошенничеств неоднократно указывалось учеными[6].

Несмотря на то что лиц, совершающих преступления с использованием скимминговых устройств, в случае задержания удается привлечь к уголовной ответственности, действия лиц, изготовивших или сбывших названное оборудование, в настоящее время нельзя признать преступными. Данное обстоятельство приводит к тому, что при расследовании хищений денежных средств с банковских счетов правоохранительные органы не выявляют производителей и каналы сбыта скимминговых оборудования.

Распространение хищений с использованием специальных технических устройств приводит к необходимости внесения изменений в действующее уголовное законодательство с целью недопущения роста количества таких преступлений.

В Государственной Думе России на рассмотрении находится законопроект «О внесении изменений в статьи 187 и 272 Уголовного кодекса Российской Федерации»[7], в соответствии с которым ч. 2 ст. 272 УК РФ предлагается отнести к категории преступлений средней тяжести, предусмотрев наказание в виде лишения свободы на срок до четырех лет, а диспозицию ч. 1 ст. 187 изложить в новой редакции:

«Статья 187. Неправомерное изготовление или сбыт средств платежей

1. Изготовление в целях сбыта и (или) сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов

[5] См. подробнее: По делу о проверке конституционности положений статьи 159.4 Уголовного кодекса Российской Федерации в связи с запросом Салехардского городского суда Ямало-Ненецкого автономного округа : постановление Конституционного Суда РФ от 11 декабря 2014 г. № 32-П / URL: http://www.rg.ru/2014/12/24/ks-uk-dok.html

[6] См., например: *Гаухман Л.* Мошенничество : новеллы уголовного законодательства // Уголовное право. 2013. № 3. С. 25–27 ; *Егорова Н. А.* Ответственность за «служебные» мошенничества : необходимость новых правовых подходов // Рос. юстиция. 2014. № 8. С. 19–22 ; *Тюнин В. И.* «Реструктуризация» уголовного законодательства об ответственности за мошенничество // Уголовное право. 2013. № 2. С. 35–41 ; *Александрова И. А.* Новое уголовное законодательство о мошенничестве // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2013. № 21. С. 54–62.

[7] О внесении изменений в статьи 187 и 272 Уголовного кодекса Российской Федерации : проект федер. закона № 537952-6. URL: http://oduma.org/StateDumaBills/View/191

или средств оплаты (за исключением случаев, предусмотренных ст. 186 УК РФ), а также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств, – …».

В случае принятия указанного законопроекта у правоохранителей появится больше возможностей для противодействия рассматриваемым преступлениям.

Однако в законопроекте вновь не уделено внимания повышенному уровню общественной опасности хищений, совершаемых с использованием специальных технических средств, обусловленному относительной доступностью скимминговогo оборудования, простотой его использования и возможностью хищения значительных объемов денежных средств за сравнительно короткий промежуток времени.

Так, К., совместно с не установленным следствием лицом с целью завладения информацией о расчетных счетах физических лиц, а также компьютерной информацией, достаточной для изготовления дубликатов банковских карт, осуществил установку на банкомат «№» специального технического оборудования для несанкционированного считывания информации с банковских карт. В период с 8 часов 45 минут по 18 часов 45 минут получил доступ к информации со 190 банковских карт с лимитом денежных средств в общей сумме 2 990 607,52 рублей[8].

Как выход из сложившейся ситуации некоторые авторы предлагают дополнить УК РФ специальной нормой о краже, предусматривающей ответственность за хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу расчетной или иной платежной карты[9].

С указанным предложением нельзя полностью согласиться. Безусловно, рост числа хищений с использованием скимминговогo оборудования влечет необходимость принятия уголовно-правовых мер реагирования. Однако установление уголовной ответственности за кражу, совершаемую с использованием технических устройств путем выделения из состава кражи специальной нормы, приведет к излишней дифференциации ответственности и избыточности уголовного закона.

Представляется целесообразным включение действий, связанных с использованием электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного считывания и передачи информации о банковской карте и осуществления приема, выдачи, перевода денежных средств, в качестве квалифицирующего признака в ст. 158 УК РФ.

[8] Приговор Рузского районного суда Московской области от 28 августа 2014 г. № 1-115/2014. URL: http://sudact.ru/regular/doc

[9] См.: *Боровых Л. В., Корепанова Е. А.* Проблема квалификации хищения с использованием банковских карт // Рос. юрид. журнал. 2014. № 2. С. 87.

С учетом изложенного предлагаем дополнить ч. 2 ст. 158 УК РФ пунктом «д» следующего содержания (редакция примерная):

«д) с использованием электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного доступа к информации о банковской карте и осуществления приема, выдачи, перевода денежных средств».

Волгоградская академия МВД России

Лихолетов А. А., кандидат юридических наук, старший преподаватель кафедры организации следственной работы

E-mail: A.Likholetov@mail.ru

Тел.: 8-927-517-38-17

Volgograd Academy of the Russian Ministry of Internal Affairs

Likholetov A. A., Candidate of Legal Sciences, Senior Lecturer of the Investigative Activities Department

E-mail: A.Likholetov@mail.ru

Tel.: 8-927-517-38-17