УДК 336

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ БАНКА

Бабукин Г.М.

Студент 4 курса

Финансовый университет при Правительстве Российской Федерации,

Москва, Россия

Аннотация

В данной статье автором подчеркивается важность использования информационных технологий в обеспечении безопасности банка. Рассмотрены основные проблемы обеспечения безопасности банка. Изучены основные инструменты обеспечения банковской безопасности на практике. Автор акцентирует внимание на использовании банками электронных векселей. Разработан механизм обеспечения безопасности банка.

Ключевые слова: информационные технологии, безопасность, банк, риск, методики, инструменты.

USE OF INFORMATION TECHNOLOGIES IN ENSURING THE SECURITY OF THE BANK

Babukin G.M.

4rd year student

Financial University under the Government of the Russian Federation

Moscow, Russia

Summary

In this article, the author emphasizes the importance of using information technology in ensuring the security of the bank. The main problems of ensuring the bank's security are considered. The main tools for ensuring banking security in practice have been studied. The author focuses on the use of electronic bills by banks. A mechanism for ensuring the bank's security has been developed.

Key words: information technology, security, bank, risk, techniques, tools.

Современные достижения науки и техники превратили информацию в продукт, который можно покупать, продавать и обменивать. Стоимость информационных данных часто во много раз превышает стоимость всей технической системы, хранящей и обрабатывающей информацию. Качество деловой информации обеспечивает современным банкам и организациям необходимый экономический эффект. Поэтому важно защитить важные информационные данные от незаконной деятельности. Это позволяет коммерческим банкам успешно выжить на рынке.

Использование информационных технологий в обеспечении безопасности банка представляет собой такое положение информационной базы, в которой минимизировано или вообще исключено внешнее вмешательство или отрицательные воздействия со стороны третьих лиц.

Безопасность данных также включает управление рисками, связанными с раскрытием информации или воздействием на аппаратные и программные модули безопасности. Безопасность информации, обрабатываемой в банке, состоит из ряда мер, направленных на решение проблемы защиты информационной среды. При этом информация не должна ограничиваться в использовании и динамическом развитии уполномоченными лицами. На основании вышеизложенного проблема внедрения и использования информационных технологий в обеспечении

банковской системы представляется наиболее актуальной и остро стоящей во время высокоскоростной автоматизации XXI века.

Структурирование концепции банковской безопасности представляет собой комплекс задач, направленных на создание и оперирование в деятельности банка системы защиты с использованием современных информационных технологий.

Создание такой системы защиты на практике обусловлено решением большого количества проблем. Сюда входят задачи организации концепций по повышению правовой, нормативной, методической, научной, технической и организационной безопасности; создание целевого информационного контента для защиты имущества, инфраструктуры и информационной базы данных банка.

Принимая во внимание гипотезы по модернизации работы отделений банковской системы с клиентами и увеличения степени производительности бизнес-операций, рекомендуется модернизировать систему публичности информационных данных и применять безопасный интернет-контент и сайты для реализации банковской деятельности.

Денежные средства физических лиц являются основным источником фондирования активной деятельности банков в виду тех фактов, что рынок розничных кредитов и вкладов физических лиц систематически набирает высокие темпы, что в свою очередь непосредственным образом отражается на качестве банковской деятельности в целом. На данный момент реализован проект поэтапного перехода к модели Electronic Sparkasse, которая предусматривает получение всех видов банковских услуг дистанционно – в удаленном формате. Сейчас этот проект внедрен в программы мобильных терминалов и терминалов самообслуживания.

Предполагается, что осуществление поставленных задач будет способствовать наилучшей координации и закреплению позиций на рынке

вкладов и кредитов физическим и юридическим лицам, а также – в свою очередь – обеспечить безопасность.

Электронный документооборот в современной банковской системе набирает обороты, в связи, с чем увеличивается ценность электронно-цифровых подписей, что также является залогом безопасности проводимых банковских операций. Направления развития электронного денежного обращения основываются на организации и обращении электронных денег.

Если эти транзакции выполняются в электронном виде и подписываются электронной подписью, то соответственно будет формироваться электронный счет. В связи с этим приобретает особую актуальность такой электронный документ как электронно-переводной вексель. Он представляет собой электронный документ, который может быть применен для обналичивания денежных средств. Данный документ имеет широкое мировое распространение.

Электронный вексель обеспечивает безопасность совершаемых банков операций за счет:

1) личного присутствия в момент получения процентов или основной суммы выплаты по векселю, что является, в свою очередь, простым и надежным способом защиты личных средств;

2) все операции в обязательном порядке подтверждаются через отправку смс-кода на личный мобильный телефон инвестора.

В России уже были безуспешные попытки выступить против «монополии», инициированной Федеральной комиссией по рынку ценных бумаг Российской Федерации по введению электронной валюты в безбумажной форме. Минэкономразвития России сделало это сегодня, в этом видятся большие перспективы и уже развивается система электронного выставления счетов. Похоже, что банковской системе придется пойти на компромисс во второй раз, поскольку очевидно, что незаконные и недоступные по цене технологии могут только отсрочить появление

электронных денег и обращение векселей и тем самым потерять большую часть своего контроля в будущем, что естественным образом может отрицательно отразиться на безопасности информационных данных банковской системы.

Еще одна актуальная проблема – это проблема защиты информации в банках. В настоящее время существует большое количество организационных и технических средств защиты от информационных атак.

Организационные инструменты связаны с разработкой и внедрением нормативных документов в компаниях, определяющих требования информационной безопасности AIS [3].

Технические средства защиты AIS реализуются с использованием соответствующих программных, аппаратных или программно-аппаратных комплексов. Можно выделить следующие основные виды технических средств защиты: «криптографическая защита информации; разграничение доступа пользователей к ресурсам АИС; межсетевой экран; анализ безопасности АИС; обнаружение информационных атак; защита от вируса; анализ информационного содержания; защита от спама».

Инструменты криптографической защиты информации банков (CIPF) – это преобразование информации для обеспечения ее конфиденциальности и контроля целостности. Защита информации банков может реализовываться во время передачи по каналам связи или во время хранения и обработки в узлах AIS. Для решения этих проблем используются различные типы криптографических информационных систем.

Средства контроля доступа предназначены для защиты от несанкционированного доступа к информационным ресурсам системы.

Банкам в России также было разрешено использовать биометрические данные для идентификации клиентов в Интернете. Соответствующий законопроект был принят Госдумой в третьем и окончательном чтении 23 декабря 2020 года. Он был разработан группой депутатов Госдумы под

руководством председателя комитета по финансовым рынкам Анатолия Аксакова и значительно улучшен во втором чтении. Как поясняет ТАСС, новый закон дает банкам с базовой лицензией право собирать биометрические данные в единой биометрической системе (теперь они обязаны это делать по закону) и вводит такое обязательство для банков с универсальной лицензией. Банки с универсальной лицензией обязаны предоставлять физическим лицам возможность открывать счета (вклады) в рублях и получать ссуды в рублях без личного присутствия, идентифицируя клиентов – физических лиц в установленном законодательством порядке. Банк предлагает эту возможность через свой официальный сайт в Интернете, а также через мобильное приложение, которое соответствует критериям, установленным центральным банком.

28 декабря «Ростелеком» представил итоги работы Единой биометрической системы в уходящем 2020 году. Как утверждает компания (оператор системы), данные в ЕБС можно сдавать в 13 300 отделений 231 банка, расположенных в 95% населенных пунктов России.

К концу 2020 года общее количество скачиваний приложения «Биометрия» от «Ростелекома», с помощью которого производится удаленная идентификация, превысило 250 тысяч. В 2020 году «Ростелеком» занимался расширением клиентских сервисов на базе биометрии, велась активная техническая и нормативная подготовка к запуску новых массовых биометрических проектов. Так, в феврале 2020 года запущен пилотный проект по биометрической оплате в сети кофеен Coffee Bean.

Учитывая, что ЕБС защищена по высоким требованиям информационной безопасности, а ее функционирование технологически связано с функционированием системы, предоставление дистанционных услуг с использованием Единой биометрической системы обеспечит достоверную идентификацию физических лиц, надежную защиту

биометрических персональных данных, а также пресечение мошеннических действий при оказании банками дистанционных услуг.

Также биометрическая идентификация не является единственной технологией для подтверждения личности клиента банковских услуг; в тех же целях могут использоваться камеры наблюдения или системы слежения за зрачками глаз.

Процесс использования и оперирования современными информационными технологиями распахнул для банков массу разнообразных возможностей управления рисками, позволил разработать и апробировать продвинутые формы и модели продуктивного обслуживания клиентов и дальнейшей диверсификации банковской деятельности.

Процесс активного использования информационных технологий в банковском деле способствует минимизации рисков и компенсации недостатков в работе банковской системе. В связи с тем, что банковский сектор является наиболее уязвимым для злоумышленников и мошенников, финансово-экономическая система заинтересована во всеобщей глобализации и апробации информационных ресурсов [1,с.24].

После радикального рыночного реформирования банковский сектор страны кардинально модернизировался: не только количественными, но и качественными показателями, что обуславливает работу банков через призму финансово-рыночных отношений, что создает, в свою очередь, благоприятные условия для развития конкуренции на рынке банковских услуг.

Таким образом, на основании проведенного анализа актуального использования информационных технологий в обеспечении безопасности банка необходимо выделить проблемные стороны, которые требуют радикальных мер:

1) развитие информационных технологий в целом намного опережает систему безопасности банковского сектора, необходимо этот пробел исключить, иначе апробированные инструменты теряют смысл;

2) вечная проблема – персонал банка. В большинстве случаев решающую роль в обеспечении защиты информационных данных банка играет человеческий фактор: необходимо детальное урегулирование систематической обучаемости персонала различным новшествам и внедрения их в работу банков.

В данной статье нами разработан механизм обеспечения безопасности банка, включающий себя комплекс практических рекомендаций. Данный механизм представлен на Рисунке 1.

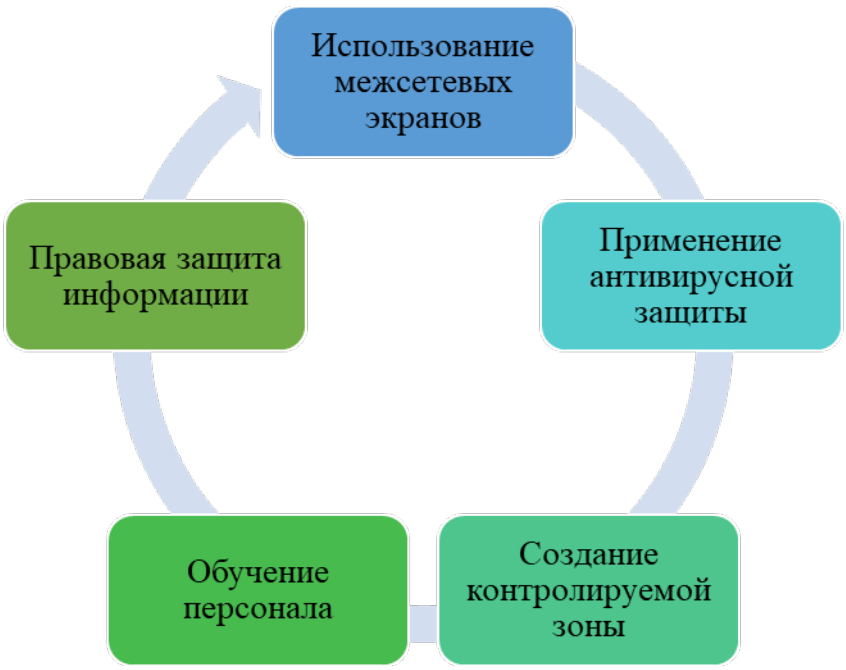

Рис.1. Механизм обеспечения безопасности банка

Считаем, что такой механизм позволит повысить безопасность банков. Основой его реализации является использование грамотного подхода к применению инструментов и методов к обеспечению безопасности.

Синергетический эффект достигается за счет реализации комплексного подхода.

Библиографический список

1. Гамза В.А. Безопасность банковской деятельности / В.А. Гамза, И.Б. Ткачук, И.М.Жилкин - М.: Юрайт, 2017. - с. 96.

2. Левшин М.А. Информационные технологии в Российских банках и безопасность данных. - Финансовый Университет при Правительстве Российской Федерации, 2020.

3. Партыка, Т.Л. Информационная безопасность. - М.: Форум, Инфра-М, 2019. - 368 с.

4. Щелканов А.А., Форгунова А.Ю. Экономическая безопасность кредитных организаций в условиях трансформации финансового сектора. - Международный банковский институт им. Анатолия Собчака, 2020.

5. Ясенев, В.Н. Информационная безопасность. - Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с.

Оригинальность 93%