УДК 004.056

БЕЗОПАСНОСТЬ ПОЛЬЗОВАТЕЛЕЙ ЭЛЕКТРОННОГО БАНКИНГА

Бердюгин А.А.,
аспирант, Финансовый университет
a40546b@gmail.com

Аннотация. *В статье рассматриваются отличительные признаки глобальной сети Интернет и ее влияние на развитие банковского бизнеса, а также особенности поведения людей в киберпространстве. Обсуждаются вопросы внедрения в кредитных организациях технологии дистанционного банковского обслуживания (ДБО) и появление новых источников банковских рисков, на которые в большей степени оказали влияние технологии ДБО. Уделено внимание применению «облачной» обработки данных в банках. Определены актуальные задачи в сфере безопасного применения технологий ДБО.*

Ключевые слова: *дистанционное банковское обслуживание; Интернет; компьютерные преступления; кредитная организация; информационная безопасность.*

SECURITY OF USERS OF THE ELECTRONIC BANKING

Berdyugin A.A.,
post-graduate student, Financial University
a40546b@gmail.com

Abstract. *The article examines distinctive features of the global network Internet and its impact on the development of the banking business, as well as the peculiarities of people's behavior in cyberspace. The issues of introduction of remote banking services (RBS) in the credit organizations are discussed. It is analyzed the emergence of new sources of bank risks, which are more heavily influenced by the RBS technology. Attention is given to the use of "cloud" data processing in banks. The actual tasks in the sphere of safe application of RBS technologies are determined.*

Keywords: *remote banking services; The Internet; Computer crimes; credit organization; Information Security.*

Введение

Сегодня Интернет предоставляет необъятный массив информации, открывающий широкие возможности для развития бизнеса. Банковская деятельность чрезвычайно консервативна и, казалось бы, она менее всего нуждается в новациях в части применения новых технологий и инструментария. Тем не менее именно банковское сообщество в наш информационный век весьма активно и заинтересованно откликнулось на возможности использования новых достижений в области информационных технологий и средств связи.

Кредитные организации нашли в информационных технологиях не только действенное средство учета, мониторинга, контроля за движением и хранением мировых денежных потоков, но и мощнейший инструмент воздействия

Научный руководитель: ***Марков А.С.,*** *доктор технических наук, профессор кафедры информационной безопасности.*

на существование самой денежно-финансовой и банковской системы, средство защиты этой системы и ее участников, а также эффективный инструмент регулирования сложных банковских процессов [1].

Таким образом, развитие информационных телекоммуникационных технологий привело к тому, что за последние 20 лет сформировалось так называемое информационное общество. Электронный контент производится и потребляется сегодня с огромной скоростью. По данным последнего пресс-релиза Международного союза электросвязи (МСЭ) за июль 2016 г., количество пользователей Интернета в мире составляет 3,5 млрд человек. По оценке ООН, численность мирового населения в 2015 г. достигла 7,3 млрд. В период с 2000 по 2015 г. удельный вес пользователей Интернета увеличился почти в семь раз — с 6,5 до 43% мирового населения.

По оценкам экспертов рынка, потенциал развития интернет-банкинга огромен. Аудитория российской зоны Интернета уже сейчас насчитывает более 80 млн пользователей[1] и, согласно данным опросов, каждый третий готов управлять своим банковским счетом через Сеть. Рынок интернет-торговли увеличивается на 30–50% ежегодно, а число абонентов мобильной связи уже существенно превышает численность населения России. Можно утверждать, что прирост клиентской базы через мобильные сервисы значительно увеличится в ближайшие годы [3].

Формируется благоприятная почва для развития электронных платежных сервисов. Однако при работе банка с клиентами проблемы обслуживания отнюдь не редкость. Ведь развитие виртуальных взаимоотношений между людьми и различными организациями создали и новый класс преступников, специализирующихся на преступлениях в области высоких технологий,— киберпреступников.

Проблемы и задачи

Интернет-технологии не только быстро внедряются в политику, бизнес, государственное управление, но и трансформируют характер межличностных отношений в обществе (формируются виртуальные онлайновые сообщества, устанавливаются отношения информационного партнерства, осуществляется группировка пользователей по определенным информационным интересам). Все это приводит к тому, что общество привыкает к активному использованию современных информационных и коммуникационных технологий. Тенденция распространяется и на банковские услуги.

Но наряду с очевидными преимуществами ДБО приносит и ряд проблем:

– технологический прогресс в банковской сфере обусловливает постоянное отставание нормативной базы, регламентирующей данный бизнес;

– применение новых технологий для выполнения банковских операций и обслуживания клиентов может снизить надежность и устойчивость кредитных организаций;

– технологические нововведения в банковской деятельности могут привести к ослаблению контроля над кредитными организациями со стороны регулятора.

Отсюда вытекают самые неотложные задачи в сфере безопасного применения технологий ДБО:

– совершенствование нормативной базы;

– адаптация контроля надежности банковских автоматизированных систем к условиям ДБО;

– повышение качества подготовки специалистов регулирующих и контрольных органов в сфере ДБО.

Помимо этого, надзорные и регулирующие органы должны обеспечить юридическую основу, которая сделает дистанционные платежи полностью легитимными. Она может включать:

– законодательство, регулирующее услуги денежных переводов с низким риском (переводы небольших денежных сумм, не предусмотренные традиционным банковским законодательством);

– разрешение небанковским организациям осуществлять транзакции (банковскому агенту или провайдеру денежных переводов принимать наличные, поступающие с электронных устройств);

[1] Число интернет-пользователей в России в 2015 году выросло на 9,2%. URL: https://ria.ru/society/20160413/1409762197.html (дата обращения: 15.12.2016).

– по возможности, реализация законодательных актов в виде системы, не затрагивающей потребительский интерфейс [2].

Останавливаясь на вопросах безопасности информации в системах ДБО, можно сказать, что за последние 6–7 лет мошенничество в системах ДБО прошло путь от единичных случаев до криминального бизнеса с оборотом примерно 100 млн долл. США в год. В нашей стране все начиналось в 2006–2007 гг. с редких краж средств банковских клиентов — физических лиц. Тогда это было легко: банки, заботясь об удобстве работы клиентов, для подтверждения платежа в большинстве случаев требовали ввести лишь обычный пароль, который можно было узнать, установив и настроив кейлоггер[2]. Скретч-карты[3], ключи электронно-цифровой подписи (ЭЦП), отправка одноразовых паролей на мобильный телефон широкого распространения не имели — поддержка таких средств защиты была реализована в ДБО ограниченного числа банков.

Мошенники могли украсть у одного клиента лишь небольшую сумму, что было связано с ограничениями на сумму платежа, которые устанавливали сотовый оператор и банк. Отличительная особенность мошеннических платежей того времени — преступники, перестраховываясь, работали в системе ДБО через анонимные прокси-серверы, находящиеся в других странах. Это, с одной стороны, в немалой степени затрудняло работу правоохранительных органов в проведении оперативно-розыскных мероприятий. С другой стороны, эта особенность позволяла антифрод-системам (системам обнаружения мошеннических платежей в ДБО) просто и эффективно обнаруживать факт хищения средств.

Ограниченность функций ДБО физических лиц не позволяла злоумышленникам воспользоваться всеми преимуществами дистанционного обслуживания, в частности перечислять большие суммы непосредственно на банковские карты. Поэтому функции специализированного программного обеспечения, с помощью которого похищались данные для аутентификации в ДБО, расширились — помимо логина и пароля злоумышленники могли копировать файлы, содержащие ключи ЭЦП.

Банковские операции в «облаке» данных

Все большая часть того, что мы делаем, должна быть отделена от рабочего компьютера или сервера фирмы. Несмотря на мобильность устройств, составляющих Интернет вещей, необходимость получения доступа к корпоративным данным остается. Данные должны перемещаться вместе с гаджетами, ведь информация является ядром всех технологий. Здесь выручает облачная (рассеянная) обработка данных. При этом возникают проблемы со службой безопасности. Поэтому пока большинство банков с неохотой обращаются с облачными хранилищами данных. Службы безопасности оправдывают отказ переводить важнейшие функции с серверных систем в «облако» тем, что это поставит под угрозу информацию, требующую особо деликатного обращения.

За последние 6–7 лет мошенничество в системах ДБО прошло путь от единичных случаев до криминального бизнеса с оборотом примерно 100 млн долл. США в год.

Это так. Только за последний год 50% утечки информации произошло через «облако», заявила гендиректор компании InfoWatch Наталья Касперская на конференции Skolkovo Cyberday и подчеркнула, что основной своей задачей в 2017 г. компания считает трансформацию системы защиты от утечек данных в систему, которая не только сможет перехватывать утечки и останавливать их, но и предсказывать риски в более широком смысле, показывать потенциальные области опасности

[2] Кейлоггер (от англ. *key* — клавиша и *logger* — регистрирующее устройство) — программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя: нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т.д.

[3] Скретч-карта (*scratch card*) — карта из картона или пластика с нанесенной на ней (под защитным непрозрачным и стирающимся слоем) некой секретной информацией.

внутри предприятия[4]. Однако потенциальные преимущества этой модели для отрасли финансовых услуг таковы, что полный отказ от облачных технологий станет для банков большой ошибкой.

Ущерб от мошенничества в ДБО уже в 2009 г. возрос практически в три раза, что заставило кредитные организации создавать внутренние подразделения для контроля транзакций.

Целесообразность перехода к облачным технологиям объясняется, прежде всего, ограниченностью нынешних систем. Поскольку среднестатистический клиент сотни раз в год получает доступ к банку через цифровые каналы (такие, как веб-сайты, мобильный телефон или онлайн-приложения), существует настоятельная необходимость перевода операций на более гибкую платформу.

На Западе есть банки, которые уже делают первые шаги в использовании облачных технологий. В январе 2012 г. BBVA заявил, что переводит свои компьютерные приложения в «облако» с помощью приложений Google. В своем заявлении BBVA подчеркнул, что эта мера направлена на повышение производительности, а не на то, чтобы переводить в «облако» личную информацию клиентов. По крайней мере пока [2]. К тому же общая производительность при работе с данными в «облаке» может быть ниже, чем при работе с их локальными копиями.

Автоматизация криминала

Психологи прошлого века отмечали, что война качественно изменилась. Враги перестали смотреть друг другу в глаза: «Современная война в воздухе следует принципам современного автоматизированного производства, в котором и рабочие, и инженеры полностью отчуждены от своего труда. В соответствии с общим планом производства и управления они выполняют технические задания, не видя конечного продукта. Но даже если они видят готовую продукцию, она их прямо не касается, они за нее не отвечают, она лежит вне сферы их ответственности. От них никто не ждет, что они спросят, что несет эта продукция — пользу или вред. Это решают управляющие. Что же касается управляющих, то для них „полезно"все то, что „выгодно" (и что приносит пользу предприятию), а это не имеет ничего общего с объективной оценкой полезности продукта. В войне „полезно" то, что служит уничтожению противника, и решения о том, что в этом смысле полезно, часто принимаются на основе весьма приблизительных данных[5]».

Подобный процесс мы наблюдаем и сейчас. Развитие программного обеспечения, используемого злоумышленниками, дало возможность автоматизировать кражи секретной информации клиента, требуемой для входа и создания платежа в системе ДБО (т.е. логина, пароля, секретного ключа клиента, а также IP-адреса сервера ДБО, с которым работает клиент). Вся собранная информация автоматически интегрировалась на центральном сервере, и преступникам достаточно было последовательно заходить в систему ДБО под собранными учетными записями клиентов и выводить средства с их счетов.

Ущерб от мошенничества в ДБО уже в 2009 г. возрос практически в три раза, что заставило кредитные организации создавать внутренние подразделения для контроля транзакций. Тогда же стали разрабатываться первые автоматизированные системы мониторинга транзакций. И все же гораздо большую угрозу информационной безопасности в системах ДБО представляет утечка конфиденциальной информации, произошедшая из-за халатности или в результате злонамеренных действий инсайдеров.

Как показывают экспертные опросы, более всего банки озабочены прямыми финансовыми убытками от утечки конфиденциальной информации (46,0%). На втором месте — ухудшение имиджа и общественного мнения (42,3%), на

[4] Касперская: половина утечек информации происходит через облачные сервисы. URL: http://tass.ru/ekonomika/3853695 (дата обращения: 21.12.2016).

[5] Фромм Э. Анатомия человеческой деструктивности: перевод и авт. вступ. ст. П.С. Гуревич. М.: Республика, 1994. С. 297.

третьем — потеря клиентов (36,9%), далее идут снижение конкурентоспособности (25,2%), юридические издержки (10,0%) и др.

Выводы

Из вышесказанного следуют выводы:

– современный банковский бизнес будет стремиться расширять применение электронных банковских услуг, поэтому коммерческие банки будут вынуждены конкурировать с различными организациями, осуществляющими аналогичные услуги и постоянно снижающими комиссию за транзакции. Конкуренция в этой сфере идет не ради состязательности, а ради получения дополнительной прибыли;

– применение методов социальной инженерии (науки об управлении поведением человека без технических средств на основе психологии) и других способов массового хищения электронных денег и информации повышает важность обеспечения информационной безопасности;

– регулирующим органам следует в кратчайшее время принять необходимые нормативные и законодательные акты в сфере ДБО;

– идеальных способов и средств обеспечения информационной безопасности в сетевых структурах до настоящего времени не существует. Каждое из возможных средств защиты имеет индивидуальные недостатки;

– с клиентами кредитных организаций, пожелавшими использовать технологии ДБО, следует проводить разъяснительную работу и инструктажи по порядку хранения носителей с конфиденциальной информацией, а также информировать их о наиболее распространенных способах мошенничества в системах ДБО;

– необходимо совершенствовать способы наблюдения и контроля со стороны регулирующих и надзорных органов за применением банковскими организациями технологий ДБО (включая возможность их использования в целях легализации преступных доходов).

Проблем, сложностей и рисков, возникающих в связи с внедрением интернет-технологий в банковскую сферу, немало. Но очевидно также, что потребность в наличных деньгах будет постоянно уменьшаться — их в определенной степени заменят электронные деньги.

Литература

1. *Юденков Ю.Н., Тысячникова Н.А., Сандалов И.В., Ермаков С.Л.* Интернет-технологии в банковском бизнесе: перспективы и риски: учебно-практ. пособие. 2-е изд., стер. М.: КНОРУС, 2014.
2. *Кинг Бретт*. Банк 3.0. Почему сегодня банк — это не то, куда вы ходите, а то, что вы делаете. М.: ЗАО «Олимп-Бизнес», 2014. 520 с.
3. *Горчакова М.Е*. Дистанционное банковское обслуживание: учеб. пособие. Иркутск: Изд-во БГУЭП, 2009.
4. *Скиба В.Ю., Курбатов В.А*. Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер, 2008.
5. *Ревенков П.В., Бердюгин А.А*. Кибербезопасность в условиях Интернета вещей и электронного банкинга // Национальные интересы: приоритеты и безопасность. 2016. № 11 (344). С. 158–169.

ИНФОРМБЮРО

В ШКОЛЬНЫЕ КУРСЫ ВВЕДУТ ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Школьников и учителей обучат основам кибербезопасности. Необходимые программы разработает Министерство образования и науки. Об этом заявила глава министерства Ольга Васильева на слушаниях в Совете Федерации по поводу безопасности в Интернете, передает агентство «РИА Новости».

По ее словам, «навык информационной безопасности» нужно прививать «с малых лет». «И в стандартах начального образования, и чуть позже на уроках, прежде всего, информатики, обществознания, права, ОБЖ, во внеурочной деятельности, а также в рамках программы воспитания и социализации мы должны говорить школьникам об этой самой безопасности», — уточнила Васильева. Министр образования отметила, что родители играют большую роль «в борьбе с угрозами в Интернете», так как ребенок большую часть времени проводит дома, а не в школе.

Источник: http://www.rbc.ru/rbcfreenews/58f49b069a7947a9789f9bc1