УДК 336.717

С. В. Буйзанова,
Л. В. Татаринова

Мошенничество в дистанционном банковском обслуживании

На сегодняшний день дистанционное банковское обслуживание (далее – ДБО) прочно вошло в нашу жизнь, и является ее неотъемлемой частью. Для банка своевременное и эффективное использование информационных технологий дает возможность привлечь новых и удержать старых клиентов. Одно из преимуществ ДБО, является его мобильность, клиент может получить доступ к своему к счету без непосредственного визита в банк. С ростом популярности ДБО растет уровень мошенничества. В данной статье рассмотрены основные виды мошенничества с использованием ДБО и способы борьбы с ними.

Ключевые слова: дистанционное банковское обслуживание, мошенничество, интернет банкинг.

S. V. Buizanova,
L. V. Tatarinova

FRAUD REMOTE BANKING

Today, remote banking services is firmly established in our lives, and is its integral part. For the bank, the timely and effective use of information technology makes it possible to attract new and retain old customers. One of the advantages of remote banking, is its portability, the client can get access to your account without a direct visit to the bank. With the growing popularity of remote banking increases the level of fraud. This article describes the main types of fraud using remote banking and ways to combat them.

Keywords: Remote banking, Internet banking, fraud.

В научной литературе ДБО чаще всего рассматривается, как предоставление банковских услуг на расстоянии. Так, Г. Н. Белоглазова, Л. П. Кроливецкая трактуют дистанционное банковское обслуживание как: «предоставление возможности клиентам совершать банковские операции, не приходя в банк, с использованием различных каналов телекоммуникаций» [3, с. 254]. А. М. Тавасиев определяет ДБО как предоставление банковских продуктов (оказание банковских услуг) на расстоянии, вне офиса банка, без непосредственного контакта клиента с сотрудниками банка [9, с. 146]. В. В.

Трофимов дополняет данные определения и говорит о том, что дистанционно могут предоставляться, не только банковские услуги, но и банковские продукты. Исходя из этого, им предлагается следующее определение: ДБО – это оказание банковских услуг (предоставление банковских продуктов) на расстоянии, без посещения клиентами офиса банка, без непосредственного контакта с сотрудниками банка – из дома (так называемый «home-banking»), офиса, автомобиля и т.д.» [11, с. 54]. В отличие от вышеперечисленных авторов А. Ванин и К. Сумманен под ДБО понимают не просто предоставление банковских услуг, а технологии, с помощью которых проведение банковских операций не требует визита клиента в банк [4, с. 46]. В качестве каналов связи могут использоваться телефонная и мобильная связь, связь посредством сетей (локальных либо интернета), технические устройства (банкоматы и терминалы). В зависимости от выбранного канала связи О. М. Маркова выделяет следующие формы дистанционного банковского обслуживания [7, с. 435]:

– ПС-банкинг (PC-Banking) предполагает установку специального программного обеспечения на компьютер клиента для связи с банком;

– интернет-банкинг (Internet-banking) предполагает использовать для осуществления доступа к банковским операциям интернет-браузер;

– телебанкинг или телефонный банкинг (phone-banking) для управления счетом используются возможности телефонов с функцией тонального набора номера и факса;

– мобильный банкинг (mobile-banking) – обмен информацией между клиентом и банком осуществляется с использованием либо мобильного телефона через SMS-сообщения либо посредством мобильного-интернета (SMS-banking,
WAP-banking, GSM-banking);

– банковское обслуживание через банкоматы (ATM-banking) и терминалы самообслуживания.

Е. П. Жарковская выделяет 4 разновидности дистанционного банковского обслуживания [6, с. 423]:

– PC – банкинг, подразумевает доступ к счету с помощью персонального компьютера, осуществляемый посредством прямого модемного соединения с банковской сетью, а не через интернет. При этом используя специальное банковское программное обеспечение;

– видео банкинг, это система интерактивного общения с персоналом в банке, своего рода видеоконференция;

– телефонный банкинг, предоставление банковских услуг с пи помощи мобильного телефона;

– интернет банкинг, предоставление клиенту прямого доступа к банковскому счету через Интернет с помощью компьютера с использованием обычного браузера.

По субъектам обслуживания (клиентской базе) ДБО подразделяются на две группы [8, с. 9]:

– системы, обслуживающие корпоративный сектор, т.е. юридических лиц и индивидуальных предпринимателей;

– системы, используемые частными (физическими) лицами.

По данным аналитического агентства Markswebb Rank & Report на 2015 год рост аудитории интернет-банкинга фактически остановился. В основе исследования лежит онлайн-опрос 3 тыс. интернет-пользователей в возрасте от 18 до 64 лет, выходящих в Сеть не реже одного раза в месяц с компьютера или ноутбука. Исследователи оценивают активность респондентов в части использования интернет-банков, банковских мобильных приложений и других каналов дистанционного банковского обслуживания, электронных денег, совершения онлайн-покупок и применения различных способов оплаты услуг в сети. Как показывают результаты опроса, 97 % интернет-пользователей в стране являются клиентами российских банков как частные лица, то есть имеют хотя бы одну банковскую карту, счет, вклад или непогашенный кредит. 75 % банковских клиентов, регулярно выходящих в Интернет, используют хотя бы один канал дистанционного доступа к своим картам, счетам и другим банковским продуктам. Хотя бы одним интернет-банком пользуются 35,3 млн человек, или 64,5 % всех российских интернет-пользователей. Количество пользователей интернет-банкинга в России за год не изменилось – рост аудитории интернет-банкинга, наблюдавшийся в предыдущие годы, фактически остановился. Наибольшее количество клиентов имеет интернет-банк «Сбербанк Онлайн» – им пользуются более 28 млн человек, или почти 82 % всех пользователей интернет-банкинга в Российской Федерации. Второе, третье и четвертое места по количеству пользователей занимают «ВТБ24-Онлайн», «Альфа-Клик» и интернет-банк «Тинькофф» – сервисы ВТБ 24, Альфа-Банка и Тинькофф Банка, которыми пользуются 9, 7 и 6 % всех пользователей интернет-банкинга в России соответственно[1].

Любая система ДБО характеризуется большим количеством банковских рисков в силу наличия неконтролируемой банком технологической среды и

[1] Третья волна ежегодного исследования пользователей электронных финансовых и платежных сервисов в России (E-Finance User Index 2016), проводимого агентством Markswebb Rank & Report [Электронный ресурс]. – Режим доступа: http://markswebb.ru/e-finance/e-finance-user-index-2016.

конечных пользователей (клиентов) [2, с. 235]. В. А. Таран связывает использование ДБО с такими банковскими рисками [10, с. 2]:

– операционный риск;

– правовой риск;

– стратегический риск;

– риск потери деловой репутации; – риск ликвидности.

Ю. Н. Юденков связывает интернет банкинг с такими рисками, как кредитный, процентный, фондовый, валютный, стратегический, операционный, репутационный, правовой риск, при этом подчеркивая, что указанные виды не являются исчерпывающими [12, с. 84].

Защита клиентов дистанционного банковского обслуживания всегда была проблемой нетривиальной и потому интересной для профильных специалистов. И дело здесь не в защите систем ДБО банка, которая, по сути, ничем не отличается от обеспечения безопасности любого дистанционного доступа из недоверенной среды, имеет на вооружении целый ряд «лучших практик» и иногда даже попадает под действие регламентирующих стандартов, таких как СТО БР и PCI DSS. Нетривиальным остается одно – защита самих клиентских мест ДБО. Компьютеры клиентов – это внешняя по отношению к системам банка территория, она не контролируется информационными технологиями – и информационной безопасностью банка. Организационные меры здесь в большинстве случаев не действуют – клиент всегда прав. Можно рекомендовать клиенту поставить на рабочее место, к примеру, антивирусное программное обеспечение, но реально работающих рычагов воздействия, гарантирующих выполнение этих рекомендаций, нет. Клиентские места при этом – самая массовая часть системы ДБО. Несмотря на то, что основной ущерб в случае нарушения информационной безопасности на клиентском месте несет именно пользователь системы, банкам тоже достается их «порция» – пока это только репутационные риски, миграция клиентской базы, участие в длительных расследованиях и разбирательствах. При этом число атак на клиентские места в последнее время все возрастает. В этой сфере традиционно лидируют составители вредоносного программного обеспечения, как способные на самую массовую атаку [2, с. 236].

К наиболее распространенным способам атак на системы ДБО относятся [8, с. 5]:

– вредоносное ПО (трояны, клиенты бот-сетей и т.д.); – фишинг;

– использование атак типа Man-in-the-Middle для проведения подложных транзакций;

– внутренние атаки (для корпоративных клиентов).

Кроме этого, выделим такой вид мошенничества, как «Звонок от банка» или социальная инженерия, клиенту приходит смс оповещение, что с его счета снята некоторая сумма денег, для получения более подробной информации необходимо позвонить по номеру телефона указанному в смс. Социальная инженерия (45 %) занимает первое место в общем распределении мошеннической активности. Методы социальной инженерии используются злоумышленниками при распространении информации, побуждающей клиента сообщать информацию, необходимую для осуществления переводов денежных средств от его имени, в том числе аутентификационную информацию. Для сравнения в 2013 году наиболее популярным видом мошенничества являлся скимминг[2] т. е. кража данных с помощью специального считывающего устройства, по данным на конец 2015 года доля скимминга составляет 13 %. Хищения с помощью вредоносного ПО составляет 25 %.

Как следует из обзора Банка России о несанкционированных переводах денежных средств за 2015 год мошенниками было проведено более 260 тыс. транзакций по выпущенным российскими банками пластиковым картам, общая сумма ущерба составила около 1,14 млрд р.[3] По сравнению с 2014 годом объем несанкционированных транзакций сократился на 27 %, при этом доля мошеннических транзакций в общем объеме операций по картам постепенно снижалась на протяжении всего 2015 года. В частности, благодаря усилению мер безопасности мошенники практически лишились возможности снимать деньги с карточек в пунктах выдачи наличных: если во втором квартале 2014 года преступникам удалось получить таким образом более 24 млн р., то в апреле – июне 2015 года – только 480 тыс. р.[4]

Заметно сократилось и число случаев, когда преступникам удалось получить деньги в банкомате. В наиболее успешном для них первом квартале 2014 года мошенникам удалось похитить таким образом более 202 млн р., в четвертом квартале 2015 года объем хищений через банкоматы сократился до 59 млн р. В Банке России связывают такую динамику с обязательным переходом банков-эмитентов на карты, оснащенные чипами. Благодаря такому подходу мошенникам куда реже удается получить деньги по поддельной карте – доля таких операций в общем объеме мошеннических транзакций сократилась с 24 % в начале 2014 года до 8 % в конце 2015 года. Одновременно в полтора раза уменьшилось количество операций, проведенных мошенниками с помощью украденных у законных владельцев

---

[2] Скимминг [Электронный ресурс]. – Режим доступа: http://www.banki.ru/wikibank/skimming.

[3] Обзор о несанкционированных переводах денежных средств [Электронный ресурс]. – Режим доступа: http://cbr.ru.

[4] Мошенники стали чаще красть деньги россиян с помощью интернет-банков [Электронный ресурс]. – Режим доступа: http://www.rbc.ru/finances/01/04/2016/56fe4b059a79479e78cedbf2.

или потерянных ими пластиковых карт. В то же время доля операций, проведенных мошенниками через интернет, с использованием реквизитов чужого «пластика» выросла с 65 до 84 %. В 2015 году было совершено более 190 тыс. так называемых CNP-транзакций, то есть операций, проведенных онлайн или по телефону, без физического предъявления банковской карты (Card not present transaction). Объем таких транзакций мошенников составил половину всех несанкционированных операций по картам.

Таким образом, в 2015 году отмечалась тенденция к перемещению интересов «карточных» мошенников из контактной инфраструктуры (банкоматы, материальные носители платежных карт) в более технологичную инфраструктуру дистанционного доступа (системы дистанционного банковского обслуживания, электронные кошельки, интернет – и мобильные транзакции).

В 2015 году многократно выросло число случаев хищения средств россиян с использованием систем дистанционного банковского обслуживания (ДБО, интернет-банк, SMS-банкинг, телефонный банкинг). Если за последние три месяца 2014 года было проведено лишь около 1,6 тыс. таких транзакций, то в четвертом квартале 2015 года их число перевалило за 15 тыс. При этом в подавляющем большинстве случаев (92 %) остановить списание денег со счетов физических лиц не удалось, о том, что та или иная операция проведена мошенниками, банки в девяти случаях из десяти узнают только после жалобы клиента[5].

Активизацию карточных мошенников в сфере ДБО и CNP-транзакций связывают с общим ростом популярности интернет-сервисов оплаты товаров и услуг и платежей с мобильных устройств, а также тем, что мошенникам нет нужды приобретать специальное оборудование и навыки – всю необходимую информацию можно получить у законных владельцев карт с помощью «методов социальной инженерии». Чаще всего в 2015 году получившие доступ к системам ДБО мошенники похищали со счетов россиян достаточно скромные суммы – от 1 до 10 тыс. р. (примерно 9,7 тыс. раз) и от 10 до 50 тыс. р. (почти 13,7 тыс. раз). Однако как минимум однажды преступникам удалось увести с чужого счета более 20 млн р.[6]

В связи с изменением методов карточных мошенников Банк России рекомендовал кредитным организациям активнее внедрять технологии, направленные на подтверждение дистанционно проводимых операций, использовать системы фрод-мониторинга, а также информировать клиентов о рисках использования платежных карт в интернете.

---

[5] Обзор о несанкционированных переводах денежных средств [Электронный ресурс]. – Режим доступа: http://cbr.ru/psystem/P-sys/survey_2015.pdf.

[6] Обзор о несанкционированных переводах денежных средств [Электронный ресурс]. – Режим доступа: http://cbr.ru/psystem/P-sys/survey_2015.pdf.

Полностью безопасный интернет-банкинг невозможен. ДБО – это процесс, а абсолютно безопасных процессов не бывает, некоторый риск присутствует всегда. Однако безопасность можно рассматривать как состояние, при котором уровень риска использования сервиса приемлем как для пользователя, так и для владельца. Качество предоставляемой услуги ДБО для банков – это вопрос привлечения клиентов. Качество определяется, прежде всего, объемом предоставляемых услуг, удобством использования, доступностью и защищенностью. Именно защищенность становится все более весомым критерием при выборе системы ДБО и в немалой степени влияет на выбор банка [1, с. 293].

Количество угроз в сфере ДБО только растет, и появляются новые типы атак. Мошенники атакуют не только счета клиентов банка, но и сами кредитные организации. Отметим, что некоторые из этих угроз еще не существовали год–два назад, с ростом рынка ДБО и банковских интернет-услуг растет и привлекательность атак на данные услуги. Соответственно, растут потенциальные и реальные потери клиентов, а со следующего года – и реальные денежные потери банков. При этом существует достаточно большой выбор средств и методов для защиты ДБО. Если говорить об их внедрении для массового использования, особенно для обслуживания физических лиц через средства webбанкинга, можно констатировать, что немногие решения проходят ценовую стоимость и возможности масштабирования. В то же время сложившаяся на текущий момент ситуация с развитием киберпреступности и низкий процент раскрываемости подобных преступлений доказывают, что использование банками подобных технологий для защиты своих клиентов более чем оправдано [1, с. 2]. Необходимость выживания в условиях жесткой конкуренции в банковском секторе диктует банкам свои условия, особенно на фоне возросшей культуры потребления физических лиц. Клиентам уже мало просто иметь возможность получить тот или иной продукт – сейчас их интересует качество предоставляемой услуги и временные затраты на ее получение. В данной ситуации преимущество получают банки, предоставляющие своим клиентам услуги по дистанционному банковскому обслуживанию. В конкурентной борьбе победят те банки, которые полностью перестроят свою деятельность в соответствии с новыми требованиями банковского бизнеса и современными информационными технологиями.

Список использованной литературы 1. Бекетов Н. В., Извольская И. В. Инновационные направления развития интернет-технологий в системе банковского обслуживания // Финансы и кредит. – 2008. – № 3. – С. 2–5.

2. Беликова О. И. Банковские услуги. – Иркутск : Изд-во БГУЭП, 2007. – 256 с.

3. Белоглазова Г. Н. [и др.]. Банковское дело. Организация деятельности коммерческого банка. – М. : Издательство Юрайт, 2014. – 652 с.

4. Ванин А., Сумманен К. Банк, который всегда с тобой // Банковские
технологии. – 1999. – № 4. – С. 46–52.

5. Воронцов А. А Защита банков от мошенничества // Jet Info. – 2012. – № 5. – С. 5–9.

6. Жарковская Е. П. Банковское дело. – М. : Омега-Л, Высш. шк., 2003. –
625 с.

7. Маркова О. М. [и др.]. Банковские операции. – М. : Издательство Юрайт, 2014. – 520 с.

8. Рудакова О. С. Банковские электронные услуги: учеб. пособие. – М. : Вузовский учебник, 2009. – 398 с.

9. Тавасиев А. М. Банковское дело: дополнительные операции для клиентов. – М. : Финансы и статистика, 2005. – 416 с.

10. Таран В. А. Электронный банкинг: виды, риски, перспективы развития // Машиностроитель. – 2013. – № 7. – С. 2–14.

11. Трофимова В. В. Информационные системы в экономике и управлении. – М. : Высшее образование, 2006. – 480 с.

12. Юденков Ю. Н. Интернет-технологии в банковском бизнесе: перспективы и риски: учеб.-прак. пособие. – М. : КноРус, 2010. – 120 с.

Информация об авторах *Буйзанова Светлана Витальевна* – магистрант, кафедра банковского дела и ценных бумаг, Байкальский государственный университет, 664003, г. Иркутск, ул. Ленина, 11, e-mail: soulnaran@gmail.com.

Татаринова Лариса Валентиновна – кандидат экономических наук, доцент, кафедра банковского дела и ценных бумаг, Байкальский государственный университет, 664003, г. Иркутск, ул. Ленина, 11, e-mail: baikal253@mail.ru.

Authors

Svetlana V. Buizanova – master's degree student, Department of Banking and Securities, Baikal State University, 11 Lenin St., 664003, Irkutsk, Russian Federation, e-mail: soulnaran@gmail.com.

Larisa V. Tatarinova – PhD Economics, Department of Banking and Securities, Baikal State University, 11 Lenin St., 664003, Irkutsk, Russian Federation, email: baikal253@mail.ru.