УДК 338.2 DOI: 10.14451/1.239.261

Идентификация и классификация угроз и рисков экономической безопасности Сбербанка

© 2024 **Каширская Людмила Васильевна**
Доктор экономических, профессор кафедры аудита и корпоративной отчетности Факультета налогов, аудита и бизнес-анализа. Финансовый университет при Правительстве РФ, Москва, Россия.
E-mail: kashirskaya76@mail.ru

© 2024 **Резепова Виктория Викторовна**
Руководитель отдела продаж. Сбербанк, Москва, Россия.
E-mail: v_nebolsina@mail.ru

Ключевые слова: аудит, риски, угрозы, экономическая безопасность, совершенствование аудита, мошенничество, санкции, кибербезопасность.

Статья посвящена актуальной проблеме идентификации и классификации угроз и рисков, влияющих на экономическую безопасность крупнейшего российского банка — ПАО «Сбербанк». В фокусе исследования находятся ключевые факторы, которые могут негативно повлиять на финансовую стабильность банка в условиях изменения геополитической ситуации, санкционного давления и активизации киберпреступности.

В настоящее время в связи с изменением геополитической ситуации в мире и большого санкционного воздействия на Россию, актуальным ресурсом влияния на финансовый сектор российской экономики является кибермошенничество, от которого имеют ущерб как простые граждане, так и крупные банки. В связи с этим, на первый план выходит моделирование киберрисков для исключения финансовых потерь и дестабилизации в банковском секторе экономики. С этой целью для основы анализа рассмотрим состояние угроз экономической безопасности в ПАО «Сбербанк» (Сбербанк).

Экономическая безопасность банка — это сложная система, зависящая от множества внутренних и внешних факторов, которые могут представлять угрозу для его нормальной работы.

И. М. Подколзина в своей книге «Современные угрозы экономической безопасности банковской деятельности» подчеркивает, что для предотвращения финансовых потерь банка и его клиентов, необходимо своевременно предупреждать, устранять или делать невозможными эти угрозы [3].

В. А. Гамза в своих исследованиях добавляет, что для обеспечения безопасности банка нужна сбалансированная система мер, защищающая

его финансовые ресурсы, информацию и имущество от различных угроз [1].

Особое внимание следует уделить информационной безопасности, чтобы исключить финансовые потери банка и его клиентов.

Центральный Банк Российской Федерации контролирует и регулирует систему экономической безопасности коммерческих банков в России.

Классификация экономических преступлений в отношении банков

1. Преступления против компьютерных данных и систем.
2. Преступления, связанные с использованием технологий.
3. Правонарушения, связанные с содержанием данных или контентом.
4. Нарушение авторских и смежных прав.
5. Деяния, посягающие на общественную безопасность.

Ключевыми показателями экономической безопасности коммерческого банка являются финансовые риски (риск невозврата кредитов, нестабильность финансовых рынков); ущерб репутации и позициям на рынке (потеря доверия клиентов, негативное влияние на имидж банка, снижение конкурентоспособности); кадровые риски (некомпетентность сотрудников, утечка конфиденциальной информации, неэффективное управление персоналом); технико-информационные риски (хакерские атаки, сбои в работе IT-систем); правовые (юридические) риски (несоблюдение законодательства, неправильное толкование договоров, неэффективное управление правовыми рисками); организационные риски (неэффективная структура управления, недостаточное взаимодействие отделов) [4].

В условиях геополитической нестабильности в мире кибербезопасность становится одной из самых важных проблем для любого банка, представляя собой особую форму технико-информационного риска.

Мошенники используют все доступные информационные каналы, чтобы похитить деньги и персональные данные. Сбербанк как один из крупнейших российских банков со значительной долей финансовых активов является привлекательной целью для киберпреступников особенно в условиях ухудшения геополитической обстановки.

В таблице 1 приведем краткую историческую справку о нарушениях в сфере кибербезопасности в Сбербанке.

Таблица 1. Историческая справка о нарушениях кибербезопасности в Сбербанке.

Период	Характеристика
2024	– крупнейшая кибератака на Сбербанк, которая длилась 13 часов; – Сбербанк применяет искусственный интеллект более чем из 100 моделей для обеспечения безопасности своих активов и активов клиентов.
2023	– ликвидация более чем 120 DDoS-атак, 300 млрд руб. не удалось вывести злоумышленникам; – мощная DDoS-атака, преступники отправляли 1 млн запросов в секунду; – объемная фишинговая атака на банк в процессе функционирования.
2022	– 1,4 млрд руб. спасено от кибермошенничества; – DDoS-атака с участием более 100 тыс. хакеров, более 450 гигабайт в секунду оценивалась ее мощность; – кибератаки фиксируются в основном с территорий Европы, Китая, США, Тайланда; – остановлена кибератака с Украины, при помощи которой преступники собирались похитить личные данные и финансовые активы клиентов банка.

Продолжение на следующей странице

Таблица 1. Историческая справка о нарушениях кибербезопасности в Сбербанке. (Продолжение таблицы)

Период	Характеристика
2021	– за кражу 2,4 млн руб. у клиента получил уголовный срок сотрудник банка; – Сбербанк исключил из своей деятельности иностранные программные продукты в процессе фрод-мониторинга.
2020	– преступник, который похитил у клиентов банка более 122 млн руб. задержан и ему предъявлено обвинение; – заблокирован мошеннический колл-центр на территории Мелитополя; – граждан Украины задержали за хищение денежных средств в банкоматах Сбербанка на территории Боснии и Герцеговины; – объемная DDoS-атака за несколько лет истории банка.
2019	– за украденные более чем 10 млн руб. из банкоматов банка осуждены хакеры; – поступило более 2,0 млн жалоб на мошеннические действия со стороны клиентов банка; – сотрудникам Сбербанка запретили фотографирование экранов рабочих компьютеров.
2018	– 90 DDoS-атак за год отразили в банке; – за 2 дня отражено 6 крупных кибератак на Сбербанк, они производились из 6 стран, задействовано более 100 серверов; – спасено от кибермошенников 32 млрд руб. активов клиентов; – аналитики компании «Доктор Веб» зафиксировали, что более 77 млн руб. денежных средств клиентов банка под угрозой.
2017	– Центру управления кибербезопасностью Сбербанка выдали международный сертификат соответствия; – при помощи искусственного интеллекта определены процессы хищения денежных активов из банкоматов.
2016	– отражение более 74 DDoS-атак; – более 8,6 млрд руб. денежных средств клиентов банка сохранены при угрозах кибермошенничества; – образован центр управления киберзащитой; – для усиления кибербезопасности выделено отдельное структурное подразделение в функционале управления банка.
2014	– удалось спасти от кибермошенников более 3,0 млрд руб. денежных активов клиентов банка.
2013	– удалось спасти от скимминговых операций более 5,6 млрд руб. денежных активов клиентов банка.

Источник: Исоставлено автором по архивам Сбербанка.

Сбербанк является одним из крупнейших банков в России с более чем 100 миллионами клиентов и более 82 миллионами пользователей СберБанк Онлайн.

Ежедневно специалисты по кибербезопасности Сбербанка отслеживают более 120 миллиардов событий и фиксируют более 40 тысяч атак на клиентов банка.

Сбербанк активно борется с кибермошенничеством, анализируя схемы мошеннических действий, создавая систему фрод-мониторинга и сотрудничая с правоохранительными органами.

Система фрод-мониторинга проверяет данные о карте, имени плательщика, IP-адресе и другой информации. Если транзакция связана с украденными картами, IP-адресами из черного списка или другими признаками мошенничества, она немедленно блокируется автоматически.

С 2022 года Сбербанк сталкивается с постоянными DDoS-атаками. Киберпреступники перегружают серверы банка мусорным трафиком, блокируя доступ пользователей к онлайн-банкингу и замедляя работу сайтов. Это приводит к значительным финансовым потерям и ущербу репутации банка.

Несмотря на это, Сбербанк успешно отражает атаки благодаря комплексной системе защиты,

которая включает в себя различные средства защиты, взаимодействие с правоохранительными органами и мобильными операторами связи. Глава Сбербанка Герман Греф оценил уровень защиты клиентов от киберугроз на уровне 99,6%. Сбербанк занимается вопросами кибербезопасности с 2010 года.

Сбербанк активно переходит на использование собственных разработок, заменяя зарубежные программные продукты отечественными аналогами. Это позволяет обеспечить более глубокую интеграцию с отечественными ресурсами и законодательством.

Применение передовых технологий, таких как блокчейн и биометрия, обеспечивает высокую защиту данных от несанкционированного доступа. Алгоритмы искусственного интеллекта снижают риск мошенничества, включая атаки социальной инженерии, предотвращая утечки данных, блокируя подозрительные операции и предупреждая пользователей о потенциально опасных звонках.

В 2015 году был создан Центр управления кибербезопасностью Сбербанка, а в 2017 году была открыта Академия кибербезопасности для подготовки специалистов. В центре работает более 1600 сотрудников, которые занимаются расследованием деятельности мошеннических колл-центров. Сбербанк использует более 1 миллиона элементов инфраструктуры и 50 технологий защиты и имеет более 35 патентов на средства киберзащиты.

Сотрудники Сбербанка ежедневно отмечают подозрительное поведение некоторых клиентов, например, попытки снять крупные суммы наличными или закрыть вклад с утратой процентов. Служба безопасности вмешивается, предоставляя клиентам информацию о возможных угрозах и рисках и раскрывая схемы мошенничества.

Для информирования клиентов Сбербанк запустил онлайн-сервис «Кибрарий», который предоставляет информацию о кибербезопасности и защите от мошенничества. Сервис включает в себя разделы с памятками, видеороликами, обучающими материалами, описанием схем обмана, статьями для разных возрастных групп и информацией для экспертов.

Система безопасности Сбербанка была признана «Лучшим решением по информационной безопасности и фрод-менеджменту» по версии международной ассоциации в области финансов.

Сбербанк запустил уникальную для России программу для «белых хакеров», эксперты смогут получить до 500 тыс. руб. за найденные уязвимости в информационной безопасности банка. Исследователям необходимо проверить сайт «Сбера», веб-версию и мобильное приложение СберИнвестиции, а также СберБанк Онлайн. В онлайн-банкинге эксперты могут искать уязвимости приложения в мобильных версиях для iOS и Android, мессенджере онлайн-банка и Сбер ID — сервисе для входа на сайты и приложения Сбера и партнеров [2].

Кроме того, банк организовал за вознаграждение находить различные виды уязвимости, которые приводят к несанкционированному доступу в данные клиентов, к нарушению функциональности различных систем и сервисов, а также за устранение уязвимости.

Сбербанк перестал быть просто финансовой организацией и превратился в технологическую компанию, предлагающую клиентам широкий спектр банковских и небанковских электронных сервисов.

В этих условиях обеспечение экономической и информационной безопасности становится ключевым фактором для успеха банковской отрасли. Управление технологическими рисками позволит снизить угрозу кибермошенничества и минимизировать финансовые потери.

Для успешного функционирования Сбербанку необходимо организовать систему управления рисками в области экономической безопасности, учитывая как внутренние факторы, так и внешние угрозы, особенно в области кибербезопасности, которая с каждым годом становится все более реальной и опасной.

Библиографический список

1. *Гамза В. А.* Безопасность банковской деятельности : учебник для вузов. — М. : Юрайт, 2024. — 460 с.
2. Официальный сайт ПАО «Сбербанк». — URL: http://www.sberbank.ru/ru/about/today.
3. *Подколзина И. М.* Современные угрозы экономической безопасности банковской деятельности // Экономика, управление и право в условиях риска и неопределенности. – Пенза: Наука и просвещение. — 2019. — С. 47—55.
4. *Сторожук И. Н.* Механизм защиты экономической безопасности коммерческих банков // Пространство экономики. — 2019. — Т. 7, № 3—3. — С. 140—143.