На создание необходимых условий для ведения сельскохозяйственной деятельности направлена Государственная программа развития сельского хозяйства и регулирования рынков сельскохозяйственной продукции, сырья и продовольствия на 2013–2020 годы, а так же ускоренного импортозамещения до 2018 г.

Российские аграрии сталкиваются с пятью глобальными проблемами: колебанием курса рубля, удорожанием импорта, высокими ставками по кредитам, высоким уровнем проблемных долгов, проблемами поставок из-за рубежа.

Кризисные процессы в экономике серьезно усугубили проблемы аграрного сектора, а для выполнения плана по импортозамещению их решение должно быть найдено в короткие сроки.

С учетом предложений Минсельхоза, на 2015–2020 годы на поддержку аграриев в рамках госпрограммы дополнительно должны направить 568,2 миллиарда рублей. Приоритеты по импортозамещению – наращивание объема производства тепличных овощей, плодов и ягод, свинины и птицы. Увеличение финансирования, по расчетам Минсельхоза, позволит снизить импортные поставки мяса скота и птицы, а также овощей к 2020 году почти на 70%, молочных продуктов – на 30%, плодово-ягодной продукции – на 20%.

Список литературы

1. Налоговый Кодекс РФ.
2. Зайнуллина С.Ф. Особенности учета и контроля доходов и расходов, финансовых результатов в сельском хозяйстве / С.Ф. Зайнуллина // Молодой ученый. – 2015. – №8. – С. 528–532.
3. Хрипкова Е.П. Актуальные проблемы налогообложения субъектов аграрного сектора экономики и пути их решения/ Е.П. Хрипкова // Материалы VI Международной студенческой электронной научной конференции «Студенческий научный форум». – 2014.
4. Специальные налоговые режимы: Учебное пособие по дисциплине / М.А. Шадрина, К.А. Нурбагандова, 2014. – ФГОУ ВПО РГАУ – МСХА им. К.А. Тимирязева, 2014.С.132
5. Гончаренко Г.А. Система налогообложения в сельском хозяйстве России в современных условиях, 2012. – С.20–21.

Секция «Бизнес-информатика», научный руководитель – Чусавитина Г.Н., канд. пед. наук, профессор

ПУТИ МИНИМИЗАЦИИ РИСКОВ В ИНТЕРНЕТ-БАНКИНГЕ

Василько Ф.А., Чернова Е.В.

Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск, e-mail: grobovshik666@gmail.com

При осуществлении дистанционного банковского обслуживания возникает множество рисков. Основная проблема состоит в обеспечении доверенности среды исполнения банковских приложений. При этом собственно банки, имея необходимые средства и специалистов (или возможность таких специалистов привлечь со стороны), обычно оказываются достаточно защищенными, тогда как на стороне клиента очень часто возникают проблемы. Многие банки придерживаются той точки зрения, что клиент должен защищаться самостоятельно, и минимизируют собственные риски составлением клиентского договора, по которому практически всю ответственность за возможные проблемы несет клиент. Такая стратегия не совсем корректна, так как для минимизации рисков необходимы усилия обеих сторон (в том числе с целью снижения репутационных рисков).

«На мой взгляд, банк должен предоставить клиенту возможность применения наиболее современных и адекватных в отношении текущего уровня рисков средств защиты (и желательно обеспечить возможность выбора)» – пишет в своей статье Сергей Котов, эксперт по информационный безопасности компании «Алладин Р.Д.» [1]. Клиент должен с пониманием ситуации (а понимание возникает не само по себе, здесь тоже требуются усилия обеих сторон) сопоставить собственную оценку рисков с возможными затратами на их минимизацию и сделать осознанный выбор: осуществлять ли защиту собственных средств, и если да, то каким образом. Отсюда следует вторая задача банка: донести до клиента, который не обязан быть специалистом в области информационной безопасности, суть проблемы и объяснить разницу между предлагаемыми средствами защиты и особенностями их эксплуатации.

Что происходит со средой исполнения банковских программ на стороне клиента? Во-первых, зачастую клиенты используют одни и те же компьютеры и для повседневной деятельности, и для работы с интернет-банкингом. Эти же компьютеры используются и для доступа к самым разным ресурсам Интернета, поэтому риск заражения компьютера вредоносными программами, нацеленными на атаку систем дистанционного банковского обслуживания, очень велик. Но, даже формально понимая это, многие клиенты экономят на антивирусной защите и устанавливают программное обеспечение от совершенно неизвестных производителей либо бесплатные варианты с усеченной функциональностью. Здесь же возникает проблема, связанная с самими программами интернет-банкинга, их модулями, библиотеками, которые устанавливаются на компьютере пользователя. Вариант сотрудничества, когда от пользователя не требуется установка, значительно более надежен, поскольку если компьютер вдруг окажется зараженным, неизвестно, как это отразится на интернет-банкинге и личной информации клиентов.

Во-вторых, тонкое место любого интернет-банкинга– вопрос аутентификации: клиент должен быть уверен, что он попал в банк, а банк соответственно должен быть уверен, что к нему обратился клиент. Все старые средства аутентификации типа логин-пароль на данный момент не актуальны. Успешная атака на такие варианты защиты проходит очень легко, и потеря средств практически гарантирована. Минимум, который банк должен предложить клиенту, – двухфакторная аутентификация. Прежде всего, это USB-токены (или смарт-карты), в которых хранение ключей и сертификатов реализовано на аппаратном уровне в не извлекаемом виде.

Однако и наличие одних лишь средств двухфакторной аутентификации на данный момент уже не гарантирует от потерь. Крайне желательно иметь не просто двухфакторную, а многофакторную аутентификацию (т.е. дополнять аутентификацию по токену или смарт-карте еще одним фактором). Некоторые банки уже предлагают клиентам варианты с дополнительным введением одноразовых паролей. Эта система может быть реализована по-разному: как в виде OTP-токенов, так и с использованием SMS-канала. Хорошим вариантом дополнительного фактора аутентификации является биометрия. Она может использоваться как средство доступа к токену, если считыватель смарт-карты оснащен еще и биометрическим датчиком. Применение биометрии делает перехват пароля к USB-ключу гораздо более проблематичным.

Основная проблема состоит в том, что 100%-ной защиты от угроз не существует, и она не решается раз и навсегда. Верная стратегия состоит в том, чтобы

увеличить стоимость атаки, таким образом понижая вероятность самой атаки и ее эффективность. Разумеется, это требует инвестиций и продуманного подхода к информационной безопасности со стороны банков, но в противном случае трудно ожидать стабильного дохода от такой приобретающей постепенно массовый характер услуги, как интернет-банкинг.

Управление рисками интернет-банкинга рекомендуется организовывать таким образом, чтобы обеспечить контроль за данным видом дистанционного банковского обслуживания в целом, в том числе в рамках функционирования аппаратно-программного обеспечения систем интернет-банкинга, осуществления отдельных операций и используемых при этом массивов банковских данных.

При организации управления рисками интернет-банкинга и принятии внутренних документов кредитной организации рекомендуется учитывать:

1. Высокие темпы инновационных процессов в технологиях интернет-бнкинга;

2. Рост зависимости кредитной организации от информационных технологий в целом и от эффективности построения внутрибанковских автоматизированных систем;

3. Интеграцию новых интернет-технологий в действующие внутрибанковские автоматизированные системы;

4. Повышенную степень риска при осуществлении операций с применением систем интернет-банкинга ввиду возможности легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма [2];

5. Необходимость совершенствования процессов управления банковской деятельностью и внутреннего контроля с учетом применения интернет-технологий;

6. Необходимость повышения квалификации служащихкредитной организации и совершенствования управления рисками интернет-банкинга.

Развитие интернет-банкинга в России способствовало разработке Банком России мер по организации постоянного наблюдения за процессами расширения и модернизации данного вида банковского обслуживания. С июля 2004 г. введено в действие Указание, устанавливающее порядок информирования кредитными организациями Банка России об использовании интернет-технологий Документ предусматривает сбор посредством специально разработанной отчетной формы определенных сведений о применяемых банками интернет-технологиях, об их организационном обеспечении, а также об условиях применения[3].

На основе аналитической обработки данной информации Банк России получает сведения о текущем развитии технологий интернет-банкинга в отечественной банковской системе, одновременно формируя представление о круге проблем в данной области, требующих определенного регулирования. Так, например, в декабре 2007 г. Банк России, выражая обеспокоенность рядом негативных явлений и инцидентов, затрагивающих сайты российских банков (сетевые атаки, а также попытки неправомерного получения персональной конфиденциальной информации о пользователях), рекомендовал банкам в договорах с провайдерами интернет-услуг предусматривать принятие ряда специальных мер по восстановлению работоспособности их ресурсов в случае возникновения чрезвычайных ситуаций, оговорив обязательства сторон и ответственность контрагентов за несвоевременное исполнение[4].

В рекомендациях Банка России по организации управления рисками, возникающими при осуществлении операций с применением систем интернет-банкинга, подчеркивается, что обеспечение эффективного управления ими является одной из целей внутреннего контроля. Согласно этим рекомендациям, оптимальная модель управления рисками в данной сфере должна включать следующие компоненты:

1. Квалифицированная политика информатизации, в том числе внедрения и развития технологий интернет-банкинга, проводимая руководством кредитной организации и обеспечивающая полнофункциональность системы – выполнение предполагающихся функций банковского обслуживания;

2. Тщательно продуманная архитектура автоматизированной банковской системы [5];

3. Адекватные меры по обеспечению информационной безопасности по всему информационному контуру интернет-банкинга, гарантирующие доступность и непрерывность банковского обслуживания, а также защиту информации от несанкционированного доступа, модификации либо уничтожения;

4. Организация внутрибанковских процессов и процедур, соответствующих масштабу, технологической и технической сложности предоставляемого обслуживания клиентов посредством интернет-банкинга;

5. Отлаженная система внутреннего контроля, охватывающая всю технологическую цепочку интернет-банкинга и организационную структуру, начиная с руководства банка[6];

6. Эффективная система финансового мониторинга, оказывающая противодействи попыткам использования системы интернет-банкинга в противоправных целях;

7. Содержательное и всеобъемлющее организационное, информационное, методическое и консультационное обеспечение клиентов;

8. Оптимальные с точки зрения минимизации сопутствующих рисков взаимоотношения кредитной организации со своими провайдерами и вендорами.

Рекомендации Банка России учитывают и трансграничный характер услуг интернет-банкинга. Так, банкам рекомендуется выявлять возможные дополнительные источники рисков, возникающих в связи с нарушением законодательства зарубежных государств или территорий, а также дополнительные факторы рисков, относящихся к иным юрисдикциям, в том числе к соблюдению рекомендаций ФАТФ[7].

В настоящее время подход Банка России к организации банковского надзора в области интернет-банкинга в значительной мере сводится к наблюдению за процессами, происходящими в этой сфере, выявлению основных факторов или источников рисков, сопутствующих применению данной технологии услуг, а также разработке методического обеспечения управления рисками.

Для решения вопросов обеспечения кибербезопасности Банком России было принято решение создать в Главном управлении безопасности и защиты информации Банка России Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере.

Основной целью деятельности центра является организация и координация работ по направлению комплексного противодействия противоправным действиям при предоставлении организациями кредитно-финансовой сферы финансовых услуг и услуг по переводу денежных средств с использованием информационных и телекоммуникационных технологий, а также противодействия компьютерным атакам на информационные ресурсы ОКФС.

Работа данного центра организуется по трем направлениям:

• ведение мониторинга и анализа всех видов инцидентов информационной безопасности, формиро-

вание единой базы данных уязвимостей, видов инструментария атак;

• оперативное предоставление участвующим в этой работе банкам аналитической и «горячей» информации о новых угрозах и атаках;

• взаимодействие с правоохранительными органами в расследовании инцидентов и пресечении активности «высокотехнологичной преступности».

На сегодняшний день есть несколько первоочередных задач в области регулирования применения систем ДБО, связанных с минимизацией последствий реализации кибератак:

• повысить качество нормативно-правового обеспечения в области кибербезопасности в условиях ДБО;

• повысить уровень надежности аппаратно-программного обеспечения систем ДБО;

• организовать мероприятия, направленные на повышение финансовой грамотности населения по вопросам кибербезопасности;

• организовать подготовку (переподготовку) специалистов ОКФС по вопросам обеспечения кибербезопасности;

• расширить функции внутреннего контроля в ОКФС за счёт учета новых источников рисков, связанных с недостатками в обеспечении кибербезопасности (в т.ч. в условиях ДБО).

Успешное развитие дистанционных банковских услуг в кредитно-финансовой сфере (в первую очередь – завоевание доверия клиентов к данному виду обслуживания) может быть только в условиях обеспечения должного уровня кибербезопасности (включая надежность и защищенность аппаратно-программного обеспечения систем ДБО). Регулирующие органы должны создать работоспособную систему обеспечения кибербезопасности в кредитно-финансовой сфере, в том числе специальные надзорные подразделения, способные осуществлять как дистанционный надзор, так и надзор «на местах» (инспекционные проверки по тематике надежности и защищенности систем ДБО от кибератак).

Продолжением политики регулятора в области обеспечения кибербезопасности должны быть рекомендации для ОКФС, направленные на повышение качества управления рисками, источниками, возникновения которых могут быть «удачно реализованные» компьютерные атаки. Необходимо обеспечить своевременную подготовку (переподготовку) специалистов в области кибербезопасности (включая специалистов риск-подразделений и служб внутреннего контроля). Совершенствовать системы управления рисками и системы внутреннего контроля в ОКФС за счет учета новых источников типичных банковских рисков, связанных с появлением новых киберугроз (в т.ч. с появлением целенаправленных атак на системы дистанционного банковского обслуживания) [8].

Исходя из всего вышеизложенного, можно определить основные способы минимизации рисков в интернет банкинге:

1. Создание единой базы возможных угроз и видов хакерских атак;

2. Повышение нормативно-правового обеспечения в дистанционном банковском обслуживании;

3. Повышение качества и надёжности аппаратно-технических ресурсов используемых при создании, использовании и сопровождении интернет-банкинга;

4. Повышение уровня грамотности населения в вопросах совершения финансовых операций в сети интернет, путём подробного консультирования специалистами кредитных организаций клиентов, при оформлении интернет-банкинга.

Список литературы

1. Котов С. Безопасность интернет-банкинга / С. Котов // Банковские технологии. –2012. – №2. – С. 46–49. (дата обращения 20.12.2015).

2. Российская Федерация. Государственная дума. Федеральный закон 07.08.2001 № 115–ФЗ (ред. 29.06.2015) о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма// (Дата обращения 19.12.2015).

3. Возникновение риска потери финансовой устойчивости в кредитной организации при использовании системы интернет-банкинг. Режим доступа: http://dogend.ru/docs/index-447670.html (дата обращения 20.12.2015).

4. Интернет-банкинг, как собственное казначейство клиента. Режим доступа: http://www.klerk.ru/bank/articles/254280/ (дата обращения 20.12.2015).

5. Банковские продукты: сущность, виды и перспективы развития. Режим доступа: http://bibliofond.ru/view.aspx?id=648233 (дата обращения 20.12.2015).

6. Бухгалтерия.ru. Интернет-банкинг: экономия ресурсов или «зона риска»? Режим доступа: http://www.buhgalteria.ru/article/n133313 (дата обращения 20.12.2015).

7. Интернет-банкинг. Режимдоступа: http://www.grandars.ru/student /bankovskoe-delo/internet-banking.html (датаобращения 20.12.2015).

8. PCI DSS.RU by Digital security. Пути снижения рисков реализации кибератак на дистанционное банковское обслуживание. Режим доступа: http://pcidss.ru/articles/239.html (дата обращения 20.12.2015).

Секция «Государственные и муниципальные финансы: состояние, проблемы и перспективы повышения эффективности управления», научный руководитель – Андреева О.В., канд. экон. наук

ПРОБЛЕМА ПОВЫШЕНИЯ ПЕНСИОННОГО ВОЗРАСТА В РОССИИ

Кочетова А.И.

ФБОУ ВО РГЭУ РИНХ, Ростов-на-Дону, e-mail: ia20085@rambler.ru

Пенсионный возраст – одна из важнейших характеристик пенсионной системы, показывающая на каком году жизни пенсионер может воспользоваться благами социального государства. На сегодняшний день, в России данный показатель установлен на уровне 55 лет для женщин и 60 лет для мужчин. Жители северных регионов, а также сотрудники вредных и опасных производств могут выходить на пенсию гораздо раньше.

Активные дебаты о повышении пенсионного возраста начались после кризиса 2008–2009 годов. В 2010 году дефицит Пенсионного фонда России (ПФР) впервые превысил 1 трлн. рублей и составил 4,1% ВВП. [1]

За пять последних лет сбалансировать пенсионную систему так и не удалось. Собираемые страховые взносы не покрывают объем выплачиваемых пенсий. И решать вопрос приходится за счет бюджета. Как отмечает председатель совета директоров Европейского Пенсионного фонда Евгений Якушев, в 2015 году дефицит пенсионного бюджета составил 623 млрд. рублей. За последние шесть лет доля трансферта федерального бюджета в бюджете ПФР занимала от 62% в 2010 году и до 36% в 2015 году. [2] Примерно четверть расходов бюджета – это вынужденный трансферт в ПФР. По словам эксперта, разбалансировке пенсионной системы способствовали принятые ранее решения о валоризации пенсий (переоценка стажа, полученного в СССР), ускоренной индексации размеров пенсий, введении льготных тарифов страховых