УДК 336.719.2

Т. Е. Шилкина, Р. Р. Хайров
Саранский кооперативный институт (филиал) АНОО ВО ЦСРФ «Российский университет кооперации», Республика Мордовия, г. Саранск,
email: tekuznetsova89@mail.ru; r.r.khairov@ruc.su

ОЦЕНКА ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КРЕДИТНОЙ ОРГАНИЗАЦИИ

Ключевые слова: экономическая безопасность, банк, риски, угрозы, финансовые показатели, чистая прибыль, мобильный сервис, рекомендации, клиент, оценка.

В статье ставится акцент на актуальность решения вопросов по повышению эффективности механизма по обеспечению экономической безопасности кредитной организации, проблемы по предотвращению угроз и минимизации рисков в банковской системе. В статье раскрывается взаимосвязь финансовой устойчивости банка и его действующей системы экономической безопасности, приводятся результаты анализа основных финансовых показателей ПАО «Сбербанк России», описывается механизм по предотвращению и минимизации рисков хищения денежных средств клиентов Сбербанка с использованием вредоносного программного обеспечения. Авторы обобщили рекомендации защиты от социального инжиринга, разработанные для клиентов ПАО «Сбербанк России», раскрыли сущность системы фрод-мониторинга банка. В статье описываются направления дальнейшего развития системы обеспечения экономической безопасности банка.

T. E. Shilkina, R. R. Hairov
Saransk Coope rative Institute (bra nch) of Rus sian University of Cooperation, Republic of Mordovia, Saransk, email: egkuznecova@mail.ru; r.r.khairov@ruc.su

ASSESSMENT OF ACTIVITIES TO ENSURE ECONOMIC SECURITY OF A CREDIT ORGANIZATION

Keywords: economic security, bank, risks, threats, financial indicators, net profit, mobile service, recommendations, client, assessment.

The article reveals the relevance of the problem of a credit institution to prevent threats and minimize risks in the banking system, the relationship between the financial stability of the bank and the effectiveness of its current economic security system, provides the results of the analysis of the main financial indicators of Sberbank of Russia, describes the mechanism for preventing and minimizing the risks of money theft. funds of Sberbank clients using malicious software. The authors summarized the recommendations of protection against social engineering, developed for the clients of Sberbank of Russia, and revealed the essence of the bank's fraud monitoring system. The article describes the directions of further development of the system for ensuring the economic security of the bank.

Функционирование организаций, в т.ч. и кредитных, в условиях рыночных отношений направлено на получение прибыли. Осуществляя свою деятельность, банки сталкиваются с воздействием внешних и внутренних факторов на финансовые результаты компании. Влияние может быть, как позитивным, так и носить негативный характер.

Способность банка противостоять неблагоприятным воздействиям и угрозам напрямую зависит от его финансового состояния и от эффективной работы его системы экономической безопасности [1]. Финансовая устойчивость является ресурсом безопасности, а система обеспечения экономической безопасности кредитной организации являясь совокупностью способов и методов, правил и процедур, используемых специалистами и сотрудниками банка для предотвращения угроз его экономической безопасности, обеспечивает развитие и рентабельность деятельности банка.

Цель исследования

Учитывая такую тесную взаимосвязь двух показателей, рассмотрим современные приемы и способы работы по обеспечению экономической безопасности на примере ПАО «Сбербанк России» – одного из ведущих банков страны.

Материал и методы исследования

Согласно среднестатистическим данных за период 2017-2020гг., у банка насчитывается более 151 млн. клиентов по всему миру, из них 134,7 млн. клиентов в России и 16,3 млн. за ее пределами. В совокупности активными клиентами у ПАО «Сбербанк России» являются около 60% населения страны. К качественным характеристикам деятельности ПАО «Сбербанк России» можно отнести:

– количество активных частных клиентов – 86,2 млн. человек;

– численность корпоративных клиентов – 2,1 млн. компаний;

– численность активных пользователей удалённых каналов – 57 млн. человек;

– мобильное приложение «Сбербанк Онлайн» используют 32,6 млн. активных клиентов [2].

Кроме качественных характеристик деятельности банка, рассмотрим динамику его финансовых показателей. Его характеристика основных финансовых показателей представлена в таблице 1 [3].

На основании данных таблицы можно сделать вывод, что за исследуемый период наблюдается положительная тенденция роста всех основных показателей деятельности банка. Операционный доход до резервов увеличился на 472 млрд. руб. за счет чистого процентного дохода и чистого комиссионного доходов. Чистая прибыль Сбербанка в 2017 году составила 654 млрд. руб. Ее максимальное значение достигнуто в 2019 году с увеличением по сравнению с 2017 годом на 29,5%. Изменения условий функционирования в т.ч. пандемия повлияли на уменьшение размера чистой прибыли до 782 млрд. руб. или 7,7% к показателю 2019 года. Относительные изменения за период 2017-2020гг. по чистой прибыли составляют 119,6%, а по операционному доходу до резервов – 128,2%.

Согласно международной регуляторной практике кредитный риск оценивается и в последующем используется для определения достаточности собственного капитала с позиции покрытия непредвиденных потерь кредитной организации и для оценки возможных потерь с целью формирования резервов по требованиям кредитного характера [4]. У кредитного портфеля ПАО «Сбербанк России» высокое качество, на это указывает увеличение резерва под обесценение кредитного портфеля в 2020 году по сравнению с 2017 годом на 511 млрд. руб. Активы банка возросли на 9859 млрд. руб. или на 142,3% по сравнению с 2017 годом и составили 33146 млрд. руб. в 2020 году. Средства физических лиц и корпоративных клиентов увеличились на 3586 млрд. руб.

При этом рентабельность активов банка уменьшилась за исследуемый период на 0,4%, а рентабельность капитала снизилась на 4,7%. Оценивая финансовые показатели Сбербанка, можно сделать вывод о финансовой устойчивости кредитной организации и ее возможности дальнейшего совершенствования действующей системы безопасности.

Результаты исследования и их обсуждение

На наш взгляд, эффективная система безопасности кредитной организации заключается в нахождении оптимального соотношения между нейтрализованными рисками и угрозами, затраченными на это ресурсами и прибыльностью от деятельности кредитной организации.

Обеспечение безопасности работы банковских систем и сервисов в настоящее время является одной из приоритетных задач ПАО «Сбербанк России». С учетом высокотехнологичного внешнего влияния на деятельность кредитной организации, ПАО «Сбербанк России» активно противодействует киберугрозам и мошенничеству. В этих целях Сбербанк на постоянной основе проводит анализ потенциальных и реализованных рисков, на основании результатов которого усиливает меры защиты с учетом новых угроз.

Современное общество характеризуется быстрым развитием новых технологий, в банковской сфере это выражается в появлении новых сервисов и услуг, представляемых клиентам [7]. Одним из таких новых продуктов являются мобильные сервисы. С их созданием у банка появились обязательства нового уровня по защите клиентов от киберугроз.

Специалисты службы безопасности Сбербанка внимательно изучают информацию о поступающих угрозах и реализуют адекватные механизмы защиты денежных средств и информации о своих клиентах.

Таблица 1

Динамика финансовых показателей ПАО «Сбербанк России» за 2017-2020гг.

Показатели		2017г.	2018г.	2019г.	2020г. абсол.	Отклонение 2020/2017	
						относ.	
Отчет о финансовых результатах	Операционный доход до резервов, млрд. руб.	1672	1838	1821	2144	472	128,2
	Чистая прибыль, млрд. руб.	654	811	847	782	128	119,6
Баланс	Резерв под обеспечение кредитного портфеля, млрд. руб.	1061	1207	1210	1572	511	148,2
	Активы, млрд. руб.	23287	27034	27695	33146	9859	142,3
	Средства физических лиц млрд. руб.	12125	13039	13625	15711	3586	129,6
Качественные показатели	Рентабельность активов, %	3,0	3,3	3,1	2,6	-0,4	-
	Рентабельность капитала,%	21,2	22,6	20,5	16,5	-4,7	-

Рис. 1. Меры, разработанные ПАО «Сбербанк России», по предотвращению угроз вредоносного программного обеспечения стационарного компьютера и мобильных устройств

В этих целях, ПАО «Сбербанк России» углубляет, повышает качество взаимодействия по повышению безопасности с производителями мобильных устройств и программного обеспечения, операторами сотовой связи, экспертами по кибербезопасности, создателями антивирусов и операционных систем. Все они являются активными участниками рынка мобильных сервисов.

Специалистами банка разработаны специальные рекомендации для клиентов, использующих возможности мобильного телефона, планшета или компьютера, ими применяется современные методы по предотвращению и минимизации рисков хищения денежных средств клиентов с использованием вредоносного программного обеспечения.

Все эти инструменты можно подразделить на два вида:

– для пользователей мобильных устройств;

– для пользователей стационарной компьютерной техники.

Мобильное приложение «Сбербанк-онлайн» устанавливается на мобильные устройства уже со встроенным антивирусом, который позволяет защищать не только информацию и данные приложения, но и операции всего телефона. Пользователь, установив и зарегистрировав приложение, может быть уверен в полной сохранности своих средств. Отличительной особенностью мобильного «Сбербанк-онлайн» является активность антивируса даже в тот момент, когда клиент не пользуется приложением.

Подразделение экономической безопасности банка на регулярной основе отслеживает и анализирует потенциальные риски своих сервисов. При оценке риска банк применяет международные стандарты безопасности и лучшие практики. Так услуга «Мобильный банк» имеет уровень удельного риска для сопоставимых типов операций значительно ниже, чем у такого крупного международного игрока, как PayPal.

Центр киберзащиты Сбербанка ежедневно обрабатывает события, связанные с вредоносным ПО. Статистика показывает достаточную регулярность DDoS-атак на свои системы различной мощности, так в 2018 году Сбербанком было отражено 90 таких нападений.

Сбербанк противодействует фишингу, это когда с помощью поддельных интернет – страниц, злоумышленники получают аутентифиционные данные клиента и получают доступ к управлению его картами и счетами. Поэтому банк проводит мониторинг интернет-ресурсов. Так банк выявляет и противодействует схемам мошенничества, которые используют бренд Сбербанка, в том числе маскирующиеся под страницу для входа в Сбербанк онлайн.

Киберпреступники сегодня активно используют методы социального инжиринга, когда клиенты сами сообщают злоумышленникам данные, необходимые для осуществления переводов денежных средств от их имени. ПАО «Сбербанк России» разработал меры по предотвращению и минимизации рисков хищений денежных средств с использованием методов социального инжирнга. К таким можно отнести мероприятия по повышению осведомленности клиентов о возможных видах мошеннических действий и оценке ситуаций, использование современных аналитических приемов, позволяющих осуществлять онлайн-выявление подозрительных (несвойственных клиенту) операций (системы фрод-мониторинга).

Элементом действующей системы экономической безопасности банка является распространение и применение рекомендаций по защите от социального инжиринга при общении по телефону или электронной почте.

На экономическую безопасность Сбербанка и его клиентов влияет скимминг, когда крадут данные банковской карты при помощи специальных устройств, а после создают ее дубликат. В целях предотвращения угроз банк устанавливает антискимминговое оборудование (АСО), оперативно реагирует на сообщения о возможной установке нештатного оборудования, использует систему фрод-мониторинга, выявляет и блокирует карты и учетные записи клиентов банка, участвующих в схемах вывода похищенных средств.

Из вышеизложенного можно увидеть, что огромный вклад в обеспечении безопасности вносит система фрод-мониторинга Сбербанка, работа которой основана на искусственном интеллекте.

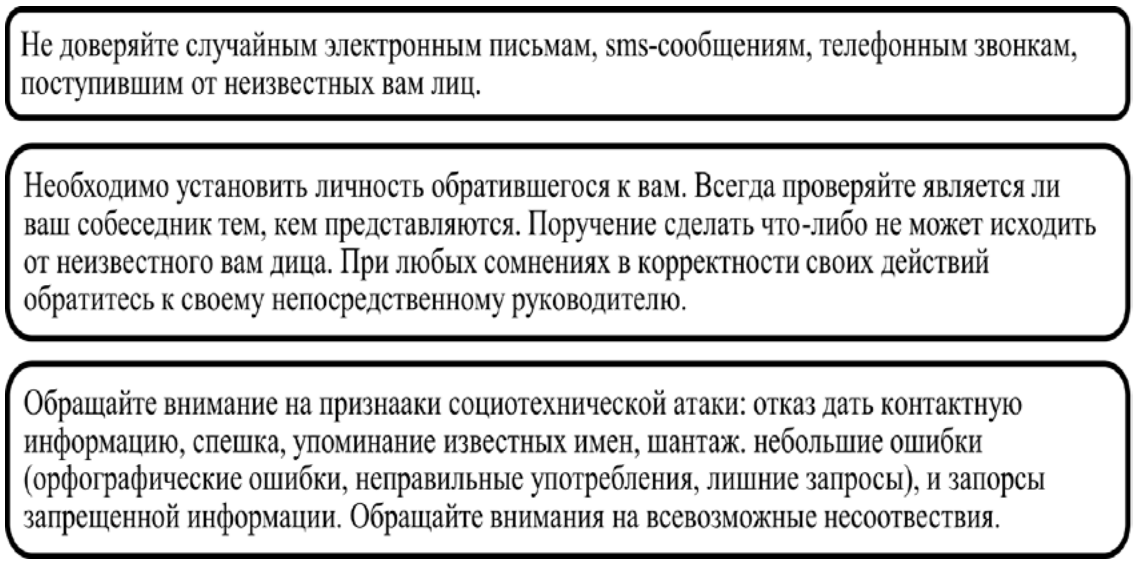

Рис. 2. Рекомендации защиты от социального инжиринга клиентам ПАО «Сбербанк России» [5]

Система проводит интеллектуальный анализ данных, обнаруживает подозрительные операции и исследует их. Сбербанк использует и продолжает разрабатывать собственную и единую клиентскую базу по физическим и юридическим лицам, обеспечивающую устойчивое удовлетворение требований бизнеса – АС «СТОП-ЛИСТ». Ее основная задача является автоматизированный учет информации, поступающей в виде предписаний государственных органов, а также информации, полученной в ходе реализации основной деятельности банка, с целью обеспечения минимизации операционных и репутационных рисков. Система реализовывает поиск паспортов в базе недействительных паспортов МВД России.

С 2018 года для защиты данных от мошенников ПАО «Сбербанк России» используют биометрию. Это надежная форма обеспечения безопасности, которая осуществляет идентификацию клиента по его уникальным чертам (например, по лицу или голосу).

Выводы

В настоящее время в Сбербанке реализуется проект по развитию риск-культуры организации, являющейся частью ее сферы управления рисками в целом. Риск-культура по своему содержанию представляет собой убеждения, ценности, разделяемые и применяемые персоналом банка. Целью данного проекта определено формирование у сотрудников банка стиля поведения, который обеспечивает открытость обсуждения и правильную реакцию на существующие и потенциальные риски. Кроме того, создаваемый поведенческий стиль персонала Сбербанка предусматривает проявление нетерпимости к замалчиванию или игнорированию рисков и рискового поведения окружающих.

Дальнейшее совершенствование системы обеспечения экономической безопасности ПАО «Сбербанк России» заключается в работе по: изучению рынка банковских услуг; регулированию текущих расходов; отслеживанию состояния рентабельности; совершенствованию процедур управления кредитом; проверке и оценке финансового состояния заемщика; роботизации операционных процессов; расширению и улучшению биометрической системы обслуживания клиентов; информированию населения о видах мошенничествах и способах защиты; организации тренингов, семинаров специалистам и работникам, клиентам Сбербанка на тему стрессоустойчивости и реагирования на действия мошенников и прочие мероприятия.

Библиографический список

1. Экономическая безопасность коммерческого банка, [учеб. пособие] / [авт.-сост.: Е.Г. Кузнецова, М.В. Мягкова, Т.Е. Шилкина]; Саран. кооп. ин-т (фил.) РУК. – Саранск: АО «Ковылкинская типография». – 99 с.

2. ПАО «Сбербанк России»: официальный сайт: [Электронный ресурс]. – Режим доступа: https://www.sberbank.ru/ru/person.

3. ПАО «Сбербанк России»: официальный сайт: [Электронный ресурс]. – Режим доступа: https://www.sberbank.com/ru/investor-relations/reports-and-publications

4. Мягкова М.В., Шилкина Т.Е., Захаркина Р.А. Деятельность финансовых кредитных организаций по обслуживанию физических лиц // Экономика и предпринимательство. 2020. №4 (117). С. 963-967

5. Портал Банки.ру.: [Электронный ресурс]. – Режим доступа: http://www.banki.ru.

6. Центральный банк Российской Федерации: официальный сайт: [Электронный ресурс]. – Режим доступа: https://www.cbr.ru.

7. Мягкова М.В. Организация деятельности коммерческого банка [учеб. пособие] / М.В. Мягкова; Саран. кооп. ин-т (фил.) РУК. – Саранск: АО «Ковылкинская типография». – 129с.