4 [2024]
ISBN 978-5-901722-87-9
ТРАНСПОРТ. ГОРИЗОНТЫ РАЗВИТИЯ

УДК 336

КИБЕРБЕЗОПАСНОСТЬ В БАНКОВСКОЙ СФЕРЕ: СОВРЕМЕННЫЕ СТРАТЕГИИ ЗАЩИТЫ И РЕШЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ

Пумбрасова Наталья Владимировна[1], начальник планово-экономического отдела, кандидат экономических наук, доцент
e-mail: target75@mail.ru
Шмонова Елена Андреевна[1], магистрант
e-mail: hshmonova@mail.ru

[1] Волжский государственный университет водного транспорта, Нижний Новгород, Россия

Аннотация. В статье представлены вопросы обеспечения кибербезопасности в банковской сфере. Определены основные термины и понятия, рассмотрены стратегии, используемые ЦБ РФ и отдельными коммерческими банками. В рамках данной статьи также представлена критическая оценка эффективности мер, используемых современными коммерческими банками, в целях обеспечения кибербезопасности. Предложены рекомендации по решению проблемы обеспечения безопасности данных.

Ключевые слова: Киберпреступления, кибербезопасность, банковская сфера, цифровые технологии, риски, финансовая грамотность.

CYBERSECURITY IN BANKING: MODERN PROTECTION STRATEGIES AND SOLUTIONS FOR ENSURING DATA SECURITY

Pumbrasova Natalya Vladimirovna[1], Head of the Planning and Economic Department, Candidate of Economic Sciences, Associate Professor
e-mail: target75@mail.ru
Shmonova Elena Andreevna[1], Master's Degree Student
e-mail: hshmonova@mail.ru

[1] Volga State University of Water Transport, Nizhny Novgorod, Russia

Abstract. The article presents the issues of cybersecurity in the banking sector. The main terms and concepts are defined, the strategies used by the Central Bank of the Russian Federation and individual commercial banks are considered. This article also provides a critical assessment of the effectiveness of measures used by modern commercial banks to ensure cybersecurity. Recommendations for solving the problem of data security are proposed.

Keywords: Cybercrime, cybersecurity, banking, digital technologies, risks, financial literacy.

Вопросам исследования кибербезопасности в настоящий момент уделяется существенное внимание. Актуальность научного исследования обусловлена стремительным увеличением числа киберпреступлений. Так, в 2023 году по данным официальной статистики число преступлений в сфере компьютерной информации возросло на 30%. Согласно отчету МВД, в России за первое полугодие 2023 года, выявлено 261 тысяча киберпреступлений, что на 27,5 процента больше, чем за такой же период прошлого года. Во второй половине 2023 года число киберпреступлений в финансовой среде увеличилось практически в два раза. Последствием таких преступлений являются не только финансовые потери, но и остановка функционирования ключевых финансовых систем, нарушение последовательности их работы. Киберпреступления в банковской сфере ведут к нарушению безопасности. Характер таких преступлений связан с использованием компьютерных и информационных технологий в корыстных целях. Несовершенство правовой базы, отсутствие должного уровня правовой культуры граждан, нестабильность политической и экономической среды, активное развитие цифровых технологий – все эти факторы способствуют совершению киберпреступлений в банковской сфере. Потери банков от киберпреступлений колоссальны, что также доказывает актуальность выбранного исследования.

На сегодняшний день назревает очевидная необходимость совершенствования организационно-правового механизма обеспечения кибербезопасности в банковской сфере.

Целью научного исследования является изучение основных особенностей обеспечения кибербезопасности в банковской среде и предложение рекомендаций по совершенствованию.

Для исследования особенностей обеспечения кибербезопасности в банковской сфере необходимо изучить перечень основных терминов и понятий. Киберпреступность представляет собой преступную деятельность, осуществляемая с использованием компьютерных сетей и цифровых устройств. Она включает в себя различные виды преступлений, такие как мошенничество, кража личных данных, утечка данных, компьютерные вирусы и другие злонамеренные действия. Киберпреступники используют уязвимости в компьютерных системах для получения несанкционированного доступа к информации, кражи конфиденциальных данных и нанесения финансового или репутационного ущерба.

Термин «кибербезопасность» является новым термином и в настоящий момент нет официального определения данного понятия. В проекте Концепции национальной стратегии кибербезопасности Российской Федерации под кибербезопасностью понимается «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями» [1].

Кибербезопасность – это сфера деятельности, которая занимается защитой компьютерных систем, сетей, программ и данных от киберугроз, таких как хакерские атаки, вирусы и вредоносное программное обеспечение. Управление кибербезопасностью направлено на обеспечение конфиденциальности, целостности и доступности информации. Концепция управления кибербезопасностью ориентирована на минимизацию финансовых рисков и угроз, на предотвращение потерь от совершаемых киберпреступлений, на повышение правовой культуры граждан и их финансовой грамотности, на обеспечение эффективного функционирования банковского сектора в частности и финансовой сферы в целом.

Среди ключевых киберрисков можно отметить хищение средств клиентов финансовых организаций, финансовые потери самих участников рынка, нарушение надежности и

непрерывности предоставления финансовых услуг, развитие системного кризиса из-за кибератак, поразивших крупнейшие организации.

Стремительное развитие цифровых и информационных технологий создает благоприятную среду для совершения киберпреступлений, нарушения при этом уровень безопасности. Киберпреступники постоянно ищут новые способы взлома данных банковских систем и онлайн-сервисов. Это приводит к утечке конфиденциальной информации о клиентах, что может привести к финансовым потерям и нарушению доверия к банку. Значительное число киберпреступлений в банковской сфере совершается через мобильные приложения. Использование банковских приложений с мобильных устройств делает банки уязвимыми для атак через смартфоны и планшеты. Отсутствие надёжного защитного программного обеспечения может привести к краже данных и несанкционированному доступу к банковским счетам.

На сегодняшний день требуется комплексный подход к решению проблемы. Необходимо предпринимать действия по обеспечению кибербезопасности как на уровне страны в целом, так и на уровне отдельных банков.

Центральный банк России регулярно оценивает объем финансовых потерь клиентов коммерческих банков. Так по данным 2023 года объем финансовых потерь составил 4,5 млрд. рублей. Одной из тенденций является стремительное увеличение объемов похищенных мошенниками средств с банковских счетов. Темп роста в 2023 году по сравнению с 2022 годом составил порядка 30%. Объем потерь банков же по данным 2022 года незначителен, как определяет ЦБ РФ. Однако если оценивать данный вопрос с позиции уровня надежности, то можно утверждать, что увеличение мошеннических операций негативно отражается на деловой репутации банка, на степени его надежности и конкурентоспособности, что напрямую оказывает влияние на результаты финансово-хозяйственной деятельности коммерческого банк [3].

Для обеспечения кибербезопасности в банковской сфере ЦБ РФ предпринимает различного рода меры. В 2023 году Банк России одобрил Основные направления развития информационной безопасности кредитно-финансовой сферы на ближайшие три года. Их цели и задачи сформулированы по результатам обсуждения с участниками рынка. Документ также учитывает результаты, достигнутые при реализации Основных направлений на 2019 – 2021 годы, актуальные вызовы в сфере информационной безопасности и предусматривает:

– защиту прав потребителей финансовых услуг и повышение уровня доверия к цифровым технологиям;

– создание условий для безопасного внедрения цифровых и платежных технологий и обеспечения технологического суверенитета;

– обеспечение контроля рисков информационной безопасности, операционной надежности для непрерывности оказания банковских и финансовых услуг.

Остановимся также на вопросах обеспечения кибербезопасности в рамках отдельных банков. Один из крупнейших банков нашей страны ПАО «Сбербанк» осуществляет целый ряд мер, направленных на предотвращение кибератак в адрес своих клиентов. В ПАО «Сбербанк» выделено специальное подразделение Департамент безопасности х4ъ.

Процедура управления кибербезопасностью в ПАО «Сбербанк» предусматривает формирование локальных нормативно-правовых актов, ориентированных на предупреждение возникновения киберпреступлений. Банковские структурные подразделения определяют риск возникновения кибератак, предупреждая об этом клиентов и блокируя определенного рода действия, например, с картами или платежами. Стоит обратить внимание, что значительная роль уделяется вопросам идентификации рисков. Для мониторинга и контроля состояния кибербезопасности ПАО «Сбербанк» разработал

методические инструменты, такие как профилирование кибербезопасности, оценка текущего уровня зрелости кибербезопасности и план развития кибербезопасности с ключевым показателем эффективности (КПЭ) «Индекс кибербезопасности». Индекс кибербезопасности стимулирует руководителей дочерних обществ к регулярному контролю состояния кибербезопасности, выделению необходимых ресурсов и является одним из важнейших инструментов повышения качества менеджмента кибербезопасности компаний экосистемы ПА «Сбербанк». Банк также активно использует совокупность технических средств для осуществления регулярного мониторинга. Результаты мониторинга служат основанием для предупреждения клиентов банка о возможных рисках. Достоинством методики, используемой ПАО «Сбербанк» является не только применение индекса кибербезопасности, но профилирование кибербезопасности. Банк формирует более точные требования и рекомендации по кибербезопасности для каждой компании с учётом специфики бизнеса и регуляторных требований.

ПАО «Сбербанк» также делит атаки на технические, информационные и относящиеся к социальной инженерии. Одной из тенденций на сегодняшний день является увеличение кибератак, относящихся к социальной инженерии и направленных на обычных пользователей банковских услуг. Соответственно, программа обеспечения кибербезопасности должна учитывать данный фактор и обеспечить повышение финансовой грамотности «простого обывателя». Таким образом, управление кибербезопасностью в ПАО «Сбербанк» основано на использовании современных методических инструментов, активном взаимодействии с организациями экосистемы и постоянном контроле состояния кибербезопасности для обеспечения непрерывности бизнес-процессов и защиты интересов всех участников экосистемы [3].

Другие крупнейшие банки страны также уделяются существенное внимание практическим вопросам обеспечения кибербезопасности. Так система управления кибербезопасностью в ПАО «ВТБ» постоянно совершенствуется и адаптируется к изменяющимся угрозам и требованиям законодательства. Это позволяет банку обеспечивать надёжную защиту своих информационных активов и поддерживать высокий уровень доверия со стороны клиентов и партнёров. Банк также осуществляет регулярный мониторинг и идентификацию группы киберрисков, предупреждает своих постоянных клиентов о риске кибератак. В 2021 году банк внедрил систему обнаружения и предотвращения кибератак, которая помогает выявлять и блокировать угрозы в режиме реального времени. Эта система использует машинное обучение и анализ поведения пользователей для обнаружения аномалий и подозрительной активности. В 2022 году банк разметил на сайте информацию о рисках кибератак.

Достоинством политики ПАО ВТБ является тот факт, что банк осуществляет политику, направленную на повышение финансовой грамотности населения. Это является достаточно значимой проблемой на сегодняшний день. Низкий уровень финансовой грамотности способствует формированию благоприятной среды для совершения киберпреступлений, многие граждане не уделяют должного внимания вопросам личной безопасности, лично оставляют данные карт, формирует малонадежные пароли для входа в личные кабинеты. В перспективе важнейшей мерой должно стать проведение банками непосредственной работы с физическими и юридическими лицами в целях формирования эффективного организационного механизма обеспечения кибербезопасности [5].

Для обеспечения должного уровня кибербезопасности практически все крупнейшие банки нашей страны осуществляют регулярное обновление операционной системы, адаптируя ее к современным реалиям, применяют резервное копирование, ограничивают доступ к отдельным интернет-магазинам и сайтам, что также служит мерой предотвращения совершения неправомерных действий со стороны мошенников.

В настоящий момент в банковской сфере требуется совершенствование организационного механизма, ориентированного на предупреждение кибератак. Требует совершенствования и сама база правовой регламентации информационной безопасности в банковской сфере. Необходимо утвердить единый комплекс мер по предотвращению киберпреступлений в банковской сфере. Также стоит отметить, что обеспечение должного уровня кибербезопасности сталкивается с определенным родом проблем. Во-первых, стремительное появление новых схем мошенничество. Одновременно с развитием информационных технологий, адаптируются и мошенники к порядку совершения киберпреступлений. Во-вторых, отсутствие географических границ затрудняет порядок внедрения мер по предупреждению киберпреступлений. Мошенники могут действовать из любой точки мира. Обозначенные проблемы свидетельствуют о необходимости внедрения мер международного сотрудничества в части обеспечения кибербезопасности в банковской сфере.

В качестве рекомендации по повышению кибербезопасности в банковской сфере также можно рекомендовать использование информационных и автоматизированных систем. DLP-системы (Data Leak Prevention) помогают банкам контролировать и защищать конфиденциальную информацию, такую как номера счетов, пароли и данные о транзакциях. DLP-системы анализируют потоки данных и предупреждают о возможных угрозах, таких как утечка информации или несанкционированный доступ. SIEM-системы (Security Information and Event Management) позволяют банкам обрабатывать и анализировать большие объёмы информации о событиях безопасности. SIEM-системы помогают обнаруживать аномалии, угрозы и подозрительную активность, что позволяет оперативно реагировать на возникающие проблемы.

Ключевые инициативы в области обеспечения кибербезопасности в банковской сфере представлены на рисунке 1.

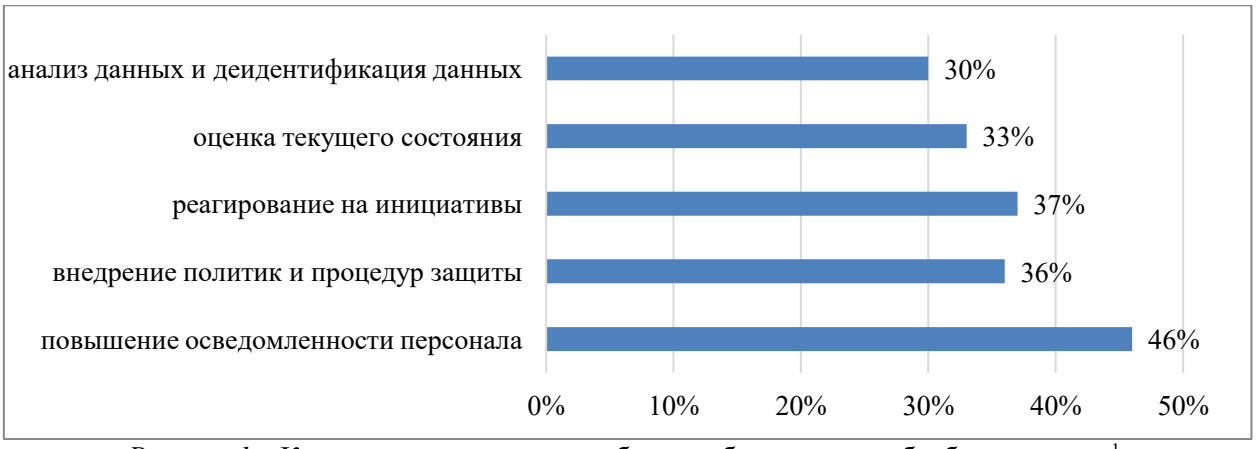

Рисунок 1 – Ключевые инициативы в области обеспечения кибербезопасности[1]

Для повышения уровня кибербезопасности целесообразно на уровне отдельных коммерческих банков совершенствовать нормативно-правовые акты, проводить регулярную оценку текущего состояния рисков, совершенствовать механизму защиты, обучать и мотивировать персонал в целях предотвращения кибератак. Сотрудники должны знать основы информационной безопасности, уметь распознавать угрозы и правильно реагировать на них. Мотивация персонала также играет важную роль, так как сотрудники должны быть заинтересованы в соблюдении правил безопасности и защите информации. Внедрение фрод-модулей в систему «Клиент-Банк» поможет банкам выявлять и

[1] Составлено авторами на материалах [5].

предотвращать несанкционированные транзакции. Фрод-модули анализируют данные о транзакциях и выявляют аномалии, которые могут указывать на мошенничество [2, с. 16].

В заключении можно сделать вывод о том, что стремительное развитие информационных и цифровых технологий создало благоприятную среду для совершения киберпреступлений. Обеспечение кибербезопасности в банковской сфере требует разработки комплексного решения по минимизации киберрисков. Необходимо совершенствовать как правовую основу, так и организационный механизм.

Список литературы:

1. Проект Концепции национальной стратегии кибербезопасности Российской Федерации. – URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения 14.04.2024)

2. Шкодинский С.В. Цифровая трансформация банковских бизнес-моделей и проблемы обеспечения кибербезопасности / С.В. Шкондинский // Вестник евразийской науки. – 2023 – №3. – с. 15 – 19.

3. Официальный сайт Банка России: информационная безопасность. – URL: https://cbr.ru/information_security/ (дата обращения 16.04.2024)

4. Официальный сайт ПАО «Сбербанк. – URL: www.sberbank.ru (дата обращения 16.04.2024)

5. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года. – URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения 16.04.2024)