УДК 336.717.1

# ПРОБЛЕМЫ БЕЗОПАСНОСТИ РАСЧЕТОВ ПЛАСТИКОВЫМИ КАРТАМИ

**Смольянинова Е.Н., Духанина Н.А., Дашидондокова А.Ц.**
*ГОУ ВПО «Дальневосточный федеральный университет», Владивосток, e-mail: Ariguna666@mail.ru*

Проблема информационной безопасности особенно актуальна в современных условиях на фоне стремительного развития карточных технологий и перехода на автоматизированные системы расчета. Сегодня банки вынуждены сами защищаться от всевозможных рисков как криминального, так и некриминального характера. Сложность защиты информации определяется не только огромными массивами обрабатываемых данных и изощренностью средств, применяемых злоумышленниками для доступа к ним. Она характеризуется еще и тем, что банки, являясь частью единой финансовой системы государства, должны соответствовать требованиям безопасности. Накопленный международный опыт по внедрению программ карточных платежных систем в разных странах показал, что развитие преступных методов и способов подчиняется определенным закономерностям, а преступность в сфере пластиковых карт развивается параллельно с самой индустрией карт. Поэтому для кредитных организаций обеспечение защиты информации является первостепенной задачей, которая минимизирует не только потерю денежных средств, но и репутационные риски банка.

**Ключевые слова: мошенничество, дистанционное банковское обслуживание, пластиковые карты, скимминг, инжиниринг, информационная безопасность**

# SECURITY PROBLEMS OF PAYMENTS WITH PLASTIC CARDS

**Smolyaninova E.N., Dukhanina N.A., Dashidondokova A.T.**
*Far Eastern Federal University, Vladivostok, e-mail: Ariguna666@mail.ru*

The problem of information security is particularly relevant in the present conditions on the back of the rapid development of card technologies and switch to automated accounting systems. Nowadays banks have to defend themselves from various risks as criminal and non-criminal ones. The complication of information security is not only defined by a huge amount of processed data and the sophistication of methods used by hackers to access to them. It is also characterized by the fact that banks being a part of a unified financial system of the State, must comply with the demand of safety requirements. International experience aimed at the implementation of programs of using card payment systems in different countries has shown that the development of criminal methods and ways comply with certain laws and crime connecting with plastic cards at the same time develops by the industry of cards itself. Therefore, guarantee of information security for credit unions is a top priority that not only minimizes the loss of money, but also minimizes reputational risks of the bank.

**Keywords: fraud, remote banking, credit cards, skimming, engineering, information security**

В последнее время тема информационной безопасности в контексте дистанционных банковских услуг затрагивается все чаще. Причин для поднятия вопросов защиты множество: антикризисные меры по сокращению штатов, убытки от мошеннических операций, сокращение репутационных рисков в нестабильных экономических условиях и стремление расширить клиентскую базу. Но гораздо важнее вопрос об эффективной реализации, прозрачной для банка и удобной для пользователей.

Целью исследования стала попытка разобраться в том, как обеспечить систему защиты электронных банковских услуг, соблюдая принцип разумной достаточности.

Исходя из цели, в работе были сформулированы и решены следующие задачи:

1. Изучить статистические данные о видах мошеннических операций, характерных для российского рынка банковских услуг.
2. Рассмотреть основные виды мошенничества.
3. Выявить основные методы защиты информации.
4. Предложить пути совершенствования системы информационной безопасности.

При написании статьи были использованы общенаучные методы: эмпирического исследования, теоретического познания, общелогические методы и приемы; а также методы: системного анализа, метод сравнений и аналогий, метод обобщений и др.

Мошенничество при расчетах пластиковыми картами стало особенно быстро развиваться последние 10 лет. Однако в 2013 г. оно достигло своего пика. На Великобританию и Францию пришлось 62% всех мошеннических операций. Если добавить Испанию, Германию и Россию, то получится уже 80% всех преступлений мира в области пластиковых карт [6].

В 2013 году совокупные убытки от мошенничества с картами в 19 европейских странах составили 1,55 миллиарда евро.

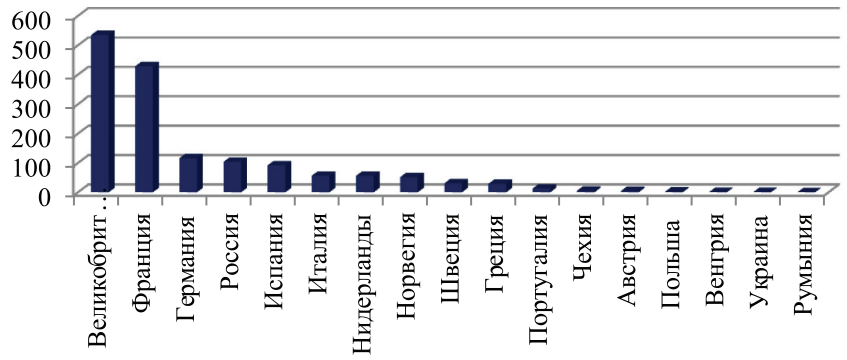


*Рис. 1. Убытки от карточного мошенничества в 2013 г., млн евро*

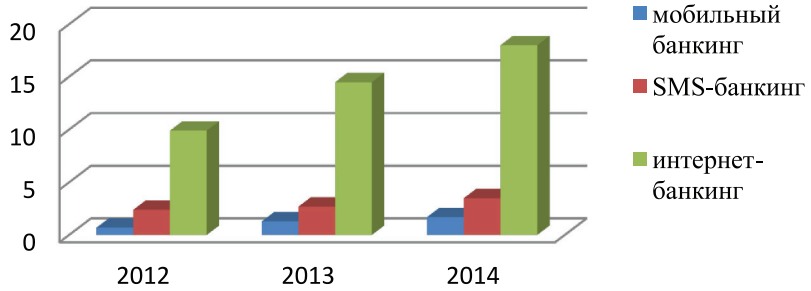


*Рис. 2. Количество пользователей среди сервисов ДБО, млн чел.*

Если говорить о России, то рынок пластиковых карт здесь расширяется быстрыми темпами, следовательно, растет круг потенциальных мошенников. С распространением услуги интернет-банкинга ситуация только усугубилась. За последние три года только количество пользователей сервисами ДБО, в частности мобильного, интернет- и SMS-банкинга, выросло почти в два раза (рис. 2).

К тому же процесс совершения преступлений облегчает доступность производственного оборудования для изготовления пластиковых карт, увеличение количества специалистов в области компьютерной техники и программного обеспечения.

По темпам роста убытков от мошеннических операций с картами в 2013 году Россия заняла первое место в Европе. Объем этих потерь вырос на 27,6 % по сравнению с показателем годом ранее и, соответственно, в 10 раз в сопоставлении с данными 2006 года, и на 365 % – 2008 года. По объему потерь, увеличившихся на 22,5 млн евро и достигших 104,1 млн евро в 2013 г., Россия находится на четвертом месте среди 19 европейских стран. Ее опережают: Великобритания (534,9 млн евро), Франция (428,9 млн евро) и Германия (116,3 млн евро).

Для эффективного предотвращения мошеннических операций необходимо учитывать российскую специфику: низкая техническая подготовка клиента, граничащую с технической и финансовой безграмотностью; правовой нигилизм и халатность клиентов.

По имеющимся оценкам, из общего числа фактов, мошенничество в сфере электронных платежей возможно из-за потери данных. Утечка информации из финансово-кредитной сферы происходит с помощью подкупа, шантажа, переманивания служащих в 43 % случаях, копирования программного продукта – 24 %, проникновения в компьютер – 18 %, кражи документации – 10 %, подслушивания телефонных переговоров – 5 % [1].

Сегодня до 80 % обращений через интернет-сайт МВД РФ посвящены мошенничеству при покупке товаров через социальные сети и интернет-магазины. Также продолжает расти разнообразие вредоносных программ для мобильных

устройств. Целью злоумышленников может быть получение доступа к мобильному банку жертвы и к конфиденциальным сведениям.

В 2014 году специалисты отмечают стремительное развитие вредоносных программ для банкоматов. Они имеют широкий функционал – от получения данных банковских карт до снятия наличных денег и несанкционированного проникновения во внутреннюю сеть банка. Не теряет популярность и «классический» скимминг.

Обобщенные данные в области разработки безопасных приложений и оценки уязвимостей показывают следующую статистику:

● в 2014 году злоумышленник оказался способен получить доступ к узлам внутренней сети субъекта национальной платежной системы в 9 случаях из 10, а в 2012 году аналогичное соотношение составляло 7 из 10;

● для проведения атаки в 82 % случаев достаточно иметь среднюю или низкую квалификацию;

● уязвимости web-приложений обнаружены в 93 % исследованных систем;

● причинами возникновения уязвимостей в АБС являются ошибки (недостатки) разработки (23 %) и отсутствие эффективных защитных механизмов (43 %);

● уязвимости приложений – один из распространенных факторов, способствующих проникновению в корпоративные сети [2].

В настоящее время известно уже около 30 приемов мошеннических действий, которые можно условно разделить на три группы.

Во-первых, это профессиональное мошенничество с применением поддельных устройств и пластиковых карт. Примерами могут служить скимминг (накладная клавиатура на банкомат) и использование фантомных банкоматов (речь идет о банкоматах, которые только с виду кажутся таковыми: как правило, используются банкоматы несуществующих банков). Наиболее распространенным видом мошенничества является изготовление поддельных банковских карт, которым занимаются организованные преступные группы в сговоре с работниками организаций, осуществляющих расчеты с помощью карт. Набирает обороты такой вид мошенничества, как «магазинный скимминг», когда данные карты могут быть считаны и зафиксированы специальным ручным скиммером при оплате покупок в магазине или ресторане, а впоследствии использованы для хищения денег.

Во-вторых, это мошенничество в системе ДБО, направленное на похищение секретной информации о счете клиента с помощью атак программ-шпионов. Преступники используют троянские программы на компьютере и мобильном телефоне пользователя ДБО, фишинговые сайты, перевыпущенные SIM-карты. Разновидностей «шпионов» в системе интернет-банкинга становится все больше, следовательно, растет количество инцидентов, но банки, стремясь сохранить репутацию, не предпринимают решительных действий, а просто покрывают убытки за свой счет. Фишинг-атаки как вид мошенничества признаются проблемой номер один среди внешних угроз банковской безопасности (согласно опросам руководителей служб безопасности ста ведущих международных финансовых институтов – 46 %). Кроме того, существует и такой тип атаки, как «человек посередине» (man in the middle) [3]. Суть состоит в том, что злоумышленник проникает в информационный обмен между пользователем и сервером, «представляясь» пользователю сервером, и наоборот.

В-третьих, наиболее распространенными являются виды мошенничества, связанные с утечкой секретной информации непосредственно от самого клиента в результате его беспечности.

Рассмотрим основные приемы мошеннических действий, следующие из российской специфики. Самый распространенный способ – халатность и правовой нигилизм клиентов, которые разглашают PIN-код путем его записи на карту или путем так называемого «дружественного мошенничества» – разглашения PIN-кода членам семьи, близким друзьям, коллегам. Еще пример – когда из-за фактора технической неграмотности клиенты впадают в панику при получении SMS-сообщения «Ваша банковская карта заблокирована» со всеми вытекающими для них последствиями.

Также распространенной схемой является помощь прохожего, называемая «ливанской петлей». Суть в том, что при блокировке карты банкоматом на помощь клиенту приходит «добрый» мошенник, изображая опытного пользователя банкоматов [5].

Но несмотря на такое разнообразие мошеннических схем, большая часть краж обусловлена человеческим фактором. Согласно статистике, на 10 инцидентов в области информационной безопасности только 1 приходится на внешнего «хакера», ещё 1 – на озлобленного, обиженного

сотрудника и остальные 8 – на нерадивых, безответственных и плохо обученных сотрудников предприятия [4].

Эффективность обеспечения безопасности по отношению к пластиковым платежным средствам может быть повышена путем технологических и организационных методов.

К первым относятся совершенствование выпуска карт и повышение уровня безопасности использования банкоматов. В России банкоматы широко используются для снятия наличных денег, а также в качестве платежных терминалов, в отличие от европейских стран. Учитывая это, банкам необходимо прилагать наибольшие усилия в противодействии использования мошенниками банкоматов в качестве технических средств получения/дублирования секретной информации (ее носителя).

Банкам следует совершенствовать механизмы защиты банкоматов: периодически изменять настройки, увеличивать количество штатных видеокамер, устанавливать банкоматы исключительно в людных общественных местах и крупных учреждениях. Также можно вводить ограничения на суммы, снимаемые в банкомате клиентами по зарплатным проектам, в зависимости от месторасположения банкомата.

Если говорить о совершенствовании информационных систем, можно выделить следующие требования:

1. Построение модели и ее параметров для выявления подозрительных операций. Принятие решение об отклонении операции и занесении карты в стоп-лист.

2. Возможность управления (блокировка) подозрительными точками обслуживания (банкоматы, терминалы, точки продаж, торговцы).

3. Статистический анализ истории операций. Выявление карт, которые были обслужены в подозрительных точках.

4. Оповещение операторов системы о фактах мошенничества для принятия соответствующих мер (SMS и E-mail-информирование, генерация оповещений) [1].

Банки активно развивают свои системы безопасности. С технической точки зрения они имеют достаточно возможностей для построения надёжной системы информационной защиты. Но главный недостаток технологий в том, что ни одно устройство не обходится без человека. Не секрет, что львиная доля мошенничества в ДБО приходится на социальный инжиниринг, т.е. мошеннические схемы, в основе которых лежит невнимательность и доверчивость клиента, его неосведомлённость, пренебрежение правилами безопасной работы в интернете.

Именно поэтому донесение до клиента необходимой информации и приучение его к соблюдению этих правил не менее важно, чем совершенствование и внедрение новых технологий обеспечения безопасности в ДБО. Данная проблема более актуальна, чем нехватка на рынке IT-решений. Не менее насущная проблема – недостаток законодательной базы в части борьбы с мошенничеством – недостаток в актах, регулирующих ответственность за мошеннические действия, формирование доказательной базы.

Отметим наиболее существенные проблемы предупреждения мошенничества, совершаемого с использованием пластиковых карт:

– умалчивание коммерческими структурами информации о совершении мошенничества в целях сохранения престижа и видимости его благополучности перед клиентами;

– отсутствие слаженной кооперации и взаимодействия служб безопасности банков и правоохранительных органов (МВД, ФСБ, СК, прокуратуры), их недостаточная активность [1].

Важно отметить эффективность организационных методов защиты, о которых забывают в погоне за техническими средствами. Необходимо организовать грамотное реагирование на сообщения держателей карт о неправомерных списаниях денежных средств, вести правильный учет и анализ этих сообщений. В раздел организационных методов защиты также входит организация защиты от собственных сотрудников. Поэтому банкам необходимо уделять внимание обучению и переподготовке персонала в области информационных технологий.

Важной задачей является определение оптимальных параметров системы, позволяющих минимизировать риск банка – опыт и интуиция оператора может работать эффективней компьютерной системы и сотрудника службы безопасности. Для повышения эффективности защитных механизмов следует проводить работу и с владельцами карт, ведь их внимательность – главный способ избежать мошенничества.

В заключение можно отметить, что качество обеспечения безопасности банковской системы зависит от уровня «честности» участников финансовых отношений, эффективности работы службы

безопасности кредитных организаций, профессионализма сотрудников правоохранительных органов, занимающихся предупреждением и выявлением мошенничества в банковской сфере, а также объема разъяснительной работы, проводимой с держателями легитимных пластиковых карт.

Перед банком и клиентом стоят общие цели, они решают одни и те же задачи. Развитие информационных технологий требует развития взаимодействия и совершенствования системы банк – клиент – банк.

### Список литературы

1. Белянина Н.В, Кожин Е.В. Информационная система определения мошенничества по платежным картам в режиме реального времени // Сервис в России и за рубежом. Вып. 2 – РГУТиС. – С. 19–32.

2. Выборнов А. Устранение уязвимостей // BIS journal. – 2014. – № 4.

3. Евдокимов Д. Безопасность мобильного банкинга: возможность реализации атаки «MitM». – 2014.

4. Крутов С., Тушканова О. Управление рисков финансовых организаций при дистанционном обслуживании клиентов // BIS journal. – 2014. – № 4.

5. Смольянинова Е.Н., Фурманов Д.В. Проблемы безопасности расчетов при использовании пластиковых карт //Актуальные вопросы экономических наук. – 2012. – С. 46–50.

6. Эволюция карточного мошенничества в Европе 2013. [Электронный ресурс]. URL: http://www.fico.com/landing/fraudeurope2013.

### References

1. Beljanina N.V, Kozhin E.V. Servis v Rossii i za rubezhom – Service in Russia and abroad, edition 2, pp. 19–32.

2. Vybornov A. BIS journal, 2014, no. 4.

3. Evdokimov D. Bezopasnost mobilnogo bankinga: vozmozhnost realizacii ataki «MitM» – Security of mobile banking: the feasibility of the attack «MitM», 2014.

4. Krutov S., Tushkanova O. BIS journal, 2014, no. 4.

5. Smoljaninova E.N., Furmanov D.V. Aktualnye voprosy jekonomicheskih nauk – Topical issues of economic sciences, 2012, pp. 46–50.

6. Jevoljucija Kartochnogo Moshennichestva V Evrope 2013 (Evolution of card fraud in Europe in 2013) Available at: http://www.fico.com/landing/fraudeurope2013/ (accessed 22 March 2015).

**Рецензенты:**

Вотинцева Л.И., д.э.н., профессор, ФГОУ ВПО «Дальневосточный федеральный университет», г. Владивосток;

Черная И.П., д.э.н., профессор, проректор по учебно-воспитательной работе, ГБОУ ВПО «Тихоокеанский государственный медицинский университет» Министерства здравоохранения Российской Федерации, г. Владивосток.