УДК 336.717 DOI 10.18698/2306-8477-2017-10-478

Интернет-банкинг: проблемы обеспечения безопасности

© Т.И. Кузнецова, Р.А. Малиновский, А.С. Несмелова

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Раскрыты причины распространения и сущность интернет-банкинга. Проанализированы состав и структура услуг, предоставляемых клиентам через интернет. Показаны риски, связанные с электронными услугами. Рассмотрены различные методы защиты банковской информации.

Ключевые слова: *интернет-банкинг, киберпреступность, электронная цифровая подпись, SSL-шифрование, одноразовые пароли*

Интернет-банкинг является одним из наиболее динамично развивающихся сегментов электронной коммерции и представляет собой вариант дистанционного способа оказания банковских услуг клиентам. В широком смысле под данным термином можно понимать самые разнообразные системы, начиная от обычных веб-сайтов банков и заканчивая сложными виртуальными расчетно-платежными системами. В более узком значении интернет-банкинг — это аналог системы банк — клиент, работающий через Интернет.

Возможности использования Интернета в области банковского дела постоянно расширяются, появляются новые службы и технологии. Об успехах интернет-банкинга свидетельствует тот факт, что космонавты, находящиеся на борту Международной космической станции, могут осуществлять платежи из космоса посредством Интернета, приобретать подарки для своих родных и близких, используя виртуальные платежные карты. С каждым годом услуги интернет-банкинга становятся все популярнее (рис. 1).

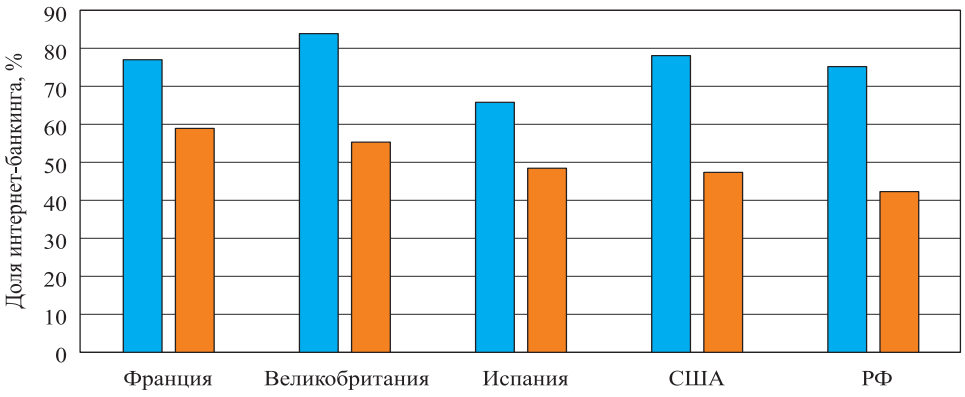

Рис. 1. Доля интернет-банкинга во Всемирной сети

Благодаря использованию систем интернет-банкинга клиент получает существенную экономию времени, круглосуточный контроль собственных счетов, ресурс мгновенно реагировать на изменения конъюнктуры финансовых рынков. Возможность работать со счетами с помощью пластиковых карт позволяет пользоваться услугами интернет-магазинов как в России, так и за рубежом на безопасном уровне.

С помощью системы интернет-банкинга клиенту достаточно перевести требуемую сумму средств на карту, а затем этой картой оплатить какую-либо услугу или товар на веб-сайте интернет-магазина. При этом в системе будут доступны выписки по карт-счету, из которых можно определить, какая сумма средств списана с карты, за что и т. п. Таким образом, больше, чем стоимость товара или услуги, с карты клиента просто не спишется и он всегда может отследить подобные операции [1–3].

Системы интернет-банкинга характеризуются доступностью, удобным интерфейсом, безопасностью, простотой установки и настройки программы, легкостью выполнения операций. Все это определяет обширный перечень услуг, которые банки могут оказывать через Интернет (рис. 2). Этот перечень включает в себя, в частности: платежи по счетам, переводы денег, в том числе в иностранных валютах, инвестиционные, кредитные, конвертационные операции, прочие виды платежей, а также получение информации о состоянии счетов, консультационные и информационные услуги, открытие различных банковских счетов [4].

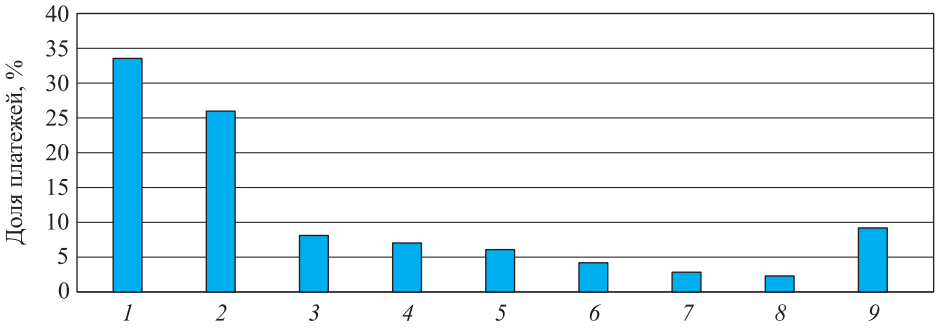

Рис. 2. Структура платежей в интернет-банкинге в РФ:
1 — платежи по произвольным реквизитам; *2* — переводы между счетами физических лиц; *3* — платежи в счет погашения кредитов; *4* — платежи за телекоммуникационные услуги; *5* — платежи за услуги ЖКХ; *6* — конвертация валют; *7* — оплата билетов; *8* — платежи в пользу государства; *9* — прочие виды платежей

При широком распространении интернет-банкинга требуется обеспечить безопасность финансовых транзакций. Современные технологии программно-аппаратной защиты гарантируют конфиденциальность операций и сохранность средств на достаточно высоком

уровне. Но самое главное, что в сохранности средств заинтересованы прежде всего коммерческие банки — поставщики услуг интернет-банкинга, отвечающие не только за сохранность финансов своих клиентов, но и за свои средства и репутацию.

В условиях рыночной экономики использование интернет-банкинга сопряжено с рядом рисков (рис. 3), а именно: мошенничеством, несанкционированным доступом к данным, киберпреступностью и т. д. [5].

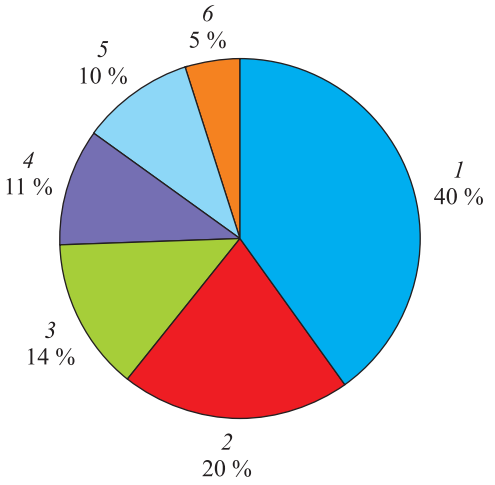

Рис. 3. Риски, связанные с интернет-банкингом:
1 — мошенничество; *2* — соответствие требованиям индустрии платежных карт; *3* — несанкционированный доступ к данным; *4* — DDoS-атаки; *5* — киберпреступность (вредоносное ПО); *6* — противодействие отмыванию денег

Для предотвращения этих угроз требуется разработка систем защиты. Во-первых, необходимо обеспечивать идентификацию субъектов (банка и клиента). Во-вторых, нужно защищать передаваемую информацию путем повышения уровня защиты для каналов передачи информации и носителей информации.

В современных условиях эти задачи решаются многими ведущими частными и государственными компаниями с помощью различных методов защиты: шифрования данных, установления одноразовых паролей, электронной цифровой подписи, использования внешних электронных устройств, интеллектуального мониторинга процесса удаленных транзакций и т. д. [6].

Одним из самых распространенных способов защиты от перехвата информации и изменения данных до получения их банком является шифрование. Наиболее успешным в данной области оказалось SSL-шифрование, которое предполагает создание среды с несколь-

кими слоями в целях обеспечения безопасного обмена информацией. Подключение открывается только целевым пользователям, что позволяет добиться конфиденциальности общения.

Безопасный SSL-протокол располагается между двумя протоколами: используемым программой клиента (HTTP, FTP, IMAP, LDAP, Telnet и т. д.) и транспортным протоколом TCP/IP. Благодаря этому образуются своеобразные барьеры, позволяющие защищать и передавать данные на уровень транспортного протокола. При SSL-шифровании поддерживается большое количество протоколов программ-клиентов (рис. 4).

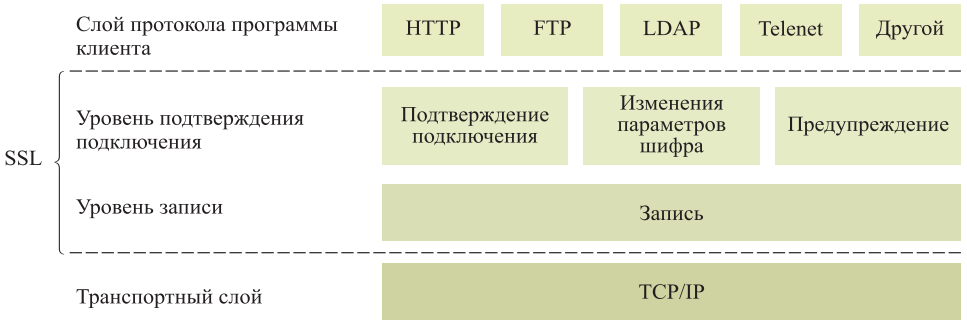

Рис. 4. Уровни SSL-шифрования

На рис. 4 изображены уровни слоев SSL. Работа протокола SSL осуществляется на двух уровнях. Первый уровень включает слой протокола подтверждения подключения (Handshake Protocol Layer), который состоит из трех подпротоколов: подтверждения подключения (Handshake Protocol), изменения параметров шифра (Change Cipher Spec Protocol) и предупредительного (Alert protocol). Второй уровень — слой протокола записи.

Для того чтобы эффективно использовать защищенную передачу данных, следует соблюдать элементарные меры безопасности в Интернете — не реагировать на подозрительные сообщения, полученные якобы от банка или центра безопасности, не переходить по неизвестным ссылкам, не сообщать секретные данные [7, 8].

Еще одним способом защиты информации являются одноразовые пароли. В коммерческих банках список одноразовых паролей можно взять в банкомате. Для совершения операции по счету через систему интернет-банкинга клиент обязан иметь карту банка и знать ПИН-код, чтобы получить список одноразовых паролей.

Вместе с тем этот метод имеет недостатки. Пароли, которые клиент получает в банкомате, распечатаны на чеке. Если такой чек будет утерян, то клиенту придется идти в банк за новыми паролями. Также пользователю необходимо получить новый чек, когда на старом за-

канчиваются данные пароли. Не всегда отделение банка, где могут выдать такие пароли, находится близко к дому. Не стоит забывать, что такой список может попасть в руки мошенников.

Если банк использует метод одноразовых паролей, то клиентам следует соблюдать ряд правил: не выбрасывать и не терять список паролей; не хранить список одноразовых паролей вместе с логином и паролем от учетной записи или картой.

К распространенным методам защиты информации относятся также одноразовые SMS-пароли, с помощью которых следует подтверждать все операции, которые совершает клиент. При этом номер счета должен быть привязан к номеру телефона.

Как и любые другие системы защиты, данный метод имеет достоинства и недостатки. Достоинства: время подтверждения операции крайне мало — меньше минуты, простота использования, повышенная мера безопасности от злоумышленников — одноразовые пароли невозможно потерять, а если мошенники узнают ваш логин и пароль, без одноразового пароля они не получат доступ к важной информации.

Недостатки: в случае кражи злоумышленниками телефона клиента его счет полностью перейдет в распоряжение преступников.

Российские компании в качестве метода защиты банковской информации широко применяют электронную цифровую подпись. Положительная сторона этого метода состоит в том, что банк может безошибочно идентифицировать пользователя. Недостаток данной системы заключается в том, что злоумышленники также могут взломать электронную цифровую подпись клиента, заразив компьютер вредоносным программным обеспечением.

При использовании электронной цифровой подписи необходимо регулярно проверять компьютер на предмет заражения вирусами, применять антивирусные программы, не оставлять ключ электронной цифровой подписи подключенным к компьютеру, когда его не используют.

Следующий способ защиты информации — внешние электронные устройства. Одни коммерческие банки для усиления защиты предлагают использовать специальные устройства, которые генерируют одноразовые пароли для выполнения операций. Генератор одноразовых паролей подключается к компьютеру через интерфейс USB-порт и не требует никаких дополнительных программ.

Другие банки рекомендуют применять внешний электронный ключ, который при самом первом подключении к интернет-банкингу генерируется, записывается на внешний носитель, а потом используется для совершения операций в системе.

Это, по сути, упрощенная электронная цифровая подпись. Недостаток системы в том, что, не имея такого ключа, клиент не может

получить доступ к своему счету. А носить его с собой не всегда безопасно и удобно.

При осуществлении мониторинга банковских транзакций одним из ключевых моментов является анализ. Имеется в виду не только анализ надежности, черных списков и прочего, речь идет об интеллектуальном мониторинге процесса удаленных транзакций.

Принятие решения об отклонении проведения платежа складывается из множества факторов. Каждому такому платежу назначается некоторая цена. При наличии нескольких факторов цены суммируются. Если превышается некоторый порог, платеж отклоняется. Цена каждого фактора определяется опытным путем в соответствии с моделью рисков, используемой банком.

Многие эксперты считают, что чаще всего причиной мошеннического доступа к данным пользователя является невнимательность и неосторожность самого клиента банка. Владельцу учетной записи следует беречь данные доступа к ней. Для повышения безопасности рекомендуется периодически менять пароли для доступа в систему [7].

Кроме того, необходимо соблюдать осторожность при работе в Интернете. Злоумышленники часто применяют методы социальной инженерии для получения аутентификационных данных (логин, пароль и т. д.).

Еще один метод мошенничества — фишинговые электронные письма, в которых получателям предлагают перейти на сайт или перезвонить по номеру технической поддержки. Для таких целей создаются копии сайтов с именами, похожими на настоящие. Если ввести на подобном сайте свои данные, они попадут к злоумышленникам.

Нередко пользователи подвергаются и другим угрозам, таким как нежелательное списание средств со счета, если клиент сам ввел неверные данные.

Специалисты отмечают, что успех в исправлении ошибки зависит от оперативности реагирования самого пострадавшего. Если средства еще не были отправлены в банк получателя, то деньги будут возвращены сразу. Если платеж уже поступил в другой банк, то придется подождать.

Помимо этого, клиент может попасть и в более неприятную ситуацию. По сообщениям СМИ, в начале 2009 г. одноразовые пароли на подтверждение платежей в системе интернет-банкинга у пользователя одного из российских банков присылались на чужой номер мобильного телефона. В результате мошенники списали крупные суммы со счета. Пострадавший уверен, что в инциденте замешаны сотрудники банка, ведь только они могли не просто сообщить злоумышленникам регистрационные данные (логин и пароль от учетной записи), но и отправлять им разовые пароли.

В данной ситуации доказать свою правоту сложно. Необходимо обращаться в суд, а его решение будет зависеть от содержания договора, подписанного с банком. Однако следует заметить, что данная ситуация является проблемой не только интернет-банка, но и недобросовестности персонала.

К сожалению, сегодня отсутствует четко сформулированное законодательство по вопросам защиты и безопасности как банковской информации, так и электронной коммерции в целом. Юридическое обоснование данной деятельности складывается из информации, содержащейся в многочисленных законодательных актах, указах и инструкциях [9].

Необходимы также разъяснительные документы по сертификации криптосредств. Сейчас сертификация осуществляется в нескольких организациях. Начавшиеся изменения в законодательной среде дают основания надеяться, что юридические вопросы в недалеком будущем все же будут урегулированы.

Популярность интернет-банкинга растет во всем мире, в том числе и в России. Это происходит потому, что он имеет ряд преимуществ, прежде всего — экономит время клиентов. Кроме того, данные системы интерактивны и просты, что позволяет привлекать новых пользователей и развивать прогрессивные формы банковского обслуживания клиентов.

ЛИТЕРАТУРА

[1] Лобачева Е.Н., Родионова В.Г. Инновации в системе электронных платежей. *Гуманитарный вестник*, 2014, вып. 1. URL: http://hmbul.bmstu.ru/catalog/econom/hidden/160.html (дата обращения 05.02.2017).

[2] Колобов А.А., Омельченко И.Н., ред. *Экономика инновационной деятельности наукоемких предприятий*. Москва, Изд-во МГТУ им. Н.Э. Баумана, 2007, 384 с.

[3] Кузнецова Т.И. Нейросетевые технологии в банковской сфере. *РИСК: Ресурсы. Информация. Снабжение. Конкуренция*, 2015, № 2, с. 177–180.

[4] Лаврушин О.И., ред. *Деньги, кредит, банки*. Москва, КНОРУС, 2016, 448 с.

[5] Кочергин Д.А. *Электронные деньги*. Москва, Маркет ДС, 2011, 424 с.

[6] *Перспективы интернет-банкинга*. URL: http://psyera.ru/5743/perspektivy-internet-bankinga (дата обращения 05.02.2017).

[7] *Проблемы безопасности интернет-банкинга*. URL: http://bosfera.ru/bo/problemy-bezopasnosti-internet-bankinga (дата обращения 10.01.2017).

[8] Кузнецова Т.И. Исламский банкинг: особенности кредитования инвестиционных проектов. *Финансовая жизнь*, 2015, № 2, с. 22–25.

[9] Кузнецова Т.И. Правовое регулирование банковской деятельности в Российской Федерации с учетом исторического опыта Западной Европы и США. *Гуманитарный вестник*, 2014, вып. 3.
URL: http://hmbul.bmstu.ru/catalog/ecoleg/hidden/185.html (дата обращения 29.01.2017).

Статья поступила в редакцию 19.06.2017

Ссылку на эту статью просим оформлять следующим образом:

Кузнецова Т.И., Малиновский Р.А., Несмелова А.С. Интернет-банкинг: проблемы обеспечения безопасности. *Гуманитарный вестник*, 2017, вып. 10.

http://dx.doi.org/10.18698/2306-8477-2017-10-478

Кузнецова Татьяна Ивановна — канд. экон. наук, доцент кафедры «Экономика и бизнес» МГТУ им. Н.Э. Баумана. Автор более 100 научных и учебно-методических работ в области теоретической экономики, финансов и кредита.
e-mail: t.kuznetsova@hotmail.com

Малиновский Роман Александрович — студент факультета «Ракетно-космическая техника» МГТУ им. Н.Э. Баумана.

Несмелова Анастасия Сергеевна — студентка факультета «Ракетно-космическая техника» МГТУ им. Н.Э. Баумана.

Internet banking: Security issues

© T.I. Kuznetsova, R.A. Malinovsky, A.S. Nesmelova

Bauman Moscow State Technical University, Moscow, 105005, Russia

The article reveals the essence of Internet banking and reasons for its spread. The composition and structure of services provided to customers via the Internet is analyzed. The risks associated with electronic services are shown. Various methods for protecting banking information are considered.

Keywords: *Internet banking, cybercrime, digital signature, SSL-encryption, one-time passwords*

REFERENCES

[1] Lobacheva E.N., Rodionova V.G. *Gumanitarnyy vestnik — Humanities Bulletin*, 2014, iss. 1. Available at: http://hmbul.bmstu.ru/catalog/econom/hidden/160.html (accessed February 05, 2017).

[2] Kolobov A.A., Omelchenko I.N., eds. *Ekonomika innovatsionnoy deyatelnosti naukoemkikh predpriyatiy* [Economics of innovative activities of high technology enterprises]. Moscow, BMSTU Publ., 2007, 384 p.

[3] Kuznetsova T.I. *RISK: Resursy, informatsiya, snabzhenie, konkurentsiya — RISC: Resources, Information, Supply, Competition*, 2015, no. 2, pp. 177–180.

[4] Lavrushin O.I., ed. *Dengi, kredit, banki* [Money, credit, banks]. Moscow, KNORUS Publ., 2016, 448 p.

[5] Kochergin D.A. *Elektronnye dengi* [Electronic money]. Moscow, Market DS Publ., 2011, 424 p.

[6] *Perspektivy internet-bankinga* [Prospects for Internet banking]. Available at: http://psyera.ru/5743/perspektivy-internet-bankinga (accessed February 05, 2017).

[7] *Problemy bezopasnosti internet-bankinga* [The problems of Internet banking security]. Available at: http://bosfera.ru/bo/problemy-bezopasnosti-internet-bankinga (accessed January 10, 2017).

[8] Kuznetsova T.I. *Finansovaya zhizn — Financial life*, 2015, no. 2, pp. 22–25.

[9] Kuznetsova T.I. *Gumanitarnyy vestnik — Humanities Bulletin*, 2014, iss. 3. Available at: http://hmbul.bmstu.ru/catalog/ecoleg/hidden/185.html (accessed January 29, 2017).

Kuznetsova T.I., Cand. Sc. (Econ.), Associate Professor, Department of Economic Theory, Bauman Moscow State Technical University. Author of over 100 research and educational publications in the field of theoretical economics, finance and credit.
e-mail: t.kuznetsova@hotmail.com.

Malinovsky R.A., student, Faculty of Rocket and Space Technology, Bauman Moscow State Technical University.

Nesmelova A.S., student, Faculty of Rocket and Space Technology, Bauman Moscow State Technical University.