

Хоткин Андрей Владимирович**Khotkin Andrey Vladimirovich**

студент факультета
«Международные экономические отношения»
Финансового университета при Правительстве РФ

Student, International Economic Relations Department,
Financial University
under the Government of the Russian Federation

ИСПОЛЬЗОВАНИЕ ИТ ДЛЯ ОПТИМИЗАЦИИ ДЕЯТЕЛЬНОСТИ СОВРЕМЕННЫХ БАНКОВ

IT USED TO OPTIMIZE MODERN BANKS ACTIVITY

Аннотация:

Банковская система совершенствуется и с каждым годом становится все более сложной и многогранной. Использование актуальных информационных технологий позволяет не только упростить работу всех отделений банка и сделать ее более слаженной, но и защитить важные сведения, составляющие банковскую тайну. Участвовавшие в последнее время хакерские атаки представляют серьезную угрозу как для отдельного учреждения, так и для всей банковской системы страны. В частности, современные технологии призваны защищать конфиденциальные сведения и предотвращать подобные атаки. В данной статье рассматриваются несколько систем на базе ИТ, применяемых в действующих российских банках, – VoIP, ERP, анализируются их преимущества и слабые стороны. Автор приходит к выводу, что информационные технологии в настоящее время напрямую определяют возможности финансовой организации по развитию бизнеса и совершенствованию внутренних процессов и системы обслуживания клиентов.

Ключевые слова:

защита данных, идентификация сотрудников, VoIP, ERP, автоматизированная банковская система, хранение информации, блокчейн.

Summary:

The banking system is under constant improvement and is becoming more complex and multifaceted year by year. The current information technologies facilitate the collaboration of all bank branches, enhance coherence, and protect sensitive information that is bank secrecy. The recent hacker attacks pose a serious threat to both individual institutions and the entire banking system. In particular, modern technologies are to protect sensitive information and prevent such attacks. The research discusses various IT systems (VoIP, ERP) used by modern Russian banks, examines their strengths and weaknesses. The author concludes that modern information technologies determine the opportunities of companies to run the business and improve business process and customer service system.

Keywords:

data protection, staff identification, VoIP, ERP, automated banking system, data storage, blockchain.

Современная банковская сфера многогранна. Сейчас банки сильно отличаются от тех, что действовали 40–50 лет назад. Изобретение Интернета и серьезный рывок в развитии информационных технологий значительно упростили работу кредитных учреждений, сделав внутреннюю структуру и систему взаимоотношений удобнее для служащих, а сами банки – доступнее и комфортнее для клиентов. В банковской сфере информационные технологии используются в разных формах, как и в любой организации. Самые простые из них – технологии для внутреннего взаимодействия персонала, ведь для эффективной работы подразделений необходима моментальная связь между работниками банка. Это позволяет любому сотруднику беспрепятственно решать любой вопрос клиента, даже если для этого нужно обратиться в другое отделение или головной офис.

Немаловажно, что современные информационные технологии обеспечивают защиту корпоративных данных банка и личной информации о клиентах от несанкционированного доступа посторонних лиц. Сегодня участились случаи мошенничества с использованием ИТ-ресурсов, поэтому системы защиты данных позволяют учреждениям сохранять не только важные сведения, но и репутацию, так как банк, подвергшийся хакерской атаке и потерявший в результате важные данные, уже не будет выглядеть в глазах клиента надежным.

На тему использования современных технологий в банковском бизнесе написано немало научных статей. Так, магистр наук по специальности «инновации и управление персоналом», представитель Торгово-промышленной палаты РФ в Болгарии А.В. Александров в публикации «Информационные технологии в управлении банковской деятельностью» рассматривает применение ИТ-механизмов в банках с позиции менеджмента и приходит к выводу, что, несмотря на значимость новых технологий, человек по-прежнему играет ключевую роль в банковском деле [1]. Кандидат экономических наук, доцент департамента анализа данных, принятия решений и финансовых технологий Финансового университета при Правительстве РФ А.В. Золотарюк в работе «Проблемы

информационной безопасности банков» исследует вопрос безопасных хранения и обработки данных, представляющих банковскую тайну [2]. На примере крупных российских кредитных учреждений автор описывает начало внедрения ИТ в деятельность финансовых организаций.

Упомянутые вопросы сегодня актуальны, однако большинство научных работ на эту тему написано давно, а учитывая постоянное развитие технологий, информация быстро устаревает. В данной статье мы представили свое видение этой проблемы и предложили варианты использования современных технологий в банках.

Наиболее распространенная система для связи внутри учреждения – это VoIP (Voice over Internet Protocol), или технология внутреннего взаимодействия сотрудников. Из перевода становится понятно, что это методика передачи голоса посредством интернет-соединения. Одной из функций VoIP является бесплатная голосовая связь для персонала компании, т. е. корпоративная телефонная сеть. Работники пользуются бесплатным соединением, даже если офисы находятся в разных городах. Контакт между служащими банка становится упрощенным, поскольку сигнал о звонке приходит на рабочее место. Также это удобно для личного пространства, ведь текущие вопросы не будут отвлекать сотрудников в выходные дни. Кроме того, защита информации – основная цель кредитных учреждений, поэтому применение закрытой внутренней сети обеспечит сохранность передаваемых данных. Техническими плюсами сервиса можно назвать легкость внедрения (сеть устанавливается на базе существующей интернет-сети), а также дешевые междугородние звонки. Из издержек – только оплата интернет-трафика [3]. Российские цены на пользование сетью Интернет одни из самых низких, поэтому технология становится выгодной [4], зарубежным предприятиям такое решение может показаться не столь удачным.

Помимо защиты сведений, передаваемых сотрудниками, финансовые организации должны обеспечивать сохранность и достоверность банковской информации. В связи с выходом положения ЦБ РФ № 552-П «О требованиях к защите информации в платежной системе Банка России» многим кредитным учреждениям придется внести изменения в методы функционирования, а именно: «провести работы по "встраиванию" средств криптографической защиты информации в собственные автоматизированные банковские системы для формирования кодов аутентификации и снабжения ими электронных сообщений, а также для формирования защитных кодов и включения их в состав реквизитов электронных сообщений в соответствии с действующим альбомом унифицированных форматов электронных банковских сообщений» [5]. Речь в данной части документа идет об использовании технологий, подобных блокчейн, которая стала хитом на финансовом рынке.

О внедрении бизнес-решений на основе блокчейн написано в отчете Blockchain Technology: from hype to reality на начало 2017 г. индийской компании Infosys [6]. Согласно данному докладу 50 % банков либо уже вложили средства в указанную инновацию, либо планируют это сделать в текущем году. Другая половина ждет, пока инструмент станет зрелым, и на данных этапах развития прибегает только к некоторым ограниченным сценариям ее применения. Треть респондентов ожидает повсеместного распространения технологии в 2018 г., однако большая часть ориентируется на 2020 год. Более 70 % опрошенных представителей финансовых организаций сообщили, что движущей силой внедрения рассматриваемого ресурса стали технические директоры и директоры по инновациям. Таким образом, специалисты в области информационных технологий почти полностью берут на себя развитие банков в сфере безопасности транзакций.

Безусловно, эта система подходит банкам, ведь сохранность первоначальных данных – главное ее достоинство. Помимо этого финансовым учреждениям интересно рассматриваемое решение из-за увеличения скорости проведения транзакций и сокращения времени, затрачиваемого на операции взаиморасчета.

После изучения двух технологий становится ясно, что основная цель использования ИТ-систем в банках – защита данных. Еще одна схема, применяемая для защиты информации, – идентификация сотрудников по биометрическим данным. Примерно 80 % взломов баз осуществляется путем подбора логинов и паролей (Computer Emergency Response Team), более 70 % нарушений безопасности происходит с участием сотрудников банка (CSI/FBI Computer Crime Survey) и около 75 % работников разглашают свои персональные сведения коллегам (SecurEnvoy) [7]. Из статистики следует, что защита идентификационных данных является одним из ключевых критериев эффективной деятельности банка. Поэтому финансовые организации стали пользоваться биометрическими параметрами для идентификации служащих. Отпечатки пальца и оболочку сетчатки глаза скопировать не так просто, как логины и пароли, поэтому кредитные учреждения прибегают к многоуровневой защите на основе этих технологий. Если возникают сомнения относительно выгоды биометрических сервисов, следует обратиться к результатам исследования Gartner Group:

– 150–200 долл. в год тратит каждая компания на администрирование паролей учетных записей сотрудников;

- 60 % запросов в службу поддержки составляют проблемы с учетными записями в связи с тем, что работник либо забыл свой пароль, либо заблокировал учетные данные;
- четверть служащих хранят пароли в текстовых файлах на рабочем столе.

Следовательно, биометрия не только повышает безопасность, но и сокращает издержки на обслуживание паролей сотрудников. Результаты исследования International Biometric Group и Acuity Market Intelligence показали, что 60 % рынка пользуется системой сканирования отпечатка пальца для идентификации персонала. Почему именно она обрела такую популярность? Методика дактилоскопии является более дешевой по сравнению со сканированием сетчатки глаза или распознаванием голоса. Ее точность от этого не становится ниже, о чем свидетельствует применение данного способа в правоохранительных органах всего мира. Кроме того, технология имеет самое большое количество резервных идентификаторов: 10 пальцев в отличие от глаз и голоса. Метод можно назвать высокоскоростным: длительность обработки заявки составляет 3–5 с для базы размером 10 млн экземпляров. Для хранения информации применяется кодирование: после сканирования отпечаток не сохраняется в виде изображения, ему присваивается уникальный код, который в дальнейшем используется. Таким образом, дактилоскопия – оптимальная система по отношению цены к качеству для реализации в банках [8].

Однако какие сведения защищают от угроз банки? Все они применяют ERP-системы для хранения информации о своей деятельности. ERP (Enterprise Resource Planning) расшифровывается как планирование ресурсов предприятия: речь идет о финансовых и трудовых резервах, активах и т. п. Система осуществляет поддержку решений и оптимизацию возможностей компании за счет прикладного программного обеспечения, основанного на данных и процессах, одним словом – хранит всю информацию о функционировании организации.

Что же отличает финансовое учреждение от любого другого? Помимо ERP-системы в каждом банке установлена автоматизированная банковская система (АБС), которая контролирует не работу в целом, а именно профильную деятельность. Это программный комплекс, фиксирующий передвижения денежных средств по счетам, начисление процентов по вкладам и кредитам и прочие операции. В связи с вводом санкций и кризисом, российские банки в настоящее время отдают предпочтение отечественным производителям АБС. Конечно, решения от мировых лидеров SAP и Oracle имеют место на рынке, но составляют меньшинство. В 2015 г. доля зарубежных АБС занимала всего 5 %, а в данный момент зарубежные системы почти не внедряются, осуществляется только модернизация текущих решений [9]. Это дает шансы развитию отечественных технологий, чем изготовители и воспользовались. Можно выделить несколько лидеров среди наших АБС: «Диасофт», «Кворум», БИС и «Новая Афина». Бренды предоставляют типизированные решения для банковской сферы с возможностью доработки под конкретную структуру учреждения. Возвращаясь к заданному вопросу, ответим, что именно сведения, хранимые в АБС, кредитной организации необходимо защищать.

В заключение еще раз отметим важность применения современных информационных технологий в банковском секторе. Они не только упрощают деятельность сотрудников и клиентов, но и защищают важные конфиденциальные сведения от возможных попыток третьих лиц получить их. В частности, системы защиты информации помогают предотвратить хакерские атаки с целью завладеть средствами клиентов и нарушить работу всех отделений организации. Применение описанных средств также способствует существенному сокращению количества утечек информации со стороны самих служащих. Об этом стали часто заявлять руководители крупных финансовых учреждений, таких как Сбербанк и ВТБ. Кроме того, информационные системы могут предотвратить невынужденные ошибки персонала, которые отрицательно влияют на функционирование всей сети представительств.

Мы пришли к выводу, что информационные технологии в настоящее время уже не являются тем второстепенным обслуживающим элементом в деятельности банка, каким они были некоторое время назад, а напрямую определяют возможности организации по развитию бизнеса, совершенствованию внутренних процессов и структуры обслуживания клиентов. В связи с этим менеджменту современного кредитного учреждения необходимо уделять пристальное внимание использованию и модернизации IT-систем и устройств, чтобы не только обезопасить себя, свои корпоративные сведения и персональные данные клиентов, но и сохранить деловую репутацию и выдержать серьезную конкуренцию на мировой финансовой арене.

Ссылки:

1. Александров А.В. Информационные технологии в управлении банковской деятельностью // Образовательные ресурсы и технологии. 2015. № 3. С. 89–95.

2. Золотарюк А.В., Федотовская В.А., Кретова Е.А. Проблемы информационной безопасности банков // Научные исследования: от теории к практике : материалы X Международной научно-практической конференции. В 2 т. Чебоксары, 2016. Т. 2. С. 147–149.
3. Что такое VoIP? Технология цифровой аудиосвязи через интернет-телефонию [Электронный ресурс] // Live Business. URL: <http://www.voipoffice.ru/tags/VOIP> (дата обращения: 11.06.2018).
4. Поляков А. Интернет и кошелек: сколько стоит доступ в сеть в разных странах мира [Электронный ресурс] // РИА «Новости». 2016. 25 окт. URL: <https://ria.ru/technology/20161025/1479892670.html> (дата обращения: 11.06.2018).
5. Пискунов И. Положение № 552: новые требования Банка России к безопасности платежных систем [Электронный ресурс] // Информационная безопасность : персональный блог И. Пискунова о безопасности, ИТ-менеджменте и управлении проектами. URL: <https://ipiskunov.blogspot.ru/2017/01/552.html> (дата обращения: 11.06.2018).
6. Ast A. Что такое блокчейн-технология? Пошаговое руководство для новичков [Электронный ресурс] // BitNovosti. 2017. 2 марта. URL: <https://bitnovosti.com/2017/03/02/cto-takoe-tehnologija-blokchein-posagovoe-rukovodstvo-dlja-novichkov-1> (дата обращения: 11.06.2018).
7. Blockchain technology. From hype to reality [Электронный ресурс] // Infosys Finacle. 2017. Febr. URL: http://images.experienceinfosys.com/Web/Infosys/%7B6f314800-4c3c-4d4a-b092-4b11ea532d56%7D_Edgeverve_Infosys-Finacle_Blockchain-Technology-Hype-to-Reality.pdf (дата обращения: 11.06.2018).
8. Идентификация сотрудников банка [Электронный ресурс] // Биометрия Сервис. URL: <http://biometris.ru/sotrudnikov-banka> (дата обращения: 11.06.2018).
9. Батаев А.В. Анализ российского рынка иностранных автоматизированных банковских систем // Молодой ученый. 2016. № 27. С. 351–354.

References:

- Aleksandrov, AV 2015, 'Information technologies in banking management', *Obrazovatel'nyye resursy i tekhnologii*, No. 3, pp. 89-95, (in Russian).
- Ast, A 2017, 'What is blockchain technology? A step-by-step guide for beginners', *BitNovosti*, March 02, viewed 11 June 2018, <<https://bitnovosti.com/2017/03/02/cto-takoe-tehnologija-blokchein-posagovoe-rukovodstvo-dlja-novichkov-1>>, (in Russian).
- Bataev, AV 2016, 'Analysis of the Russian market of foreign automated banking systems', *Molodoy uchenyy*, No. 27, pp. 351-354, (in Russian).
- 'Blockchain technology. From hype to reality' 2017, *Infosys Finacle*, February, viewed 11 June 2018, <http://images.experienceinfosys.com/Web/Infosys/%7B6f314800-4c3c-4d4a-b092-4b11ea532d56%7D_Edgeverve_Infosys-Finacle_Blockchain-Technology-Hype-to-Reality.pdf>.
- Piskunov, I 2018, 'Directive No. 552: new requirements of the Bank of Russia to the security of payment systems', *Informatsionnaya bezopasnost': personal'nyy blog I. Piskunova o bezopasnosti, IT-menedzhmente i upravlenii proyektami*, viewed 11 June 2018, <<https://ipiskunov.blogspot.ru/2017/01/552.html>>, (in Russian).
- 'What is VoIP? Digital audio technology via Internet telephony' 2018, *Live Business*, viewed 11 June 2018, <<http://www.voipoffice.ru/tags/VOIP>>, (in Russian).
- Zolotaryuk, AV, Fedotovskaya, VA & Kretova, EA 2016, 'Problems of information security in banks', *Nauchnyye issledovaniya: ot teorii k praktike: materialy X Mezhdunarodnoy nauchno-prakticheskoy konferentsii*, in 2 vols., Cheboksary, vol. 2, pp. 147-149, (in Russian).