УДК 336.71

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО БАНКИНГА: УСЛУГА И ОБЯЗАННОСТЬ БАНКА

П.В. РЕВЕНКОВ,
доктор экономических наук,
профессор кафедры
экономического анализа и бухгалтерского учета
E-mail: pavel.revenkov@mail.ru

А.А. БЕРДЮГИН,
преподаватель кафедры
экономического анализа и бухгалтерского учета
E-mail: a40546b@gmail.com
Одинцовский гуманитарный университет

В статье рассматриваются сложившиеся в настоящее время условия для внедрения систем электронного банкинга. Приводятся основные показатели активности населения в использовании электронных финансовых и платежных сервисов в России. Отмечается, что благоприятные обстоятельства будут способствовать развитию технологий дистанционного банковского обслуживания, и систем электронного банкинга в частности. Выявлены наиболее острые проблемы в регулировании электронного банкинга, связанные с отставанием нормативной базы, регламентирующей процесс предоставления электронных банковских услуг, снижением надежности и устойчивости кредитных организаций, а также ослаблением контроля со стороны регулирующих органов.

Для решения данных проблем определены основные задачи в сфере регулирования безопасного применения систем электронного банкинга: своевременное обновление нормативной базы, адаптация контроля за надежностью банковских автоматизированных систем к условиям дистанционного банковского обслуживания, совершенствование надзора за безопасным применением систем электронного банкинга, а также постоянное повышение качества подготовки специалистов регулирующих и контрольных органов по вопросам управления рисками в условиях электронного банкинга.

Приведены характерные угрозы информационной безопасности в условиях электронного банкинга и основные задачи новой науки – форензики (компьютерной криминалистики). Предлагаются наиболее действенные наказания для киберпреступников в области информационной безопасности.

Рассмотрена проблема безопасности электронного банкинга с позиций кредитной организации и клиента. Сформулирован вывод о том, что процесс обеспечения информационной безопасности при оказании электронных банковских услуг должен носить комплексный и непрерывный характер. При этом клиент может выбирать уровень защиты своих операций, выполняемых с применением систем электронного банкинга, исходя из сопутствующих рисков (в том числе максимальная сумма денежных средств, которую можно потерять).

Ключевые слова: *электронный банкинг, риски, информационная безопасность, банковские услуги*

Условия для применения электронного банкинга. Распространение информационных и телекоммуникационных технологий в различных областях ведения бизнеса, а также активное использование людьми разного поколения мобильных устройств для доступа в Интернет привели к созданию благоприят-

ных условий для внедрения технологий дистанционного банковского обслуживания, среди которых лидирующие позиции занимают системы электронного банкинга (ЭБ). Основу ЭБ составляют:

– интернет-банкинг (управление банковскими счетами и картами через Интернет и web-браузер в режиме онлайн);

– мобильный банкинг (управление банковскими счетами и картами с КПК, коммуникаторов, планшетов и смартфонов).

К ЭБ относятся также банкоматы и терминалы банковского самообслуживания, которые задержатся еще лет на пятнадцать, прежде чем их вытеснят мобильные кошельки.

В ноябре 2013 г. аналитическое агентство Markswebb Rank & Report представило результаты исследования пользователей электронных финансовых и платежных сервисов в России. В основе исследования лежит репрезентативный опрос более 3 тыс. респондентов.

Ключевые выводы исследования следующие:

1) 19,6 млн чел. совершают хотя бы одну платежную операцию в Интернете каждый месяц;
2) 15,4 млн чел. используют интернет-банк (при этом почти 3/4 этих людей пользуются интернет-банком Сбербанк Онлайн);
3) 8,9 млн чел. платят в Интернете банковской картой;
4) 7 млн чел. совершают онлайн-платежи с помощью электронных кошельков;
5) 6,6 млн чел. совершают за месяц хотя бы один онлайн-платеж с мобильного устройства.

С развитием безбанковских технологий оборот платежей российского рынка дистанционного банковского обслуживания в 2017 г. увеличится в три раза и составит 1,89 трлн руб., говорится в исследовании компании J'son & Partners Consulting. На платежи через интернет-банкинг придется 1,83 трлн руб., на мобильный банкинг – 29 млрд руб., на SMS-банкинг – 31,8 млрд руб.

Особое внимание следует уделить такому IT-гиганту, как Apple. Ведь если эта корпорация не свернет с пути роста, на который недавно встала, то после запуска IPhone 5[1] с его возможностями мобильного кошелька рост корпорации, скорее всего, превзойдет все нынешние прогнозы и IPhone станет самым популярным телефоном на планете. Чтобы достичь этого на рынках развивающихся стран, Apple придется выпустить линейку более дешевых трубок, и они окажутся у потребителей Китая, Индии, Индонезии и стран Африки. Тогда конкурентам не удастся сместить компанию с ее позиций еще долгие годы.

Представленные данные свидетельствуют о благоприятных условиях для развития и распространения технологий дистанционного банковского обслуживания (включая системы ЭБ). Традиционное отделение повседневного банкинга постепенно утрачивает свою значимость для широкого круга потребителей. Оно неэффективно по сравнению с другими каналами коммуникации, где ценность измеряется скоростью выхода на рынок и быстротой реагирования. Эксперты утверждают, что разрыв между клиентами и банками стремительно расширяется, представляя беспрецедентные возможности для новых, небанковских, участников рынка.

Сложности регулирования и угрозы безопасности электронного банкинга. Итак, какие пункты плана оптимизации банковских отделений можно осуществить достаточно быстро, чтобы они были полезны как организации, так и потребителям? В ближайшие несколько лет благоприятные возможности для усовершенствования отделений следует искать в таких областях, как финансовые операции, уровень обслуживания клиентов и степень защищенности их активов. Предстоит добиться:

– устранения трений, сложностей и препятствий к взаимодействию;

– оптимизации связи с клиентами и терминологии при общении с ними;

– более качественного анализа поведения клиентов, который поможет лучше прогнозировать и удовлетворять из потребности;

– переоснащения отделений, переучивания персонала, работающего с клиентами, или найма нового;

– более эффективного использование автоматизированных систем для осуществления транзакций в отделениях через кассу.

Однако барьером для столь перспективных решений является то, что наряду с очевидными преимуществами ЭБ[2] имеет и ряд проблем:

[1] Уточним: iPhone 5 выпущен 12.09.2012, iPhone 6 выпущен 09.09.2014.

[2] К основным преимуществам ЭБ можно отнести существенную экономию времени за счет исключения необходимости посещать банк лично и возможность 24 ч в сутки контролировать собственные счета, а также оперативно реагировать на изменения ситуации на финансовых рынках.

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

– применение систем ЭБ для выполнения банковских операций клиентов может снизить надежность и устойчивость кредитных организаций;

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

Отсюда вытекают основные задачи в сфере регулирования для безопасного применения систем ЭБ:

– своевременное совершенствование нормативной базы;

– адаптация контроля за надежностью банковских автоматизированных систем к условиям дистанционного банковского обслуживания;

– совершенствование надзора за безопасным применением систем ЭБ;

– постоянное повышение качества подготовки специалистов регулирующих и контрольных органов по вопросам управления рисками в условиях ЭБ.

Главная проблема банкинга – в его инертности. Эту инертность совершенно необходимо преодолеть для возникновения положительного клиентского опыта или налаживания качественного обслуживания клиентов. Проблема инертности имеющихся процедур состоит в том, что вокруг них создан ложный ореол безопасности, из-за чего они кажутся менее рискованными и более дешевыми, чем что-то новое.

Как уже было отмечено, основным сдерживающим фактором на пути более динамичного развития бесконтактного банкинга как на Западе, так и в России остаются опасение людей по поводу безопасности.

Компания Group-IB оценивает объем российского рынка киберпреступности в 2013 г. около 2,44 млрд долл[3]. По данным Международного центра по борьбе с преступлениями в сфере высоких технологий Microsoft, на российских пользователей ежедневно совершается более 5 млн кибератак. При этом пиратское программное обеспечение остается одним из главных источников киберугроз. Например, при скачивании программы в интернете по запросу «скачать Windows бесплатно» в 92 случаях из 100 пользователь рискует потерять деньги и раскрыть свои персональные данные[4].

На некоторых сайтах в Интернете можно встретить не только объявления о продаже скиммингового[5] оборудования для совершения краж конфиденциальной информации с банкоматов или уже украденных данных пластиковых карт клиентов банков, но и предложения по разработке целенаправленных троянских программ, организации DDoS-атак[6] и многое другое, что способно нанести серьезный ущерб аппаратно-программному обеспечению систем ЭБ.

Очевидно, что с развитием систем ЭБ и появлением новых способов совершения преступлений, связанных именно с использованием новейших достижений в области информационных технологий, возникла необходимость создания адекватной системы противодействия (включая отдельное направление – компьютерную криминалистику). Это послужило причиной появления новой прикладной науки о раскрытии и расследовании преступлений, связанных с компьютерной информацией, о методах получения и исследования доказательств, имеющих форму компьютерной информации (так называемых цифровых доказательств), о применяемых для этого технических средствах – форензики (компьютерной криминалистики).

К основным задачам, решаемым с помощью форензики, относятся:

– разработка тактики оперативно-розыскных мероприятий и следственных действий, связанных с компьютерной информацией;

– создание методов, аппаратных и программных инструментов для сбора и исследования доказательств компьютерных преступлений;

– установление криминалистических характеристик правонарушений, связанных с компьютерной информацией.

В целом изменились только технические средства, с помощью которых совершаются пре-

[3] Доходы хакеров снижаются // Ведомости. 2014. 15 октября.

[4] Там же.

[5] Скимминг (от англ. skimming) – кража данных карты при помощи специального считывающего устройства (скиммера).

[6] DoS-атака (от англ. Denial of Service, отказ в обслуживании) и DDoS-атака (от англ. Distributed Denial of Service, распределенный отказ в обслуживании) – разновидности атак на вычислительную систему. Цель этих атак – довести систему до отказа, т.е. создать такие условия, при которых легитимные (правомерные) пользователи системы не могут получить доступа к предоставляемым системой ресурсам, либо этот доступ затруднен.

ступления. По сути же в киберпространстве, как и в реальном мире, ведется отчаянная борьба за обладание информацией с применением любых методов и приемов.

Например, в начале июня 2014 г. пресечена деятельность группы лиц, подозреваемых в многомиллионных хищениях денежных средств с расчетных счетов граждан и организаций. В результате было предотвращено хищение нескольких сотен миллионов рублей. Злоумышленники на протяжении трех лет осуществляли противоправную деятельность в нескольких регионах России.

Участники группировки тщательно соблюдали конспирацию: регулярно меняли sim-карты и телефоны, место жительства. Задержали подозреваемых в Кировской области. Схема, по которой действовали мошенники, была далеко не рядовой. Вначале они устанавливали на компьютеры своих жертв, которые были подключены к системам дистанционного банковского обслуживания, вирусную программу. Та в свою очередь заменяла в платежных поручениях реквизиты получателей на данные злоумышленника. С виду все выглядело как отправка обычного электронного платежа за оказание тех или иных услуг. Но на самом деле данные уходили на счета мошенников, а их жертвы поначалу даже не понимали, что их ограбили.

Базу данных хакеров, основные финансовые документы обворованных ими фирм полицейские обнаружили во время обысков, которые прошли сразу по двенадцати адресам. Также было изъято огромное количество пластиковых банковских карт, оформленных на подставных лиц. Так, по мнению следователей, предполагаемые преступники и обналичивали похищенные денежные средства[7].

Одним из последствий недавнего мирового финансового кризиса стало снижение затрат на обеспечение информационной безопасности в банках. При этом криминальный мир, напротив, ответил значительным увеличением своей активности. Компьютерные злоумышленники сейчас совсем не похожи на тинэйджеров, получивших первоначальные знания с хакерских web-сайтов. Это специалисты с достаточно высокой подготовкой не только в области информационных технологий, но и в финансовых вопросах. Причем большинство из них действует в составе организованных преступных групп.

Эксперты в сфере киберпреступности высказывают разные мнения по поводу ужесточения наказаний за подобные преступления. В частности, некоторые из них убеждены, что компьютерные преступления необходимо квалифицировать как преступления, связанные с кражей, совершенной группой лиц по предварительному сговору в крупном размере. Более того, использование новейших аппаратно-программных средств для хищения денежных средств вполне может рассматриваться судом как отягчающее обстоятельство, так как фактически такие преступления способны совершать только очень подготовленные специалисты.

Есть предложения ввести жесткую систему штрафов, при которой преступники будут обязаны выплачивать сумму, значительно превышающую размер кражи или убытков, понесенных организацией из-за киберпреступлений.

Безопасность электронного банкинга. Информация давно стала ценным активом для многих организаций. Ведь мошенникам в конечном счете она нужна для кражи денег. Исходя из этого, обеспечение ее безопасности становится одной из главных задач для поддержания надежности и устойчивости организации. Без сомнения, стоимость несоблюдения правил безопасности обходится компаниям значительно дороже их соблюдения.

В случае с ЭБ кража конфиденциальной информации клиентов (логины, пароли, секретные ключи) может привести не только к отказу от использования данного вида дистанционного банковского обслуживания, но и к финансовым потерям из-за судебных издержек.

Рекламируя достоинства ЭБ, кредитные организации преследуют, в первую очередь, главную цель бизнеса – получение прибыли. Однако, продавая банковские продукты и услуги, кредитные организации несут ответственность за качество предоставляемых услуг.

И вот тут возникает самая сложная задача – найти решение для обеспечения информационной безопасности, при котором клиент еще соглашается потратить некоторую сумму на защиту своих операций, а мошеннику уже невыгодно[8] совершать преступление.

Такое решение может включать:

– выполнение организационных мероприятий;

[7] См. URL: http://www.pcweek.ru/security/news-company/detail.php?ID=164007.

[8] Речь идет об экономической составляющей, так как для подготовки и совершения компьютерного преступления требуются определенные затраты.

– выбор аппаратно-программного средства защиты;

– тщательный подход к составлению договора и т.д.

В связи с этим начальники служб автоматизации, исполнительные директора и начальники служб информационной безопасности должны иметь понятные бизнесу аргументы для обоснования инвестиций в информационную безопасность, т.е. представлять обоснование стоимости системы защиты информации для бизнеса. Ведь инвестиции в разработку проектов защиты объекта, закупку необходимых элементов безопасности и эксплуатацию систем защиты для владельца информации есть не что иное, как материализованный экономический ущерб.

Для оценки расходов бюджета на систему защиты информации может быть применен научно-исследовательский метод, когда сначала аналитически вычисляется необходимый инструментарий измерения уровня информационной безопасности, а затем применяется на практике. Также можно сразу пойти практическим путем и найти инвариант[9] разумной стоимости корпоративной системы защиты информации. Поскольку нередко можно обнаружить аналогичные инварианты в других областях, где значимые для бизнеса события носят вероятностный характер.

Есть примеры и совсем «беззащитных» подходов. В случае с ЭБ это может быть вариант, при котором кредитная организация не связывает своего будущего с развитием технологий дистанционного банковского обслуживания, и услуги ЭБ максимально ограничены в возможностях для клиентов (операции не превышают конкретной суммы, ЭБ используется только для конкретной операции и/или для информирования и т.п.). Но в этом случае вряд ли можно говорить о конкурентоспособности такого банка.

Экономическое обоснование выбора средств защиты информации должно включать:

– анализ состояния экономической безопасности организации и определение роли защиты информации в ее обеспечении;

– анализ и классификацию рисков, возникающих при защите информации, страхование рисков;

– определение цены и затрат на создание и эксплуатацию комплексной системы защиты информации, в том числе отдельных ее элементов;

– стоимостную или экспертную оценку уровня понесенного и/или предотвращенного ущерба в результате внедрения комплексной системы защиты информации;

– оценку эффективности создания, внедрения и использования комплексной системы защиты информации, в том числе отдельных ее элементов (аппаратных и программных средств);

– оценку эффективности инвестиций в защиту информации.

Таким образом, формирование и обеспечение системы защиты информации всегда связано с расходованием средств. Затраты на создание системы защиты информации, соотнесенные со стоимостью потерь от ее нарушения, позволят определить экономический эффект от ее использования.

Уровень безопасности: предложение от банка, выбор за клиентом. Нередко банки сопротивляются технологическим нововведениям по причине отсутствия должного уровня безопасности. Поэтому современные способы осуществления банковских операций становятся для них рискованными. А в это время у банков уже появились серьезные конкуренты в виде различных организаций, предоставляющих услуги по расчетным операциям. В погоне за прибылью они готовы пойти на существенные упрощения процедур идентификации клиентов, участвующих в расчетах (что непозволительно коммерческим банкам), и вопросы безопасности для них – дело второстепенное.

Исходя из этого не следует ориентироваться на максимально ограниченный ЭБ, так как в информационный век вряд ли будет расти спрос на такие системы. Наоборот, спросом будет пользоваться ЭБ с широкими возможностями. В этом случае вопрос безопасности станет определяющим. Уже сейчас атаки хакеров приводят к серьезным потерям. Например, летом 2014 г. хакеры взломали 83 млн банковских счетов JPMorgan Chase, открытых в этом банке.

О взломе было известно ранее, но считалось, что атаке подверглось лишь около 1 млн счетов. В действительности она затронула 76 млн частных счетов и 7 млн счетов, принадлежащих малым коммерческим предприятиям. Это крупнейший в истории взлом банка электронным путем. Ликвидация его последствий займет как минимум несколько месяцев[10].

Поэтому не подлежит сомнению тот факт, что владелец информационных ресурсов, который не

[9] Инвариант – величина, остающаяся неизменной при тех или иных преобразованиях.

[10] URL: http://ria.ru/world/20141003/1026696817.html.

проводит тщательного анализа и не оптимизирует размера средств, выделяемых на систему защиты информации, практически всегда оказывается в экономическом проигрыше. Тем более что каждый новый этап в развитии информационных технологий требует от разработчиков новых решений в области информационной безопасности.

Так что же должно быть важнее для банков: собственная прибыль или должный уровень своих финансовых услуг? Здесь можно сразу отметить, что универсально высокого уровня услуг быть не может. В экономическом плане важнее, конечно, прибыль. А с точки зрения клиента, – уровень услуг. Следует учитывать, что без высокой организации сервиса банк понесет не только денежные, но и репутационные потери. Качественное обслуживание неизменно является стратегическим активом для финансово-кредитной организации. Однако измерить количественно влияние сервиса на конечный результат оказывается не простой задачей. Лучше всего использовать несколько измерителей – как финансовых, так и нефинансовых, что даст более объективную картину зависимости роста прибыли от влияния качества сервиса в банковской организации. Таким образом, нужно создавать системы «потребительской динамики», чтобы подразделения конкурировали в борьбе за клиентов, а не за получение дохода от своих продуктов.

Дополнительно можно использовать различные услуги по уровню обеспечения безопасности. Например, если клиенту необходимо круглосуточно иметь возможность совершать банковские операции на значительные суммы, ему можно предложить более надежный способ защиты своих данных. И, наоборот, если клиент держит на счете небольшую сумму и риск ее потерять невысокий, следует использовать минимальный уровень защиты.

Но в любом случае в настоящее время банки и владельцы интернет-магазинов задействуют в основном устаревшие способы защиты информации: статические пароли, имена пользователей и набор личных вопросов и ответов. Им на смену приходят одноразовые пароли, которые являются для банков одним из основных способов верификации клиентов. Рост популярности ноутбуков, планшетов и смартфонов позволяет идентифицировать клиента по голосу, лицу или отпечаткам пальцев. По прогнозам компании Javelin Strategy & Research, начиная с 2015 г. финансовые институты и предприятия, занимающиеся онлайн-торговлей, начнут широко применять биометрическую идентификацию.

По данным канадского стартапа[11] Bionym, традиционные пароли, ключи и кошельки уходят в прошлое. Эта компания представила браслет, который обеспечивает уникальную систему идентификации: он «узнает» своего владельца по сердечному ритму. Браслет имеет встроенный датчик, который распознает владельца по уникальной электрокардиограмме (ЭКГ) и передает сигнал с паролем, подтверждающим личность, на различные устройства, используя протокол Bluetooth. Появление портативных сканеров ДНК обещает очередную технологическую революцию в области идентификации клиентов. И вот тогда можно будет смело говорить о предоставлении гораздо большего разнообразия возможностей защиты персональной информации и денежных средств.

Итак, можно сделать некоторые выводы:

– использование интернет-технологий и возможностей сотовой связи представляет собой наиболее приоритетное направление деятельности в банковском бизнесе, так как помимо значительного снижения себестоимости выполнения банковских операций (в условиях ЭБ) они дают возможность получить конкурентные преимущества перед кредитными организациями, ориентирующимися на традиционный банкинг (обслуживание клиентов через офисы);

– учитывая активное использование нашими соотечественниками интернет-технологий и сотовой связи (для общения и передачи различной информации), можно с большой долей вероятности предположить, что технологии дистанционного банковского обслуживания (включая системы ЭБ) будут самыми востребованными банковскими услугами;

– предыдущий вывод свидетельствует о том, что коммерческие банки будут вынуждены конкурировать с различными предприятиями, осуществляющими аналогичные услуги, по причине постоянного снижения комиссии за осуществление транзакций;

– регулирующим органам необходимо в кратчайшее время принять необходимые нормативные и законодательные акты в сфере защиты дистанционных банковских услуг, а также организовать эффективный надзор за безопасным применением систем ЭБ;

[11] Стартап или стартап-компания (от англ. start-up – запускать) – компания с короткой историей операционной деятельности. Как правило, такие компании созданы недавно и находятся в стадии развития или исследования перспективных рынков.

– следует принять во внимание необходимость оценки расходов бюджета на средства защиты информации и сравнение с предполагаемой стоимостью потерь от ее нарушения;

– ввиду того, что информационная безопасность может быть оценена экономически (кстати, именно поэтому совершенной защиты до настоящего времени не существует, ведь экономика неразрывно связана с изменениями), клиент должен иметь возможность самостоятельно выбирать тот способ защиты, который он предпочитает. Ведь выбор средств и методов для защиты ЭБ постоянно растет вместе с количеством угроз, а потребности клиента могут варьироваться – ведь клиент всегда прав.

Список литературы

1. Банковское дело: учебник / под ред. Г.Г. Коробовой. М.: Магистр, 2011. 592 с.

2. Банковский троян Dridex распространяется через макросы Word. URL: http://xakep.ru/dridex.

3. *Гринвальд Г.* Негде спрятаться. Эдвард Сноуден и зоркий глаз дядюшки Сэма. СПб.: Питер, 2015. 320 с.

4. *Достов В.Л., Шуст П.М., Валинурова А.А., Пухов А.В*. Электронные финансы. Мифы и реальность. М.: КноРус, 2012. 232 с.

5. ДБО – Системы дистанционного банковского обслуживания. URL: http://tadviser.ru/a/93358.

6. Интернет-технологии в банковском бизнесе: перспективы и риски: учебно-практическое пособие / под ред. Ю.Н. Юденкова, Н.А. Тысячниковой, И.В. Сандалова, С.Л. Ермакова. М.: КноРус, 2014. 318 с.

7. *Кинг Бретт*. Банк 3.0. Почему сегодня банк – это не то, куда вы ходите, а то, что вы делаете. М.: Олимп-Бизнес, 2014. 520 с.

8. Кибербандиты в России и мире. URL: http://www.banki.ru/news/daytheme/?id=7243229.

9. *Ларина И.Е*. Экономика защиты информации: учеб. пособие. М.: МГИУ, 2007. 92 с.

10. *Лямин Л.В*. Применение технологий электронного банкинга: риск-ориентированный подход. М.: КноРус, 2011. 336 с.

11. Международный бизнес: учебник / под ред. В.А. Черненко. СПб.: Нестор-История, 2011. 428 с.

12. Международное и зарубежное финансовое регулирование: институты, сделки, инфраструктура: монография / под ред. А.В. Шамраева. М.: КноРус, 2014. 640 с.

13. Основные тенденции использования электронного банкинга. 2013. URL: http://ac.gov.ru/files/publication/a/1153.pdf.

14. Основы банковской деятельности (Банковское дело) / под ред. Тагирбекова К.Р. М.: ИНФРА-М, 2003. 720 с.

15. *Ревенков П.В., Бердюгин А.А*. ДБО: Интернет создает новых клиентов и расширяет профили рисков // Банковское дело. 2013. № 12. С. 64–67.

16. *Ревенков П.В*. Управление рисками в условиях электронного банкинга: Монография. М.: Экономическая газета, 2011. 168 с.

17. Рекомендации ФАТФ. Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения. М.: Вече, 2012. 176 с.

18. Русские хакеры провели масштабную операцию по взлому банковских счетов в США и Европе. URL: http://www.cnews.ru/news/top/index.shtml?2014/10/08/588216.

19. *Скиба В.Ю., Курбатов В.А*. Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер, 2008. 320 с.

20. Форензика – компьютерная криминалистика / под ред. Н.Н. Федотова. М.: Onebook.ru, 2012. 420 с.

Finance and credit
ISSN 2311-8709 (Online)
ISSN 2071-4688 (Print)

Banking

ELECTRONIC BANKING SECURITY: A SERVICE AND A RESPONSIBILITY OF A BANK

Pavel V. REVENKOV,
Aleksandr A. BERDYUGIN

Abstract

Importance The article considers the current conditions of electronic banking systems introduction. The study includes the key figures of activity of the population in the sphere of using electronic financial and payment services in Russia. We emphasize that favorable conditions will contribute to the development of remote banking service technologies in general and electronic banking systems in particular.

Objectives The objective is to consider the problem of security of electronic banking from the position of a bank and a customer (on the basis of economic component).

Methods We analyzed the cause and effect of applying e-banking systems and emerging challenges for supervisors.

Results We identified the most severe problems in electronic banking regulation that relate to imperfect regulatory framework governing the process of electronic banking services delivery, reduction in reliability and stability of credit institutions, as well as weakened control on the part of regulatory authorities. To solve these problems, we identified major tasks in the regulation of safe use of electronic banking systems, i.e. timely update of regulatory framework, adaptation of control over reliability of banking automated systems to the conditions of remote banking services, improving supervision over safe use of electronic banking systems, and continuous improvement of the quality of training of regulatory and control bodies in risk management under conditions of electronic banking. We describe specific threats to information security in electronic banking and the main tasks of the new science, i.e. forensics (computer forensic science). We offer the most effective punishment for cyber criminals in the sphere of information security. We consider the problem of electronic banking security from the position of a credit institution and a customer. The conclusion is that the process of information security in electronic banking services delivery should be comprehensive and continuous. In this case, customers may choose the level of protection of their operations carried out through electronic banking systems based on associated risks (including the maximum amount of money that can be lost).

Conclusions and Relevance We identified the most pressing problems in the field of electronic banking regulation and proposed to ensure the level of security based on associated risks for the customer.

Keywords: electronic banking, risks, information security, banking services

References

1. *Bankovskoe delo: uchebnik* [Banking: a textbook]. Moscow, Magistr Publ., 2011, 592 p.

2. *Bankovskii troyan Dridex rasprostranyaetsya cherez makrosy Word* [The banking Trojan Dridex distributed through Word macros]. Available at: http://xakep.ru/dridex. (In Russ.)

3. Grinval'd G. *Negde spryatat'sya. Edvard Snouden i zorkii glaz dyadyushki Sema* [There is no place to hide. Edward Snowden and a sharp eye of Uncle Sam]. St. Petersburg, Piter Publ., 2015, 320 p.

4. Dostov V.L., Shust P.M., Valinurova A.A., Pukhov A.V. *Elektronnye finansy. Mify i real'nost'* [Electronic finance. Myths and reality]. Moscow, KnoRus Publ., 2012, 232 p.

5. *DBO – Sistemy distantsionnogo bankovskogo obsluzhivaniya* [Systems of remote banking service]. Available at: http://tadviser.ru/a/93358. (In Russ.)

6. *Internet-tekhnologii v bankovskom biznese: perspektivy i riski: uchebno-prakticheskoe posobie* [Internet-related technologies in banking business: prospects and risks: a workbook]. Moscow, KnoRus Publ., 2014, 318 p.

7. King Brett. *Bank 3.0. Pochemu segodnya bank – eto ne to, kuda vy khodite, a to, chto vy delaete* [Bank 3.0. Why Today's Bank is not Where You Go, But What You Do]. Moscow, Olimp-Biznes Publ., 2014, 520 p.

8. *Kiberbandity v Rossii i mire* [Cyber bandits in Russia and in the world]. Available at: http://www.banki.ru/news/daytheme/?id=7243229. (In Russ.)

9. Larina I.E. *Ekonomika zashchity informatsii: uchebnik* [Information security economy: a textbook.]. Moscow, Moscow State Industrial University Publ., 2007, 92 p.

10. Lyamin L.V. *Primenenie tekhnologii elektronnogo bankinga: risk-orientirovannyi podkhod* [Application of electronic banking technologies: a risk-oriented approach]. Moscow, KnoRus Publ., 2011, 336 p.

11. *Mezhdunarodnyi biznes: uchebnik* [International business: a textbook]. St. Petersburg, Nestor-Istoriya Publ., 2011, 428 p.

12. *Mezhdunarodnoe i zarubezhnoe finansovoe regulirovanie: instituty, sdelki, infrastruktura: monografiya* [International and foreign financial regulation: institutes, transactions, infrastructure: a monograph]. Moscow, KnoRus Publ., 2014, 640 p.

13. *Osnovnye tendentsii ispol'zovaniya elektronnogo banking* [Main trends in using electronic banking]. Available at: http://ac.gov.ru/files/publication/a/1153.pdf. (In Russ.)

14. *Osnovy bankovskoi deyatel'nosti (Bankovskoe delo)* [Fundamentals of banking business (banking operations)]. Moscow, INFRA-M Publ., 2003, 720 p.

15. Revenkov P.V., Berdyugin A.A. DBO: Internet sozdaet novykh klientov i rasshiryaet profili riskov [The Remote Banking Services Department: Internet creates new clients and expands risk profiles]. *Bankovskoe delo = Banking*, 2013, no. 12, pp. 64–67.

16. Revenkov P.V. *Upravlenie riskami v usloviyakh elektronnogo bankinga: monografiya* [Risk management in the conditions of electronic banking: a monograph]. Moscow, Ekonomicheskaya gazeta Publ., 2011, 168 p.

17. *Rekomendatsii FATF. Mezhdunarodnye standarty po protivodeistviyu otmyvaniyu deneg, finansirovaniyu terrorizma i finansirovaniyu rasprostraneniya oruzhiya massovogo unichtozheniya* [Recommendations of FATF. International standards on counteraction to money laundering, terrorism financing and distribution of weapons of mass destruction]. Moscow, Veche Publ., 2012, 176 p.

18. *Russkie khakery proveli masshtabnuyu operatsiyu po vzlomu bankovskikh schetov v SShA i Evrope* [Russian hackers performed a large-scale operation on breaking bank accounts in the USA and Europe]. Available at: http://www.cnews.ru/news/top/index.shtml?2014/10/08/588216. (In Russ.)

19. Skiba V.Yu., Kurbatov V.A. *Rukovodstvo po zashchite ot vnutrennikh ugroz informatsionnoi bezopasnosti* [A guidance on protection against internal threats of information security]. St. Petersburg, Piter Publ., 2008, 320 p.

20. *Forenzika – komp'yuternaya kriminalistika* [Forensics: computer criminalistics]. Moscow, Onebook.ru Publ., 2012, 420 p.

Pavel V. REVENKOV
Odintsovo Humanitarian University, Odintsovo, Russian Federation
pavel.revenkov@mail.ru

Aleksandr A. BERDYUGIN
Odintsovo Humanitarian University, Odintsovo, Russian Federation
a40546b@gmail.com