Цивилизационные перемены в России. 2023. С. 276–281.
Civilizational changes in Russia. 2023. P. 276–281.

Научная статья
УДК 004.056

DECEPTION – РЕШЕНИЯ КИБЕРБЕЗОПАСНОСТИ БАНКОВ

Гилян Васильевна Федотова
Федеральный исследовательский центр «Информатика и управление»
Российской Академии Наук, Москва, Россия
g_evgeeva@mail.ru

Аннотация. Популярность интернет-банкинга провоцирует рост кибератак на ценные электронные активы клиентов банков. Банки постоянно ведут работу по поиску и совершенствованию существующих решений по защите. В статье проведен обзор наиболее востребованных электронных платежных сервисов и проанализирована динамика операций без согласий клиентов банков. В статистике отражен низкий процент возврата похищенных средств, поэтому необходимо усилить защиту от взлома и кибератаки. Представлены новые решения для повышения безопасности электронных банковских сервисов.

Ключевые слова: кибербезопасность, система защиты, банк, кибератаки, мошенничество

Для цитирования: Федотова Г. В. *Deception* – решения кибербезопасности банков // Цивилизационные перемены в России. 2023. С. 276–281.

Scientific article

DECEPTION – BANKS CYBER SECURITY SOLUTIONS

Gilyan V. Fedotova
FRC «Computer Science and Control» RAS,
Moscow, Russia
g_evgeeva@mail.ru

Abstract. The popularity of Internet banking provokes an increase in cyber-attacks on valuable electronic assets of bank customers. Banks are constantly working to find and improve existing security solutions. The article provides an overview of the most popular electronic payment services and analyzes the dynamics of transactions without the consent of bank customers. The statistics of the return of stolen funds proves a low percentage of returns,

so efforts are needed at the stage of hacking and implementing a cyber-attack. New solutions for improving the security of electronic banking services are presented.

Keywords: cyber security, protection system, bank, cyber-attacks, fraud

For citation: Fedotova G. V. *Deception* – banks cyber security solutions // Civilizational changes in Russia. 2023. P. 276–281.

В настоящее время интернет-банкинг достаточно повседневная услуга, которая набирает все большее количество пользователей. Огромные возможности для экономии времени и издержек для кредитных учреждений будут способствовать расширению и дальнейшему усложнению услуг, оказываемых посредством интернета. Повсеместно доказано, что финансовый сектор выступает лидером и катализатором последующей глобализации и цифровизации всей социально-экономической системы. Развивая онлайн-сервис финансовых услуг, государство способствует росту финансовой и информационной грамотности населения. Ежедневное или периодическое использование интернета в осуществлении текущих платежей повышает доверие граждан к системам дистанционного доступа к своим счетам. С каждым годом все большее количество граждан прибегает к услугам дистанционного банковского обслуживания.

На рис. 1 представлены результаты опроса клиентов агентством *Markswebb Rank&Report* по использованию дистанционного банковского обслуживания (ДБО).

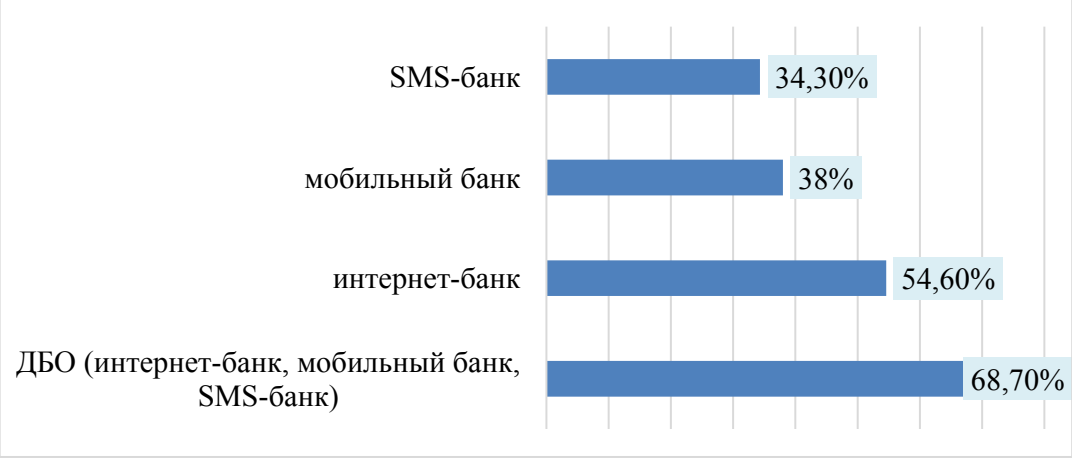

Рис. 1. Использование электронных платежных и финансовых сервисов в 2022 г. [1]

Безусловно ДБО все больше входит в повседневную жизнь людей благодаря простоте использования, удобству, круглосуточному доступу к счетам.

Сегодня современный коммерческий банк – это больше виртуальный банк, который обслуживается через интернет, что дает возможность

построить финансовую систему информационной экономики. Кредитные организации постоянно расширяют свои возможности в онлайн пространстве: предлагают новые сервисы и оформление документов без посещения офиса, проводят огромные объемы электронных платежей и транзакций ежедневно. Поэтому вопросы обеспечения максимальной безопасности операций и сохранности информации, счетов клиентов представляют собой задачу первостепенной важности в системах безопасности кредитных организаций.

С ростом количества кредитных организаций, использующих системы интернет-банкинга как наиболее эффективного канала продаж, будет расти количество кибератак на данные системы. Поэтому банки постоянно ищут новые механизмы и инструменты для защиты своих сайтов и счетов клиентов. Но никакая система не может на 100 % гарантировать безопасность счетов, она может только максимально снизить уровень угрозы. В 2022 г. проблема кибербезопасности цифровых активов стала наиболее острой по причине возросших кибератак на российские сервисы и сайты.

На рис. 2 представлены обнародованные данные Банка России по совершенным операциям со счетов клиентов без их согласия по итогам 3 квартала 2021 и 2022 гг.

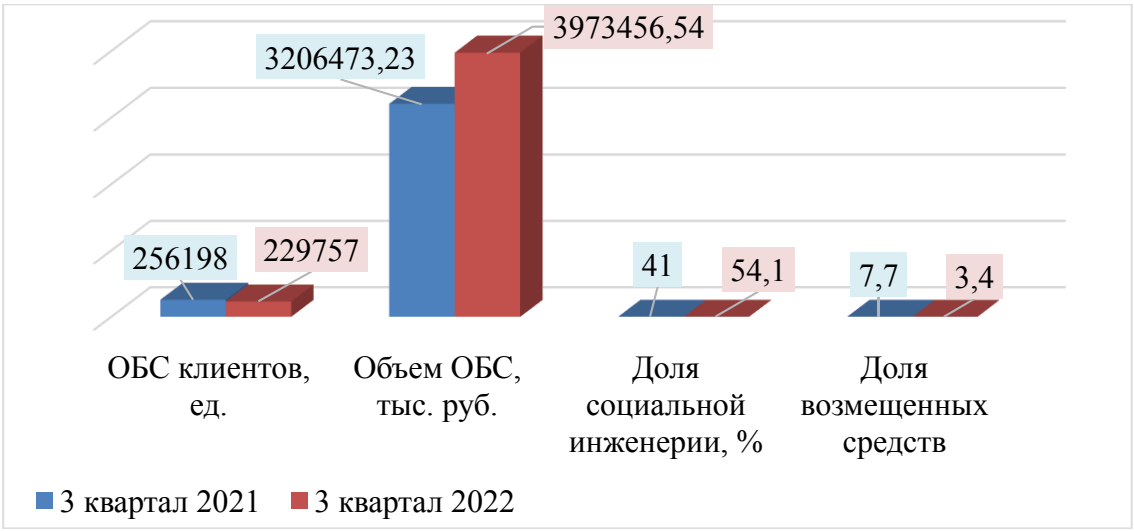

Рис. 2. Объемы операций без согласий клиентов (ОБС) за 3 квартал 2021–2022 гг. [2]

В 2022 г. в 3 квартале сумма краж со счетов клиентов банков выросла на 19,3 % по сравнению с 3 кварталом 2021 г., также выросла доля социальной инженерии – на 12,9 %. К сожалению, фактически невозможно эти средства возместить, т. к. они уходит в теневой сектор интернета и бесследно исчезают. Поэтому необходимо усиливать систему информационной защиты и мгновенно пресекать любые попытки несанкционированного входа в сервисы.

Особенностью киберпреступности в банковской сфере выступают большие объемы нанесенного ущерба в информационном пространстве. Инструментами преступников в онлайн-среде являются различные вирусы и противозаконные программы, с помощью которых мошенники получают доступы к счетам клиентов платежных систем. Основная масса вирусов направлена на кражу средств со счетов клиентов. В данной ситуации более подвержена этому система *Android*, а максимально безопасной системой является IOS. Главная угроза для всех устройств мобильной связи – банковские трояны [3].

Кредитные организации для противодействия кибермошенничеству сочетают разные комплексы правовых, технических, организационных и информационных мероприятий. Основная масса антивирусных программ сканируют привязку карт клиентов и блокируют вредоносные ПО. Так задуманы программы, но на практике все немного по-другому. Сегодня очень много видов вирусных программ, которые к тому же сами себя защищают, поэтому их очень сложно обойти. Более того, некоторые программы успешно маскируются под настоящие и способны проверить баланс счета, перевести деньги на другой счет. Идентифицировать такие программы очень сложно, жертвы мошенников узнают о несанкционированных операциях только по факту их совершения.

Специалисты по борьбе с киберпреступностью отмечают, что к тому же сами клиенты допускают ошибки из-за невнимательности и неосторожности. Владельцы должны более тщательно хранить свои учетные записи и доступы к своим счетам. Для профилактики подобных ошибок можно периодически менять пароли, входить в онлайн кабинеты только со своих компьютеров, не посещать непроверенные и сомнительные сайты.

При рассмотрении экономической безопасности кредитной организации ясно, что банки тщательно прорабатывают сценарии различных рисков и реализуют программы по управлению этими рисками. Пожалуй, единственной значимой угрозой экономической безопасности коммерческого банка является мошенничество в сфере дистанционного банковского обслуживания. В данном случае в процессе оказания удаленной услуги помимо информационно-технических ресурсов банка задействованы и ресурсы клиента: смартфоны, компьютеры и планшеты. Банк не в состоянии полностью контролировать безопасность данных устройств. Появляется необходимость в разработке и внедрению некоторых мероприятий, направленных на сохранение надежности совершаемых клиентом денежных операций.

В большинстве случаев кибермошенничество, связанное с попытками списания денег со счетов банковских клиентов через системы интернет-банкинга, были реализованы вследствие воздействия вредоносного кода на используемое клиентом мобильное или стационарное устройство.

Повышение безопасности систем интернет-банкинга будет выступать основной задачей информационной безопасности для современной кредитной организации. Рост угроз и их усложнение приводит к совершенствованию систем и процессов интернет-банкинга.

Биометрические методы и экспертные модули дают возможность автоматизировать и формализовать многочисленные движения фоноскопического идентификационного проведения исследования: отбор схожих слов и звучаний, подбор сопоставляемых голосовых и мелодических отрывков, сопоставление дикторов согласно формантам и центральному тону, аддитивные и лингвистические виды анализа. Эффекты в области каждого метода изучения воображаются в варианте числовых характеристик единого идентификационного постановления.

В идеальном варианте обезопасить систему интернет банкинга можно только при сочетании различных способов одновременно, например когнитивный отпечаток. Специфика такого способа защиты – сочетание сканирования радужки глаза, клавиатурного почерка и даже привычек веб-серфинга для непрерывной аутентификации пользователя.

Для сокращения инцидентов мошенничества, связанных с использованием интернет-технологий и несанкционированными платежами, предлагается вести постоянный контроль, а именно анализ потока клиентских платежей за определенный период времени. Если клиент совершает два или более платежа в адрес одного и того же контрагента – нет оснований полагать, что очередной платеж в адрес данного контрагента будет мошенническим. В случае если платеж совершается в адрес нового получателя, необходимо получить от клиента дополнительное подтверждение о том, что платеж не является противоправным.

В последнее время распространено решение *Deception*, которое относится к решениям класса *Intrusion Detection System* (IDS) – системам обнаружения вторжений. Основная цель такой системы – выявить попытки нежелательного доступа к сети. Иными словами, *Deception* помогает обнаруживать сетевые атаки. Она представляет собой централизованные системы управления ложными сетевыми объектами, которые принято называть ловушками (*decoys*), которые ведут злоумышленников по ложному следу и отвлекают на ложные серверы и файлы (рис. 3).

В завершение отметим, что существующие механизмы защиты, как правило, внедряются только по итогам свершившихся кибератак. Такой принцип работы не всегда является эффективным и не обеспечивает предупреждения несанкционированного доступа к системам интернет – банкинга. Существующие технологии защиты систем разрабатываются и адаптируются под конкретные типы кибермошенничества, что фактически доказывает их отставание от технологий преступников [5].

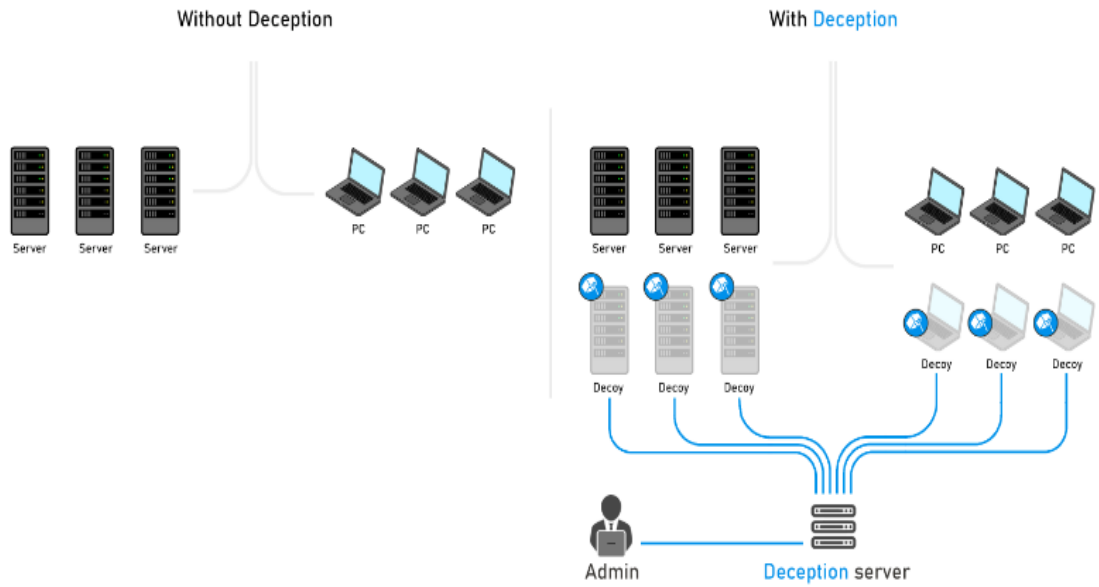

Рис. 3. Архитектура сетевого решения *Deception*

Поэтому основное направление повышения экономической безопасности систем интернет-банкинга будет заключаться в формировании превентивных механизмов защиты счетов клиентов, которые позволяют опережать будущие действия киберпреступников.

Список источников

1. Югай Е. В., Федотова Г. В. Интернет-банкинг как современный механизм банковского обслуживания // Экономическая безопасность: правовые, экономические, экологические аспекты : сборник научных трудов международной научно-практической конференции, Курск. 2017. С. 285–290.

2. Инциденты, направленные на клиентов финансовых организаций и финансовые организации (ед.), динамика (квартал к кварталу, %). URL: https://cbr.ru/analytics/ib/review_3q_2022/ (дата обращения: 14.01.2023).

3. Исследование пользователей электронных финансовых и платежных сервисов в России. URL: https://www.shopolog.ru/news/issledovanie-polzovateley-elektronnykh-finansovykh-i-platezhnykh-servisov-v-rossii/ (дата обращения: 14.01.2023).

4. Орлова Е. Р. Особенности оценки эффективности инвестиционных программ // Экономика строительства. 2006. № 1. С. 25–33.

5. Федотова Г. В., Орлова Е. Р., Бочарова И. Е. Вопросы кибербезопасности цифровых финансовых сервисов // Информационные технологии и вычислительные системы. 2022. № 2. С. 37–45.