УДК 336.719

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В РОССИЙСКИХ БАНКАХ И БЕЗОПАСНОСТЬ ДАННЫХ

***Левшин М.А.*[1]**

студент
Финансовый университет при Правительстве Российской Федерации,
Россия, Москва

Аннотация: В ходе данной работы были рассмотрены отрасли информационных технологий в банковской сфере, а также безопасность самих данных. По итогам работы были выявлены различного рода проблемы и угрозы, присущие данным областям банковского дела. В результате исследования также были определены и меры по снижению рисков угроз, возможные решения проблем с помощью цифровизации, роботизации и повсеместной информатизации.

Ключевые слова: Банки, безопасность данных, информационные технологии, информационная безопасность, роботизация, киберпреступления, кибербезопасность, цифровизация, информатизация.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В РОССИЙСКИХ БАНКАХ И БЕЗОПАСНОСТЬ ДАННЫХ

Levshin M.A .

student

Financial University,

Moscow, Russia.

[1] ***Научный руководитель: Александрова Л.С.,*** к.э.н. доцент Финансового Университета *при Правительстве Российской Федерации*, Россия, Москва.

Аннотация: In the course of this work, the information technology industries in the banking sector were considered, as well as the security of the data itself. As a result of the work, various problems and threats inherent in these areas of banking were identified. The study also identified measures to reduce the risks of threats, possible solutions to problems through digitalization, robotics, and ubiquitous Informatization.

Ключевые слова: Banks, data security, information technology, information security, robotics, cybercrime, cybersecurity, digitalization, Informatization.

Современное общество стремительно развивается. Повсеместно используются информационные технологии, в том числе и в банковской сфере. Информационные технологии значительно изменили жизнь каждого пользователя банковских услуг в лучшую сторону. Именно поэтому внедрение и использование передовых информационных технологий — это новый ключ к победе в конкурентной борьбе среди банков. Возникает вопрос – обеспечивается ли безопасность персональных данных? Обеспечение безопасности личных данных – это важная часть услуг, предоставляемых банками, так как при недостаточно эффективной системе безопасности страдают не только пользователи банка, но также и репутация банка, и сам банк. На данный момент Россия находится на этапе формирования полноценного информационного общества, в связи с чем, у граждан возникает сильная обеспокоенность вопросами сохранности персональных данных [7].

Начать анализ применения информационных технологий стоит с определения размера российской экономики, так как именно ее масштабы предопределяют потребности в информатизации банковского сектора [12]. Являясь шестой страной в мире по размеру экономики, Россия, а значит и

уровень информатизации банковского сектора, практически не отстают от наиболее развитых в IT сфере стран [5].

С 1991 года на территории Российской Федерации действует «ЦФТ (Центр финансовых технологий)» [13]. Целью данной организации является «обеспечение доступа участников финансовой индустрии к передовым технологиям для ведения бизнеса и предоставления финансовых услуг клиентам». Клиентами данной организации являются 22 крупнейших российских банка. ЦФТ занимает лидирующие позиции в различного рода рейтингах, связанных с IT услугами, разработкой программного обеспечения, в общих списках IT компаний России.

С 2016 года на территории Российской Федерации действует «Ассоциация развития финансовых технологий (Ассоциация «ФинТех»)» [1]. Ассоциация «ФинТех» была создана по инициативе Банка России, а также основных участников российского финансового рынка. Целью данной организации является формирование уникальной по своей сущности площадки, для обоюдовыгодного взаимодействия между регулятором – в лице Центрального Банка – и представителями бизнеса – в лице коммерческих банков. На территории данной площадки формируются экспертные мнения и оценки различных инновационных информационных технологий. Различные эксперты называют данную ассоциацию монополией Банка России на право предоставления передовых информационных технологий, однако на деле происходит недопущение лоббирования интересов крупнейших банков. Банк России следит за тем, чтобы банк любого размера имел доступ к информационным технологиям, чтобы иметь возможность обеспечивать информационную безопасность в соответствии со всеми нормативами.

Примером такой значимой технологии является «Единая Биометрическая Система (ЕБС)» [5].

Таким образом, на территории Российской Федерации существуют различные организации, цель которых заключается в обеспечении коммерческих банков передовыми информационными технологиями в финансовой сфере. Еще одним ярким примером является такая разработка, как «Система Быстрых Платежей (СБП)». Значение и актуальность данной разработки подчеркивают многие ведущие экономисты России [5].

Кроме того, многие банки имеют свои собственные разработки в различных сферах. Конкурентоспособность банков в применении и использовании информационных технологий крайне высока. Это наглядно демонстрирует таблица 1.

Таблица 1 - Анализ выручки компаний от IT проектов.

2018	**2017**	**Компания**	**Выручка ИТ-проектов в банках в 2018 году, млн руб. с НДС**	**Выручка ИТ-проектов в банках в 2017 году, млн руб. с НДС**	**Динамика 2018/2017, %**	**Ключевые заказчики**
1	-	Центр Финансовых Технологий (ЦФТ) *	22 600	20 500	10,2	ВТБ, Банк ТКБ, РСХБ, Банк Зенит, МТС Банк
2	1	Сбертех	20 533	30 320	-32,3	
3	-	Софтлайн	18 250	13 619	34	

4	3	ITG	13 009	12 618	3,1	ВТБ, Банк России, Газпромбанк, Московский Индустриальный банк, Московский кредитный банк, Промсвязьбанк, Сбербанк, Связь-Банк, ЮниКредит Банк, Альфа-Банк, Райффайзенбанк
-	4	Инфосистемы Джет**	12 323	10 128	21,7	Группа ВТБ, Росбанк, Тинькофф Банк, «Альфа-Банк», «Почта Банк», Банк Уралсиб, Банк «ФК Открытие», ЮниКредит Банк, «Россельхозбанк», «Газпромбанк»

Источник: TAdviser[2]

Банки все чаще и чаще обращаются к частным фирмам для интеграции новейших информационных технологий в свой бизнес. К такому выводу можно прийти, проанализировав динамику роста выручки от IT проектов компаний посредников. Наблюдается стабильный рост, а значит банки все больше и больше прибегают к совершенствованию используемых в них IT технологий и разработок.

Однако, рост применения информационных технологий в банках ведет к появлению новой угрозы – угрозы безопасности личным данным клиентов. Так,

[2] Официальный сайт компании TAdviser // Режим доступа: https://www.tadviser.ru (дата обращения 20.10.20)

например, завладев личными данными клиента, мошенники могут беспрепятственно украсть денежные средства, финансовые ресурсы, а также финансовые активы граждан. Такими утечками в первую очередь знаменит «СберБанк» [10] [11], однако утечки данных являются реальной угрозой как для рядового пользователя, так и для любого банка.

Утечки данных представляют собой либо разглашение данных клиентов банка третьими лицами, либо утечку данных через компьютерные системы и различного рода технические средства [4].

С точки зрения законодательства – утечка данных – это правонарушение, за которое предусмотрены уголовная, административная, гражданско-правовая и дисциплинарная ответственность [14].

На территории Российской Федерации используются для осуществления информационной безопасности такие меры, как:

- Разработка мер Банка России в сфере защиты информации;
- Разработка стандартов, в области обеспечения информационной безопасности;
- Создание Единой Биометрической Системы (ЕБС);
- Страхование кибер-рисков.

В 2019 году Центробанк выявил более 700 нарушений, связанных с обеспечением кибербезопасности [9]. Это вызвано в большей мере тем, что банки предпочитают иметь информационную безопасность «на бумаге» [8]. Это значит, что у большинства российских банков нет достаточной системы информационной безопасности, обеспечивающей необходимый уровень защиты данных, однако Банк России активно с этим борется. Наличие проверок и оценки эффективности банков уже говорит об исследовании Центробанком данной проблемы. В качестве мер по ее решению применяются различные

санкции. Так, например, в октябре 2019 года в интервью журналистам А. Сычев – первый заместитель директора департамента информационной безопасности – заявил о начале применения санкций в виде штрафов по отношению к банкам, у которых отсутствует «антифрод» система [3]. Уже 24 марта 2020 года Центробанк порекомендовал определенные меры по обеспечению кибербезопасности в условиях «COVID-19».

В качестве стандартов по информационной безопасности можно выделить:

- Письмо банка России от 24.03.2014 г. №49-т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности»;
- Гост Р 57580.1-2017 «безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»;
- ФЗ «О безопасности критической информационной инфраструктуре Российской Федерации» от 26.07.2017 г. №187-ФЗ;
- ПП № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Положение банка России от 24.08.2016 г. №552-П «О требованиях к защите информации в платежной системе банка России»;
- ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. №149-ФЗ и другие.

В качестве страхования кибер-рисков можно привести пример продукта Ингосстраха [6]. Страховая компания обеспечивает заказчика различными инструментами для обеспечения постоянного мониторинга подозрительной активности. Происходит защита денежных средств, электронных данных и IT –

инфраструктуры в целом как от внешних атак, так и от банальных технических сбоев. В случае возникновения каких-либо проблем страховая компания обязуется компенсировать часть потерь.

При использовании FinTech, как у коммерческих банков, так и у банковской системы в целом, появляются новые возможности, однако, при этом растут и риски. [2, с.169-170]

В качестве основных проблем, связанных с информационной безопасностью, аудиторами в сфере информационной безопасности выделяются [8]:

- Дефицит финансирования отдела, занимающегося информационной безопасностью;
- Недостаток высококвалифицированных кадров;
- Аудит, проводимый в сфере информационной безопасности «по фотографиям» и «на бумаге».

Для решения этих проблем необходимы проверки банков со стороны регулятора; необходим контроль за аудиторскими компаниями, осуществляющими аудит в данной сфере; необходимо время, так как именно со временем современные банки «эволюционируют» в банки «будущего», для которых информационная безопасность будет ключом к привлечению клиентов.

В качестве главной угрозы для информационной безопасности можно выделить сотрудников самого банка. Нередки случаи, когда «белые воротнички», используя свои полномочия, завладевают конфиденциальными данными и продают их мошенникам. Возможны и иные случаи, когда «верхушка» банка, имеющая доступ к данным – уходит к банку-конкуренту, располагая такими важными данными как информация о VIP-клиентах,

банковская маржа, коммерческая тайна и прочие. Это необходимо для выстраивания более конкурентоспособной стратегии развития [12]. Решением данной проблемы, вызванной «человеческим фактором», может выступать лишь полная информатизация и цифровизация банковских процессов, переход к роботизации, к чему и стремятся большинство банков. Именно поэтому лидеры рынка «инвестируют» в информатизационные технологии (Таблица 1).

Современные банки на всех уровнях своей архитектуры должны стремиться к инновационной модели «Банк будущего» (Рисунок 1).

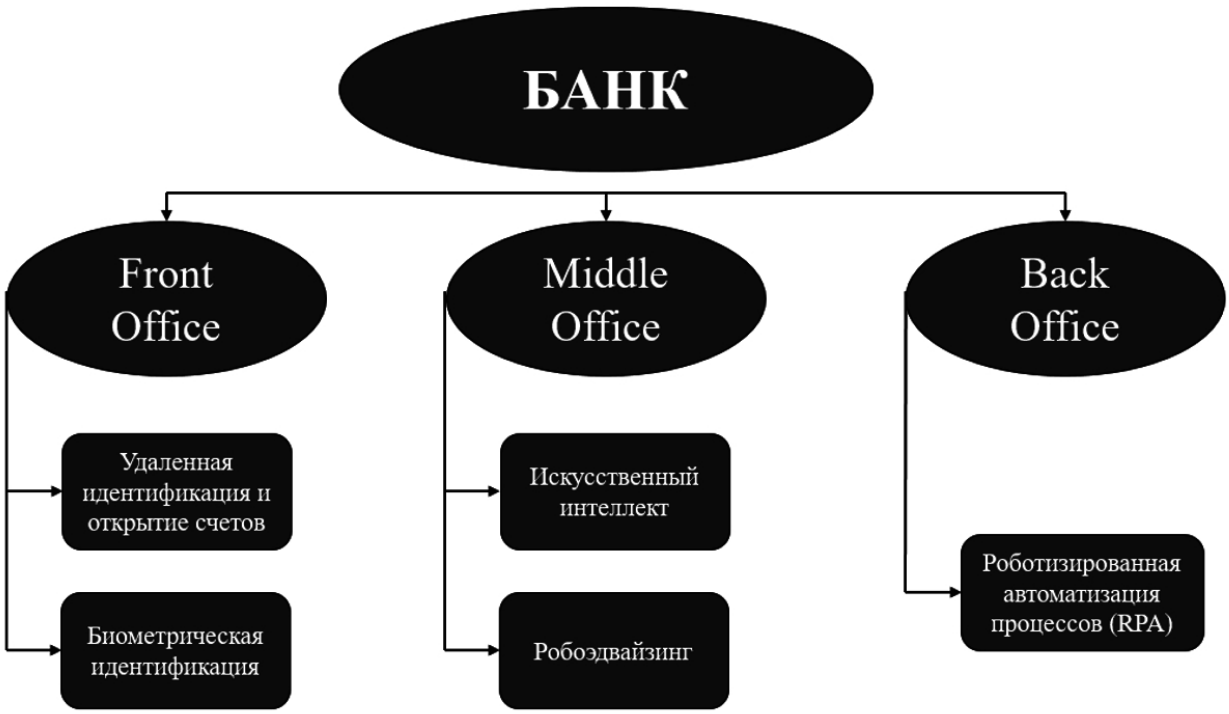

Рисунок 1 - Банк Будущего. Источник: TAdviser[3]

Во фронт-офисе — это удаленная биометрическая идентификация клиента, вместо использования привычных пластиковых карт. В мидл-офисе –

[3] Официальный сайт компании TAdviser // Режим доступа: https://www.tadviser.ru (дата обращения 20.10.20)

это синергия искусственного интеллекта и аналитической сферы, основанной на хранилищных данных. Цель мидл-офиса – более эффективный «скоринг», повышение конкурентоспособности банка и эффективности маркетинговых мероприятий. В бэк-офисе – роботизированная автоматизация процессов для снижения издержек.

Исходя из всего выше сказанного, можно сделать вывод о том, что для банков важно внедрение новейших информационных технологий. Это обеспечит приток новых клиентов, повысит качество предоставляемых услуг, что является профилактической и превентивной мерой по недопущению оттока клиентов. Тем не менее, при этом важно не забывать про информационную безопасность, так как она является частью экономической безопасности банка, играет огромную роль в репутации банка и прямо влияет на количество клиентов, а соответственно и прибыль банка. В России на данный момент существует огромное количество методов по обеспечению информационной безопасности. Причем, данная проблема настолько значима, что даже государство, в лице Банка России, осуществляет контроль за соблюдением необходимого минимума по обеспечению информационной безопасности, а также оценивает новые технологии и дает рекомендации, связанные с угрозами кибер-преступлений.

Подводя итог, можно сказать, что на сегодняшний день в России все еще существуют серьезные проблемы, связанные с информационной безопасностью банковского сектора. Эти проблемы носят системный характер. Тем не менее, банки и Банк России активно борются с этим. Реальное количество проблем снижается. Это достигается за счет сотрудничества власти в лице Банка России и представителей бизнеса. Наиболее значимые технологии, цель которых заключается в обеспечении информационной безопасности, передаются в

общее пользование всем банкам. Другими значимыми факторами в информационной безопасности банков являются: повсеместное распространение и применение новейших информационных технологий; повсеместная цифровизация; переход к новейшим моделям работы банков. Только использование совокупности методов по повышению информационной безопасности банков обеспечит стабильную систему, работающую не только на бумаге, но и защищающую как клиентов банка, так и сам банк от возможных проблем. Кроме того, внедрение перечисленных методов в работу банков позволит обеспечить приток клиентов и снизить издержки на обслуживание кредитов, депозитов и проведение банковских операций, что положительно скажется не только на прибыли банков, но и на их репутации.

Библиографический список

1. Ассоциация «ФинТех» [Электронный ресурс]. — Режим доступа — URL: https://fintechru.org/ (дата обращения 20.10.20)
2. Банки и финтех-компании: взаимодействие и конкуренция: монография. - /Под ред. Л.С.Александровой – Москва: РУСАЙНС, 2020.
3. Ведомости – ЦБ впервые оштрафует банки за отсутствие систем распознавания мошеннических операций [Электронный ресурс]. — Режим доступа — URL: https://www.vedomosti.ru/finance/news/2019/10/10/813384-dva-banka (дата обращения 20.10.20)
4. Гамза, В. А. Безопасность банковской деятельности /В.А. Гамза // Экономика. Бизнес. Банки. 2017. Т. 3. С. 263-268.
5. Информационный портал TAdviser [Электронный ресурс]. — Режим доступа — URL: https://tadviser.ru/ (дата обращения 20.10.20)
6. ИнгосСтрах – «Ингосстрах» и «Информзащита» представляют новый продукт по киберстрахованию [Электронный ресурс]. — Режим доступа — URL: https://www.ingos.ru/company/news/detail/788471/ (дата обращения 20.10.20)
7. Крохина Ю. А. – Без бумажки – человек /Ю.А.Крохина. - //Профиль 28 – 29. (132) 27.07.2002. С. 7

8. КомНьюс – Как меняется информационная безопасность в российских банках [Электронный ресурс]. — Режим доступа — URL: https://www.comnews.ru/content/209347/2020-10-01/2020-w40/kak-menyaetsya-informacionnaya-bezopasnost-rossiyskikh-bankakh (дата обращения 20.10.20)

9. РИА Новости – ЦБ усилит надзор над киберустойчивостью банков [Электронный ресурс]. — Режим доступа — URL: https://ria.ru/20191106/1560626650.html (дата обращения 20.10.20)

10. РосБизнесКонсалтинг (РБК) – Сбербанк выявил новые утечки данных карт своих клиентов [Электронный ресурс]. — Режим доступа — URL: https://www.rbc.ru/finances/07/10/2019/5d9b874f9a79475c84375ca0 (дата обращения 20.10.20)

11. РосБизнесКонсалтинг (РБК) – СМИ обнаружили новую утечку данных клиентов СберБанка [Электронный ресурс]. — Режим доступа — URL: https://www.rbc.ru/finances/14/02/2020/5e46339a9a794720b519014f (дата обращения 20.10.20)

12. Скиннер К. Цифровой человек /К.Скиннер - // Экономика. Технологии. Банки. 2020. Т.1. С. 63-69.

13. Центр Финансовых Технологий [Электронный ресурс]. — Режим доступа — URL: https://cft.group/ (дата обращения 20.10.20)

14. Электронный ресурс «Консультант плюс» – ФЗ №152 «О персональных данных» [Электронный ресурс]. — Режим доступа — URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 20.10.20)

Оригинальность 91%