Секция «Большие данные и искусственный интеллект в государственном и корпоративном управлении»

Цифровой банкинг: возможности и уязвимости

Научный руководитель – Истратов Василий Николаевич

Афанасьева Мария Александровна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Факультет государственного управления, Кафедра международных организаций и проблем глобального управления, Москва, Россия
E-mail: mafanaseva757@gmail.com

Вступление в цифровую эпоху и внедрение передовых технологических достижений обусловило появление в секторе банковского обслуживания нового дистанционного способа взаимодействия с клиентом, интернет-банкинг. Следовательно, наиболее актуальным вопросом совершенствования предоставления банковских услуг является организация комплексного банковского обслуживания потребителей с использованием инновационных телекоммуникационных технологий. По данным исследования Digital Bank Report, цифровой банкинг признается главным стратегическим приоритетом развития банкового обслуживания около 71% финансовых организаций в мире [2]. Можно сказать, что цифровой банкинг является новым способом реализации банковских процессов, суть которого состоит в проведении транзакции и предоставлении услуг через цифровые каналы взаимодействия с помощью электронных сетей и искусственного интеллекта. К основным преимуществам цифрового банкинга для самих банковских организаций относится дифференцированный характер работы с клиентами, определяемый их индивидуальными предпочтениями. Благодаря использованию автоматизированных информационных систем и цифровых каналов взаимодействия с клиентурой банки значительно повышают качество предоставляемых услуг, что в свою очередь наряду со способностью к внедрению инноваций является определяющими факторами успеха банковской деятельности в конкурентной среде. Кроме этого, происходит оптимальное выполнение банковских операций, расширение доли на рынке услуг и сокращение операционных расходов. Так, если традиционно расширение круга обсуживаемой клиентуры происходило путем увеличения сети физических отделений. Теперь подобный механизм признается экономически неоправданным, поскольку требует больших инвестиций на эксплуатацию помещения и на фонд оплаты труда. Успех данного направления также определяется оптимизацией интернет-сервисов банковских организаций под мобильные устройства, которыми владеют практически все жители планеты. Анализ практики дистанционного цифрового обслуживания позволил выделить ряд основных тенденций развития в данной области: переход на электронную обработку данных и электронные платежи, автоматизация биллинговых процедур, использование цифровых сертификатов и электронно-цифровых подписей, разработка банками собственных систем web-закупок. Интенсификация перехода к дистанционному банковскому обслуживанию связана с существенным удешевлением предоставляемых банковских услуг, совершаемых при помощи цифровых каналов взаимодействия. Вместе с инкорпорированием новых цифровых технологий в банковскую деятельность получают развитие новые методы систематического анализа больших объемов клиентских данных. Следствием последнего является создание персонифицированных схем банковского обслуживания, в том числе за счет расширение возможностей доступа к наиболее финансово обеспеченным индивидуальным клиентам. На современном этапе для российского банковского сектора основной задачей является формирование целостной национальной концепции цифрового

банкинга. Несмотря на достигнутые успехи в данном направлении, аналитиками отмечается технологическое отставание банковских цифровых систем. Реализация концепции должна содержать следующие этапы: создание цифровых каналов взаимодействия (мобильный банк), инкорпорация цифровых продуктов, повсеместная цифровизация банковских операций, создание цифровой банковской клиентоориентированной модели, в основе которой лежит ИИ. Большинство ключевых российских кредитных организаций таких, как ПАО "Сбербанк";, АО Банк Инноваций и Развития, АО "Райффазенбанк"; и др. перешли на универсальную технологическую платформу для построения сервисов дистанционного обслуживания "CORREQTS", объединяющую цифровые решения для различных категорий клиентов банков и позволяющую автоматизировать все внутренние процессы [1]. Перечисленные преобразования являются предпосылками пересмотра целевых установок в обеспечении цифровой безопасности кредитной организации. В связи с чем требуется проводить систематическое совершенствование программного обеспечения, поскольку именно дисфункции ПО являются проблемными зонами, которыми могут воспользоваться мошенники с целью хищения денежных средств со счетов клиентуры. Проблема безопасности приложений онлайн-банкинга является одной из первостепенных в области обеспечения информационной безопасности, поскольку наличие уязвимостей в программных ресурсах цифровых платформ обуславливает возможность реализации мошенническим схем в банковской сфере, которая всегда вызывала большой преступный интерес. Стоит отметить, что в реальной практике обеспечения цифровой безопасности отсутствует общепринятое толкование понятия уязвимости программного обеспечения, что связано с объединением ошибок, допущенных на этапе программирования (дефект безопасности), и непосредственно известных уязвимостей онлайн-сервисов в одну категорию. Согласно Национальному стандарту Российской Федерации "Защита информации. Уязвимости информационных систем"; уязвимость является недостатком программного средства или ИС в целом, который может быть использован для реализации угроз безопасности информации [3]. Для устранения указанного пробела в целях развития отечественных инструментальных средств выявления уязвимостей следует ввести аналогичный национальный стандарт обеспечения информационной безопасности цифрового банкинга. Что касается мобильных платежных систем и интернет-сервисов, для которых характерно взаимодействие без личного присутствия клиента, то основным риском представляется мошенничество, связанное со злоумышленным использованием персональных данных [4]. Аналитиками предлагаются рекомендации по обеспечению цифровой безопасности, например, корректная реализация протокола OAuth2 и RFC 6749, поскольку типичной ошибкой онлайн-разработчиков ПО для дистанционного банковского обслуживания является нарушение технологии единого входа (SSO), на базе указанного протокола. При совершении подобной ошибки учетные данные могут быть переданы по незащищенному протоколу или же перехвачены мошенниками. Благодаря пенетрации инновационных технологий в банковский сектор, стало возможным использование передовой финансовой аналитики и нового дистанционного способа взаимодействия с клиентами. Таким образом, цифровой банкинг становится неотъемлемым элементом банковского обслуживания. С учетом динамичности развития цифровых технологий и сложности конфигурации программного обеспечения решение рассматриваемой проблемы требует перманентного сканирования уязвимостей, совершенствования методов обеспечения цифровой безопасности и контроля.

Источники и литература

1) CORREQTS [Электронный ресурс]: Сайт компании BSS - Дистанционное банковское обслуживание и управление финансами – Режим доступа:

http://www.bssys.com/solutions/financial-institutions/correqts/ (дата обращения: 07.02.2021).

2) Top 10 Strategic Priorities for Banking in 2017 [Электронный ресурс]: The Financial Brand. - Режим доступа: https://thefinancialbrand.com/62711/top-10-strategic-priorities-for-banking-in-2017/ (дата обращения: 07.02.2021).
3) ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем [Электронный ресурс]: Кодекс – Электронный фонд нормативно-правовой документации - Режим доступа: http://docs.cntd.ru/document/1200123702 (дата обращения: 07.02.2021).
4) Матыцына Ю.Д., Новик А.Г. Обеспечение безопасности цифрового банкинга // «Национальная безопасность как основа конкурентоспособности и экономического роста страны». 2019 С. 144-151.