ПОЛИТИКА БАНКА РОССИИ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ В БАНКАХ

POLICY OF THE BANK OF RUSSIA IN THE FIELD OF PROTECTION OF INFORMATION IN BANKS

УДК 336.71+336.74

Щепкин Михаил Алексеевич, студент, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации, г. Москва
Александрова Лариса Станиславовна, научный руководитель, к.э.н., доцент Департамента банковского дела и финансовых рынков, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации, г. Москва

Shchepkin M.A. ergoproxy000name@gmail.com
Aleksandrova L.S. als.007@yandex.ru

Аннотация

В данной статье проводится анализ формирования политики Банка России в сфере информационной безопасности. Высокий уровень информационной защищенности является одним из ключевых факторов функционирования банковской системы. Актуальность изучения связана с тем, что с развитием и внедрением информационных технологий в кредитно-финансовую сферу, возникают новые риски и угрозы, которые в разной степени препятствуют функционированию системы. Рассмотрены основные аспекты формирования нормативных документов Банка России. Также приведена цель и сформулированы основные задачи, ставящие перед собой Банк России. Проведено изучение изданных Банком России указов по снижению рисков кибербезопасности. Отражены основные тенденции и

сценарии развития информационной безопасности, основываясь на различных вариантах противодействующих событий, связанных с киберпреступлениями.

Annotation

This article analyzes the formation of the Bank of Russia's policy in the field of information security. A high level of information security is one of the key factors in the functioning of the banking system. The relevance of the study is due to the fact that with the development and implementation of information technologies in the credit and financial sphere, new risks and threats arise that to varying degrees hinder the functioning of the system. The main aspects of the formation of regulatory documents of the Bank of Russia are considered. The purpose and main objectives of the Bank of Russia are also presented. The study of decrees issued by the Bank of Russia to reduce cybersecurity risks was conducted. The main trends and scenarios of information security development are reflected, based on various variants of counteracting events related to cybercrime.

Ключевые слова: кибербезопасность, Банк России, политика Банка России, кибер-риск, информационная безопасность, киберустойчивостью, банковский сектор, киберпреступлений, киберугрозы, киберзащита.

Keywords: cybersecurity, Bank of Russia, Bank of Russia policy, cyber risk, information security, cyber resilience, banking sector, cybercrime, cyber threats, cyber defence.

Банковская система постоянно является для злоумышленников привлекательной мишенью, в том числе и в киберпространстве. Почти всегда информация, обрабатываемая в банковской среде, эквивалентна деньгам. В России, по данным Центра мониторинга и реагирования на кибератаки в банковской сфере, по итогам 2019 г. объем несанкционированных операций со счетов организаций составил 6,43 млрд руб. (в 2018 – около 1,5 млрд руб.,

в 2017 г. – 1,57 млрд руб., в 2016 г. – 1,89 млрд руб., в 2015 г. – 3,7 млрд руб.) [1]. Именно поэтому вопросу обеспечения информационной безопасности в банках традиционно уделяется много внимания со стороны государства. На сегодняшний день основным регулятором, занимающимся вопросами обеспечения информационной безопасности в банковском секторе, является Банк России.

Именно политика Центрального банка Российской Федерации определяет систему взглядов на положение кибербезопасности и представляет собой систематизированный перечень целей и задач защиты, как свод инструкций, регламентов, правил и процедур в области обеспечения информационной безопасности, которыми обязан руководствоваться коммерческий банк в своей деятельности. Под политикой понимается совокупность документированных управленческих действий, направленных на обеспечение безопасности всех видов информационных систем в банке, к этому можно отнести документооборот, а также обмен речевой конфиденциальной информации. Обеспечение информационной безопасности в банковском секторе требует формирования системы правового регулирования, которая включала бы полномочия Банка России по организации такого обеспечения и установление определенных требований к участникам банковского сектора [2].

Под угрозой безопасности подразумевается набор факторов, которые создают риск несанкционированного доступа к данным и их последующим уничтожением, изменением, блокировкой, копированием, распространением.

Цель политики Центра Банка РФ в данном направлении — это постоянное совершенствование нормативного регулирования информационной безопасности, а также обеспечение реальной защищенности банковской сферы от различного рода информационных угроз, кибератак и прочей компьютерной преступности [3].

В области информационной безопасности и киберустойчивости можно выделить основные задачи, которые ставит перед собой Банк России:

1. Обеспечение устойчивости к кибератаками:

2. Защита прав потребителей через мониторинг показателей уровня финансовых потерь.

3. Поддержка развития инновационных технологий и обеспечение необходимого уровня информационной безопасности.

Далее будут рассмотрены более значимые указы, стандарты и проекты регулятора по решению определенно возникших проблем, и результаты их введения, а также вкратце описано мнение различных источников и дано свое соображение по этому поводу.

Одним из наиболее важных документов такого плана является указ от 7 мая 2018 года №4793, изданный Банком России, принимающий ряд мер для повышения уровня кибербезопасности при проведения финансовых операций [4]. В вышеназванном Указе ЦБ РФ в обеспечении информационной безопасности применяется следующее:

- Банк России обязал банки раскрывать финансовый ущерб от кибератак. В 2017 году финансовый сектор столкнулся с волной кибератак; согласно официальным данным ЦБ РФ, общий объем хищения в России в результате кибератак составил 2,0 млрд. рублей. С 1 июля 2018 года изменил форму отчетности, связанным с нарушением обеспечения киберзащиты. По нашему мнению, данное введение позволило повысить достоверность данных о случаях, так как, предоставляемая информация позволит более точно оценить качество системы безопасности банка и в дальнейшем позволит сфокусироваться на более уязвимых местах информационной системы.

- Банк России ввел гост по информационной безопасности. С 1 июля 2018 года внедрен стандарт оказания услуг в кредитно-финансовом секторе [5]. На наш взгляд, это позволило систематизировать информационную составляющую банков, ужесточить контроль над процессами и событиями в системе и своевременное обнаружить нарушения, при этом позволяет отследить подозрительный исходящий трафик,

связанный с активностью вредоносных программ, в том числе используемых и для хищения информации. Введение позволит вовремя обнаружить любую подозрительную активность в пределах защищенной сети.

Для Центробанка РФ критически важно своевременно получать информацию по каким-либо информационным происшествиям и в дальнейшем создать ряд противодействующих мер по возникшим проблемам. Для реализации подобных задач был создан специальный департамент информационной безопасности [6]. Он разрабатывает методологию и обеспечивает развитие информационной безопасности в банковском секторе с учетом мировых трендов по всем основным направлениям.

Центробанк РФ пристально следит за исполнением своих указов банками, чтобы те, в свою очередь, тщательно выполняли возлагаемые на них обязательства. Так 17 апреля 2019 года ЦБ ввел новое наказание для банков за плохую киберзащиту. Из-за таких случаев специально была запущена новая характеристика для кредитных организаций — риск-профиль по уровню информационной безопасности, которая отражает вероятность возникновения проблем у банка из-за несоблюдения норм [7].

По нашему мнению, данный показатель показывает уровень защищенности информационный системы банка и позволяет оценивать, как руководство банка справляется с возникающими киберугрозами. В зависимости от этого показателя по уровню кибербезопасности ЦБ дает банкам определенные рекомендации, а для банков с низкими показателями могут быть предусмотрены штрафы и усиление надзора.

Результатом этого введения является то, что в начале марта 2020 года Центробанк РФ оштрафовал два банка за отсутствие систем распознавания мошеннических операций. По заявлению первого замдиректора департамента информационной безопасности Центра Банка Артема Сычева, в ходе плановых проверок в двух банках отсутствовала система распознавания мошеннических операций, а именно технологии антифрода. Более того ЦБ

РФ осуществил 109 проверок банков на предмет киберустойчивости, в ходе которых было выявлено более 730 нарушений. Около 80% из них так или иначе связаны с недостаточной защитой информации внутри кредитной организации [8].

Чтобы атаки не приводили к таким серьезным последствиям, Банк России постоянно следит за киберустойчивостью финансовых организаций, старается предупреждать их о возможных новых типах атак и способах реагирования на них.

Сколько бы ни была надежна информационная безопасность в банках, в большинстве случаев в мошеннических операциях определенную роль играет человеческий фактор. Только в 2020 году 68% от общего количества киберпреступлений пришлась на социальную инженерию. По сравнению с 2018 г. клиенты стали немного осторожнее: на социальную инженерию приходилось 97% мошеннических операций [9].

Проблема заключается в том, что клиент сам нарушает конфиденциальность своей банковской карты, если он сообщил номер карты, пароль из СМС, CVV-код или любым другим способом передал информацию о своей банковской карте. Банк России старается предотвратить такие преступления путем введения обязательств для банков, чтобы те проверяли устройства клиентов, которые они используют [10]. Система собирает множество параметров: информация о самом устройстве, в какой области чаще всего работает, время работы устройства, особенности использования устройства, все действия пользователя в системе фиксируются. Словом, все эти параметры собираются воедино, что позволяет системе выявлять подозрительные моменты поведения и нарушения шаблонов, одним словом, отличать мошенников от обычных пользователей. [11, с.217] К тому же ЦБ РФ применяет механизм, позволяющий различать мошеннические сайты (в том числе и сайты, принимающие оплату) и принимать определенные меры по их устранению.

Новейшие технологии формируют огромный спектр новых источников для развития банковской сферы, но одновременно с этим возникают другие проблемы с кибербезопасностью. Киберугрозы образуются в виде ориентированно спланированных атак на определенные системы различных компаниях. Исходя из этого, каждая система кредитно-финансовой организации система требует серьезных модернизаций, чтобы она могла надлежащим образом противостоять этим атакам.

По результатам анализа документов можно сделать однозначный вывод, что политика Банка России отражает тенденцию к усилению нормативного регулирования информационной безопасности в банковской сфере. При этом особое внимание уделяется обеспечению реальной защищенности участников платежных систем.

Банк России определяет точки развития, и затем постепенно начинает адаптировать законодательную базу и внедрять новейшие стандарты кибербезопасности в кредитно-финансовую сферу.

Необходимо подчеркнуть, что проблема банковской уязвимости представляет собой угрозу безопасности не только для банковского сектора и платежной системы, но и для всего государства в целом. Рассмотренные документы и действия Банка России по регулированию и обеспечению безопасности банковской систем и системы платежей должны повысить эффективность борьбы с киберпреступностью, снизить уязвимость кредитно-финансового сектора и его инфраструктуры.

Литература

1. Банк России. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов.

2. Внуков А. А. Защита информации в банковских системах: учеб. пособие для бакалавриата и магистратуры. – М.: Юрайт, 2018.

3. Официальный сайт Центрального банка Российской Федерации – [Электронный ресурс]. – URL: cbr.ru

4. Указание ЦБ РФ от 07.05.2018 №4793-У о внесении изменений в Положение Банка России от 9 июня 2012 года №382-П.

5. Политика ЦБ в сфере защиты информации (кибербезопасности) – [Электронный ресурс]. – URL: tadviser.ru/index.php/

6. Банк России. Департамент информационной безопасности – [Электронный ресурс]. – URL: cbr.ru/about_br/bankstructute/dib/

7. Положение ЦБ РФ от 17 апреля 2019 г. № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»

8. Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. - Москва: ИНИОН РАН, 2020. - № 1. - С. 77-96.

9. Кибербезопасность финансовой сферы: отчет Банка России – [Электронный ресурс]. – URL: cbr.ru/Press/event/?id=3928

10. Положение Банка России от 9 января 2019 г. № 672-П «О требованиях к защите информации в платежной системе Банка России регламентирует обеспечение информационной безопасности при переводах денежных средств в рамках платежной системы Банка России».

11. Банки и финтех-компании: взаимодействие и конкуренция: монография. - /Под ред. Л.С.Александровой – Москва: РУСАЙНС, 2020.

Literature

1. The Bank of Russia. The main directions of development of information security of the credit and financial sphere for the period 2019-2021.

2. Vnukov A. A. information Protection in banking systems: textbook. Handbook for undergraduate and graduate studies. - Moscow: Yurayt, 2018.

3. Official website of the Central Bank of the Russian Federation- [Electronic resource]. – URL: cbr.ru

4. Instruction of the Central Bank of the Russian Federation of 07.05.2018 No. 4793-U on amendments to the Regulation of the Bank of Russia of June 9, 2012 No. 382-P.

5. Central Bank Policy in the field of information security (cybersecurity) - [Electronic resource]. - URL: tadviser.ru/index.php/

6. The Bank of Russia. Department of information security - [Electronic resource]. - URL: cbr.ru/about_br/bankstructute/dib/

7. Regulation of the Central Bank of the Russian Federation No. 684-P of April 17, 2019 "On establishing mandatory requirements for non-credit financial organizations to ensure information protection when performing activities in the financial markets in order to counteract illegal financial transactions»

8. Semeko G. V. Information security in the financial sector: cybercrime and counteraction strategy // Social innovations and social Sciences. - Moscow: INION RAN, 2020, No. 1. P. 77-96.

9. Cybersecurity of the financial sphere: report of the Bank of Russia- [Electronic resource]. – URL: cbr.ru/Press/event/?id=3928

10. Regulation of the Bank of Russia No. 672-P of January 9, 2019 “On requirements for information protection in the Bank of Russia payment system regulates information security when transferring funds within the Bank of Russia payment system”.

11. Banks and fintech companies: interaction and competition: monograph. - / Ed. L.S. Aleksandrova - Moscow: RUSAYNS, 2020.