Журавлева Валерия Вадимовна, Целых Александр Николаевич

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКИХ СИСТЕМ И МЕРЫ ПО ЕЕ ОБЕСПЕЧЕНИЮ

В статье рассматриваются принципы информационной безопасности банковских систем, учитывающие их специфические особенности и отличия от информационных систем других организаций, а также требования последнего отечественного Стандарта Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации. Предлагаются меры по защите банковских данных, являющиеся актуальными после выхода "Положения о защите информации в платежной системе" и других подзаконных актов. Проводится анализ степени уменьшения рисков для банков, обеспечивающих необходимый уровень информационной безопасности.

Адрес статьи: www.gramota.net/materials/1/2015/9/17.html

Статья опубликована в авторской редакции и отражает точку зрения автора(ов) по рассматриваемому вопросу.

Источник

Альманах современной науки и образования

Тамбов: Грамота, 2015. № 9 (99). С. 67-71. ISSN 1993-5552.

Адрес журнала: www.gramota.net/editions/1.html

Содержание данного номера журнала: www.gramota.net/materials/1/2015/9/

© Издательство "Грамота"

Информация о возможности публикации статей в журнале размещена на Интернет сайте издательства: www.gramota.net

Вопросы, связанные с публикациями научных материалов, редакция просит направлять на адрес: almanac@gramota.net

4. **Жуплей И. В., Дьяков И. И.** Формирование эффективной структурной политики в сельском хозяйстве региона // Известия Оренбургского государственного аграрного университета. 2015. № 1 (51). С. 220-222.
5. **Курбатов А. С.** Перспективы модернизации сельскохозяйственного производства в России с точки зрения перехода к устойчивому развитию // Экономика, труд, управление в сельском хозяйстве. 2014. № 3 (20). С. 9-21.
6. **Регионы России. Социально-экономические показатели. 2011**: стат. сб. / Росстат. М., 2010. 900 с.
7. **Регионы России. Социально-экономические показатели. 2014**: стат. сб. / Росстат. М., 2014. 900 с.
8. **Стратегия устойчивого развития сельских территорий Российской Федерации на период до 2030 года** // АПК: экономика, управление. 2015. № 3. С. 83-88.
9. **Устойчивое развитие сельских территорий на 2014-2017 годы и на период до 2020 года** [Электронный ресурс]: Федеральная целевая программа. URL: http://www.garant.ru/products/ipo/prime/doc/70319016/ (дата обращения: 15.06.2015).
10. **Ушачев И.** Аграрный сектор России в условиях международных санкций и эмбарго: вызовы и перспективы // АПК: экономика, управление. 2015. № 6. С. 9-22.
11. **Хайруллин А.** Пути импортозамещения продовольственных товаров сельхозтоваропроизводителями России // АПК: экономика, управление. 2015. № 4. С. 3-8.

SUSTAINABLE DEVELOPMENT OF AGRICULTURE: REGIONAL AND APPLIED ASPECT

Zhuplei Irina Viktorovna, Ph. D. in Economics, Associate Professor
Far Eastern Federal University (Branch) in Ussuriisk
zirinavik@mail.ru

The article examines the range of the problems of the sustainable development of agricultural sphere through the lenses of economic sanctions and anti-sanctions; the critical analysis of legislative acts on the sustainable development of rural territories is conducted; the problems of providing the sustainability of agriculture at regional level (by the example of the Far East of the Russian Federation) are highlighted; the dynamics of the profitability of agricultural produce as to the federal subjects of the Far East region is analyzed. The author's model of the impact of the structure of regional agriculture sectors on its sustainability is suggested.

Key words and phrases: sustainable development; agriculture; The Far East of the Russian Federation; Primorsky krai; rural territories; profitability of agricultural produce.

УДК 004.056.53
Технические науки

В статье рассматриваются принципы информационной безопасности банковских систем, учитывающие их специфические особенности и отличия от информационных систем других организаций, а также требования последнего отечественного Стандарта Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации. Предлагаются меры по защите банковских данных, являющиеся актуальными после выхода «Положения о защите информации в платежной системе» и других подзаконных актов. Проводится анализ степени уменьшения рисков для банков, обеспечивающих необходимый уровень информационной безопасности.

Ключевые слова и фразы: информационная безопасность; банковская система; национальная система платежных карт; несанкционированный доступ; скимминг; фишинг.

Журавлева Валерия Вадимовна
Целых Александр Николаевич, д.т.н., профессор
Южный федеральный университет
baleranka@mail.ru; ant@sfedu.ru

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКИХ СИСТЕМ И МЕРЫ ПО ЕЕ ОБЕСПЕЧЕНИЮ©

Коммерческие банки, являясь важнейшим финансовым институтом современного социума, должны следовать определенным правилам информационной безопасности и уметь противостоять дестабилизирующим факторам [6].

В настоящее время стоимость и значимость банковской информации многократно возросли, что привело к росту преступного интереса к ней [8]. Каждый банк обязан обеспечить безопасность хранимых им данных, именно поэтому он должен следить за регулярной сменой и проверкой паролей, а также за контролем вероятности утечки информации.

Банковские информационные системы и базы данных содержат конфиденциальную информацию о клиентах банка, состоянии их счетов и проведении различных финансовых операций. Необходимо поддерживать сохранность этих данных, обеспечивать их информационную безопасность, осуществлять быстрый

© Журавлева В. В., Целых А. Н., 2015

и своевременный обмен и обработку информации, чтобы банковская система не дала сбой. Для этого необходима целая структура, которая будет способна обеспечить защиту информации, а также конфиденциальность клиентской базы.

План действий, обеспечивающих информационную безопасность банков, принципиально отличается от плана действий других организаций. Главными причинами этого являются специфический характер угроз, а также публичная деятельность банков, которые обязаны делать доступ к счетам несложным с целью удобства для клиентов.

Факторы, которые следует учитывать для обеспечения информационной безопасности банков [10]:

1. Информация, которая хранится и обрабатывается в банках, – это реальные деньги. При открытом доступе к данной информации через компьютеры могут открываться кредиты, производиться выплаты, а также могут переводиться значительные суммы денег без ведома владельца данного счета. Совершенно ясно, что такое незаконное манипулирование информацией приведет к убыткам различной степени. Данная особенность увеличила число мошенников, которые покушаются именно на банки, ведь информация, к примеру, промышленных компаний чаще всего не представляет такого интереса.
2. Информация, которая относится к банковской сфере, касается большого количества людей и организаций, то есть клиентов банков. Банк должен обеспечить достаточный уровень конфиденциальности информации, что является приоритетной задачей, поскольку каждый клиент вправе рассчитывать, что банк будет заботиться о его интересах, ведь от этого напрямую зависят репутация и успешность самого банка.
3. От того, как клиенту удобно работать с банком, а также от широкого спектра предоставляемых им услуг напрямую зависит конкурентоспособность банка. Именно поэтому банк должен предоставлять возможность быстрого и неутомительного распоряжения денежными средствами. Но именно такая легкость доступа к денежным активам и увеличивает число преступников, которые проявляют интерес к банковским системам.
4. Банк обязан обеспечить высокую надежность работы компьютерных систем даже в случае нештатных ситуаций, ведь банк, в отличие от большинства компаний, отвечает не только за свои денежные средства, но и за деньги клиентов.
5. Банк хранит важную информацию о своих клиентах, что расширяет круг потенциальных злоумышленников, заинтересованных в краже или порче такой информации.

Чтобы защищать интересы и цели всей банковской системы Российской Федерации в условиях угроз, были созданы отечественные стандарты по информационной безопасности (Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы РФ) [5]. Но, к сожалению, даже эти стандарты не могут ответить на все вопросы, поэтому они постоянно меняются и усовершенствуются за счет ранее накопленного всеми поколениями опыта по защите информации.

В условиях современной геополитической ситуации явно прослеживается тенденция к переходу на национальную систему платежных карт. Это, в свою очередь, требует повышение надежности и безопасности банковских информационных систем.

Все эти факторы привели к очередному переизданию стандартов СТО БР ИББС. Июнь 2014 года ознаменовался вступлением в силу пятой обновленной версии СТО БР ИББС – 2014. В отдельных блоках этого стандарта подробно описаны требования к обеспечению безопасности, а также даются конкретные перечни мер защиты по тому или иному блоку (Таблица 1).

Таблица 1.

Требования к обеспечению информационной безопасности в обновленной версии СТО БР ИББС – 2014 [6]

№	Требования к обеспечению информационной безопасности
1	При назначении и распределении ролей и обеспечении доверия к персоналу
2	В автоматизированных банковских системах (АБС) на стадиях жизненного цикла
3	При управлении доступом и регистрацией пользователей
4	К средствам антивирусной защиты
5	При использовании ресурсов сети Интернет
6	При использовании средств криптографической защиты информации
7	В банковских платежных технологических процессах
8	По обработке персональных данных
9	Отдельным заголовком вынесены требования к системе менеджмента информационной безопасности

5 мая 2014 года Президент Российской Федерации Владимир Владимирович Путин подписал закон о создании в России национальной системы платежных карт, а также об обеспечении бесперебойной работы международных платежных систем [9].

Национальная система платежных карт создается в форме ОАО, 100% активов которого принадлежит Банку России. Цель проекта – информационно замкнуть процесс осуществления денежных переводов внутри России. Если ранее деньги могли появляться из «ниоткуда» и исчезать в «никуда», то после выхода закона

ситуация изменилась, то есть национальная платежная система позволяет отслеживать все денежные операции. Например, финансирование сомнительных сделок и мошеннические операции. И, что немаловажно, уход от наличного оборота, как считает правительство, поможет государству в борьбе с коррупцией.

Чтобы обеспечить безопасность национальной платежной системы, был выпущен целый ряд подзаконных актов, среди которых основополагающее «Положение о защите информации в платежной системе» от 13.06.2012 г. № 584 [4]. Большую роль сыграло выпущенное ответственным департаментом Банка России «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств…» от 09.06.2012 г. № 382-П [7].

После внесения изменений в Положение Банка России от 09.06.2012 г. № 382-П тенденции обеспечения защиты смещены в сторону [3]:

- применения банкоматов и платежных терминалов;
- применения пластиковых платежных карт;
- использования сети Интернет (систем дистанционного банковского обслуживания (ДБО) и мобильного банкинга);
- требований к порядку разработки и распространения специализированного программного обеспечения, предназначенного для использования клиентом при переводе денежных средств;
- расширения требований по повышению осведомленности клиентов о возможных рисках получения несанкционированного доступа к защищаемой информации и рекомендуемых мерах по их снижению;
- требований о необходимости проведения классификации банкоматов и платежных терминалов, результаты которой должны учитываться при выборе мер защиты;
- процедур приостановления проведения платежа оператором по переводу денежных средств в случае обнаружения признаков мошеннических действий;
- процедур защиты от современных угроз безопасности, таких как скимминг (путем использования специализированных средств, препятствующих несанкционированному считыванию треков платежных карт);
- защиты сервисов, расположенных в сети Интернет, от внешних атак (DoS-атак);
- защиты от фишинга (фальсифицированных ложных ресурсов сети Интернет);
- требования по применению платежных карт, оснащенных микропроцессором, с 2015 года и запрета выпуска карт, не оснащенных микропроцессором, после 1 января 2015 года.

На наш взгляд, банковские структуры должны взять курс на эти тенденции, а именно, на скорейший переход от пластиковых карт с магнитной полосой к картам с чипами, технологически более защищённым от несанкционированного воздействия. Также банкам следует непрестанно совершенствовать механизмы защиты банкоматов от установки скиммингового оборудования. В том числе периодически изменять настройки, увеличивать количество штатных видеокамер, устанавливать банкоматы исключительно в людных общественных местах и крупных учреждениях.

Если банки смогут обеспечить высокий уровень информационной безопасности, то это позволит свести к минимуму следующие риски [1]:

- риск потери, а также разрушения ценных данных;
- риск утечки информации, которая составляет служебную/коммерческую/банковскую тайну;
- риск распространения во внешней среде информации, которая будет угрожать репутации банка;
- риск использования неполной или искаженной информации в деятельности банка.

И, конечно же, нельзя забывать о работе по широкому освещению проблематики информационной безопасности. В том числе, о разработке рекомендаций для клиентов, выработке у них навыков безопасного использования банкоматов и других дистанционных сервисов, ведь безопасность банков, как известно, имеет две составляющие: безопасность со стороны банка и безопасность со стороны клиента [2].

Вторая составляющая предполагает обеспечение безопасности процедуры подтверждения клиентом платежа.

Данная задача решается посредством использования устройств защищенного хранения ключей электронной подписи (ЭП) и защищенной выработки электронной подписи, доверенных устройств отображения ключевых реквизитов и подписи платежного поручения, доверенных каналов подтверждения платежа, доверенной среды для работы с приложением «клиент – банк», а также посредством мониторинга платежей на предмет выявления подозрительных и потенциально мошеннических сделок.

Если говорить о безопасности платежных систем, признанным стандартом безопасности считается *Payment Card Industry Data Security Standard* (PCI DSS). В него вошли такие карточные брэнды как *Visa*, *MasterCard*, *American Express*, *JCB* и *Discovery*.

Основной акцент в стандарте *PCI DSS* делается на обеспечении безопасности сетевой инфраструктуры и защите хранимых данных о держателях платежных карт как наиболее уязвимых с точки зрения угроз конфиденциальности местах [11]. Также следует отметить, что стандарт регламентирует правила безопасной разработки, поддержки и эксплуатации платежных систем, в том числе процедуры их мониторинга. Не менее важную роль стандарт отводит разработке и поддержке базы нормативных документов системы менеджмента информационной безопасности.

Сертификация российских банков по зарубежному *PCI DSS* стандарту шла довольно медленно, а отечественного аналога на сегодняшний день нет.

Однако, выполняя пункты «Положения о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств…» и последней редакции СТО БР ИББС – 2014, можно во многом

подготовиться к прохождению сертификации по *PCI DSS*, ведь многие его положения пересекаются с требованиями из отечественного документа: антивирусная безопасность, шифрование, фильтрация с помощью межсетевых экранов, разграничение доступа, отслеживании сеансов связи, а также мониторинг, аудит и менеджмент системы информационной безопасности (ИБ) (см. Рисунок 1).

Категория информации	ФЗ «О НПС»	СТО БР	PCI DSS
Информация об остатках денежных средств на банковских счетах	+	+	–
Информация об остатках электронных денежных средств	+	–	–
Информация о переводах денежных средств	+	+	–
Информация о распоряжениях клиентов, участников платежной системы, ПКЦ	+	+	–
Информация о платежных клиринговых позициях	+	+	–
Информация, необходимая для удостоверения клиентами права распоряжения денежными средствами, в том числе ДПК	+	+	+
Ключевая информация СКЗИ	+	+	+
Информация о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, а также информации о конфигурации, определяющей параметры работы технических средств по защите информации	+	+	–
Информация ограниченного доступа, в том числе ПДн и иная информация, подлежащая обязательной защите в соответствии с законодательством России	+	+	+

Рисунок 1. *Сравнение категорий защищаемой информации различными стандартами* [6]:
ФЗ «О НПС» – Федеральный закон «О национальной платежной системе»; СТО БР – Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы РФ

Таким образом, СТО БР ИББС является очень важной вехой эволюционного пути развития отечественной системы обеспечения информационной безопасности. Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы – один из первых отраслевых и адаптированных под российскую действительность стандартов.

Выполняя требования стандарта, многие банки готовят себя к международной сертификации обеспечения безопасности платежных систем *PCI DSS*, обеспечивают защиту персональных данных в соответствии с последними требованиями регуляторов. Проводимый ежегодный внутренний аудит позволяет объективно проверить защищенность банков от существенных рисков и угроз ИБ, а руководителям – эффективнее спланировать построение и управление комплексной системой защиты. И, разумеется, нужно развивать программы, направленные на повышение грамотности населения в сфере компьютерной безопасности. Перед банками, обществом и государством стоят общие цели, поэтому нужно развивать взаимодействие между данными структурами и совершенствовать методики их взаимной работы.

Список литературы

1. **Информационная безопасность банков** [Электронный ресурс]. URL: http://www.arinteg.ru/articles/informatsionnaya-bezopasnost-bankov-26722.html (дата обращения: 06.07.2015).
2. **Информзащита собственными силами** [Электронный ресурс]. URL: http://nbj.ru/publs/upgrade-modernizatsija-i-razvitie/2014/02/05/informzaschita-sobstvennymi-silami/index.html (дата обращения: 06.07.2015).
3. **О внесении изменений в Положение Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»** [Электронный ресурс]: Указание Банка России от 05.06.2013 г. № 3007-У. URL: http://www.consultant.ru/document/cons_doc_LAW_148817/ (дата обращения: 06.07.2015).
4. **Об утверждении Положения о защите информации в платежной системе** [Электронный ресурс]: Постановление Правительства РФ от 13.06.2012 г. № 584. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW; n=131173 (дата обращения: 06.07.2015).
5. **Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения: Стандарт Банка России СТО БР ИББС-1.0-2014** [Электронный ресурс]: Распоряжение Банка России от 17.05.2014 г. № Р-399. URL: http://www.consultant.ru/document/cons_doc_LAW_163762/ (дата обращения: 06.07.2015).
6. **Особенности обеспечения информационной безопасности в банковской системе** [Электронный ресурс]. URL: http://www.antimalware.ru/analytics/technology_analysis/features_information_security_in_the_banking_system (дата обращения: 06.07.2015).
7. **Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств** [Электронный ресурс]: утверждено Банком России 09.06.2012 г. № 382-П. URL: http://www.consultant.ru/document/cons_doc_LAW_131473/ (дата обращения: 06.07.2015).

8. **Проблемы информационной безопасности банков** [Электронный ресурс]. URL: http://uchit.net/catalog/Bankovskoe_delo/81596/ (дата обращения: 06.07.2015).
9. **Путин подписал закон о создании национальной системы платежных карт** [Электронный ресурс]. URL: http://ria.ru/economy/20140505/1006613510.html (дата обращения: 06.07.2015).
10. **Ясенев В. Н.** Информационная безопасность в экономических системах [Электронный ресурс]: учебное пособие. Н. Новгород: Изд-во ННГУ, 2006. URL: http://www.iee.unn.ru/files/posobya/ib_yasenev.pdf (дата обращения: 06.07.2015).
11. **PCI DSS – Payment Card Industry Data Security Standard** [Электронный ресурс]. URL: http://partner.jcbcard.com/security/pcidss/index.html (дата обращения: 06.07.2015).

PECULIARITIES OF INFORMATION SECURITY OF BANKING SYSTEMS AND MEASURES FOR PROVIDING IT

Zhuravleva Valeriya Vadimovna
Tselykh Aleksandr Nikolaevich, Doctor in Technical Sciences, Professor
Southern Federal University
baleranka@mail.ru; ant@sfedu.ru

The article examines the principles of the information security of banking systems taking into account their specific peculiarities and differences from the information systems of other organizations, and also the requirements of the latest native Bank of Russia Standard for providing the information security of the organizations of the banking system of the Russian Federation. Measures are suggested to protect banking data, which are topical after the appearance of "Statute on Information Security in Payment System" and other by-laws. The analysis of the degree of reducing risks for banks providing the necessary level of information security is conducted.

Key words and phrases: information security; banking system; national system of payment cards; unauthorized access; skimming; phishing.

УДК 618.396; 612.129
Медицинские науки

Цель работы – определить диагностическую значимость концентрации ТФР-бета у пациенток с очень ранними преждевременными родами. В ходе исследования выявлено, что у пациенток с очень ранними преждевременными родами концентрация ТФР-бета – достоверно выше. В качестве предиктора очень ранних преждевременных родов данный диагностический тест имеет среднее качество в связи с тем, что чувствительность составила 52%.

Ключевые слова и фразы: очень ранние преждевременные роды; ТФР-бета; вульвовагинит; угрожающий выкидыш; отслойка плаценты; преждевременное излитие околоплодных вод.

Зильбер Марина Юрьевна, д. мед. н., профессор
г. Москва
aza7777777@gmail.com

Гребнева Ольга Сергеевна
Агаян Хаджак Гамлетович
Уральский государственный медицинский университет, г. Екатеринбург
aspirant-gkb24@mail.ru; hajak78@mail.ru

ДИАГНОСТИЧЕСКАЯ ЗНАЧИМОСТЬ КОНЦЕНТРАЦИИ ТФР-БЕТА У ПАЦИЕНТОК С ОЧЕНЬ РАННИМИ ПРЕЖДЕВРЕМЕННЫМИ РОДАМИ©

Частота преждевременных родов в мире в последние годы составляет 5-10% и, несмотря на появление новых технологий, не снижается. А в развитых странах она повышается, прежде всего, в результате применения новых репродуктивных технологий [7]. В связи с новыми критериями живорожденности, классификация преждевременных родов в соответствии со сроком гестации пересмотрена. Роды с 22 до 27 недель 6 дней включительно относятся к очень ранним преждевременным родам или сверхранним родам [1]. По данным различных авторов, рождается около 5% глубоко недоношенных детей, которые имеют экстремально низкую массу тела (до 1000 г). Прогноз – крайне неблагоприятный, так как преждевременные роды в данном сроке являются основным фактором, определяющим неонатальную смертность и заболеваемость, и имеют долгосрочные, неблагоприятные последствия для здоровья детей. Формирование инвалидности с детства приводит к тому, что эта проблема выходит за рамки медико-биологической и приобретает социальное значение [8; 9; 14]. В связи с этим важным является определение предикторов преждевременных родов.

© Зильбер М. Ю., Гребнева О. С., Агаян Х. Г., 2015