ЭКОНОМИЧЕСКИЕ НАУКИ

ОСОБЕННОСТИ И ПЕРСПЕКТИВЫ БИОМЕТРИЧЕСКИХ МЕР БЕЗОПАСНОСТИ В ОПЕРАЦИЯХ С ПЛАТЕЖНЫМИ БАНКОВСКИМИ КАРТАМИ

DOI: 10.31618/ESU.2413-9335.2020.6.73.688

Джаксыбекова Г.Н.
д.э.н., профессор
Пулатов И.
магистрант 1 курса
профильной магистратуры
по специальности «Финансы»
УО «Алматы Менеджмент университет»,
г. Алматы Казахстан

АННОТАЦИЯ

В данной статье рассмотрены проблемные аспекты особенностей и перспектив биометрических мер безопасности в операциях с платежными банковскими картами.

Биометрическая идентификация клиентов - одна из самых инновационных и современных технологий на рынке банковских услуг. Инновационные технологии идентификации способны поднять не только экономику казахстанского банка, но и имидж банка, а также несут в себе огромные перспективы для развития не только банковской сферы, но и экономики в целом.

ANNOTATION

This article discusses the problematic aspects of the features and prospects of biometric security measures in operations with payment bank cards.

Customer biometric identification is one of the most innovative and modern technologies in the banking services market. Innovative identification technologies are capable of raising not only the economy of a Kazakhstani bank, but also the image of the bank, and also have enormous prospects for the development of not only the banking sector, but also the economy as a whole.

Ключевые слова: банк, карта, биометрия, система биометрической идентификации, платеж, инновационные технологии, банковские (финансовые) инновации, безопасность, защита, мошенничество, интернет, мобильный банкинг, банкомат, скимминг, ,сканирование, конкурентоспособность.

Keywords: bank, card, biometrics, biometric identification system, payment, innovative technologies, banking (financial) innovations, security, protection, fraud, Internet, mobile banking, ATM, skimming, scanning, competitiveness.

Введение

На сегодняшний день каждый банк стремится предложить клиенту широкий спектр новых продуктов и услуг, с помощью которых появляется перспектива повысить конкурентоспособность, так как классические продукты и услуги становятся методом второго плана завоевания клиентов. Для большей конкурентоспособности на банковском рынке, необходима многовариантность и нестандартность предлагаемых условий, отличие проводимых финансовых операций, одним словом инновационность в работе банков второго уровня. Постоянное увеличение роли инноваций является важной особенностью в банковской сфере, позволяющее банку развиваться и занимать ключевые позиции на рынке. Банковские инновации являются актуальной темой для обсуждения, используются как на бытовом, так и на профессиональном уровне.

Согласно мнению участников Всемирного экономического форума, бизнес среда продолжает изменяться и по сей день, а сектор финансовых услуг нуждается в решении многих вопросов, чтобы быть конкурентоспособным. В частности, технологии и инновации являются вопросами высшего звена; они создают как возможности, так и угрозы [1].

Внедрение и развитие финансовых нововведений в мировой системе объясняется ростом числа населения в мире, что способствует росту потенциальных клиентов на финансовом поле, бурным ростом передовых технологии в этом столетии, несмотря на ограниченность финансовых, производственных ресурсов. Это все, бесспорно, новые предпосылки для развития социально-экономических отношений в нынешнем обществе, где главная роль будет отведена финансовым институтам как особому звену социально-экономической системы государства.

Основная причина инноваций - это «технологический толчок» и «вызов спроса». Инновации предложения и инновации спроса выбирают в соответствии со значимостью исходя из приоритетности каждого [3.

В случае успешного внедрения нововведении, положительного развития инновационных технологий в банковской сфере, будут достигнуты:

- создание конкурентной среды в сфере банковских продуктов и услуг;
- концентрация занятости банковских сотрудников во фронт-офисах без отвлечения на консультации, текущего обслуживания клиентов;
- обеспечение оптимизации и совершенствования банковских операций;

- конкурентоспособность банковских продуктов и услуг не только на отечественном, но признания на мировом рынке[2].

Цель исследования

Тенденция банковского дела во всем мире сводится к тому, что потребители банковских продуктов и услуг стали реже обращаться в отделения, выбирая услуги использования интернет- и мобильного банкинга.

С нашей точки зрения, всего 10 лет назад казахстанские банки еще не спешили внедрять банковские продукты и услуги через интернет в Казахстане. На тот момент, как банки, так и клиенты, считали интернет несовершенным, не серьезным видом бизнеса, за исключением тех, кто на сегодняшний день представляет Топ-5 казахстанских банков.

Внедрение платежных карт в Республике около двадцати лет ранее не сразу было воспринято казахстанскими потребителями, вызывая разную реакцию: к примеру, если некоторые стали развивать новый продукт, то другие еще относились недоверчиво. На сегодняшний день представление клиента банка без наличия платежной карты невозможно.

В этих условиях особенно актуальной проблемой является вопрос защиты клиентов банка при реализации операций с платежными картами.

Целью исследования является внедрение новой услуги для клиентов банков Казахстана – совершенствование системы идентификации личности клиентов для повышения безопасности дистанционного банковского обслуживания и **предотвращения фактов мошенничества** при совершении платежей и снятии наличности с банкоматов.

Материал и методы исследования

По мере развития информационных технологий, увеличиваются и методы исследования вопросам укрепления систем безопасности и снижения риска мошенничества в сфере платежей. Исследование тенденций развития новых форм платежей и переводов подразумевает собой, как и экономико-статистические методы, так и методы оценки рисков и снижения мошенничества, обеспечения безопасности счетов и переводов клиентов банка. Наиболее популярным видом мошенничества сегодня является скимминг (от англ. skimming) — кража данных держателя карты, с помощью специального устройства считывающего информацию (скиммера). Мошенники копируют всю информацию с карты (имя владельца, номер карты, срок действия, CVV- и CVC-код), узнать ПИН-код можно используя мини-камеры или накладки на клавиатуру банкомата. Жертвой скимминга могут быть лица, снимающие не только наличные, но и оплачивающие покупки в торговых точках используя платежные терминалы.

Гео-блокирование инициировано компаниями стран Европы, с целью исключения сделок с потребителями из стран с высоким уровнем мошенничества в сфере платежных систем. Таким образом, в банковских информационных системах мониторинга безопасности прописываются ограничения на использование пластиковых карт в «критичных» регионах, где зарегистрировано много случаев мошенничества. Сегодня таким регионам относятся Украина, Египет, Италия, Турция, Таиланд, Шри-Ланка, Англия и США.

Для обнаружения факта мошенничества платёжные системы и банки используют системы фрод-мониторинга, анализирующие транзакции клиентов и принимающие дальнейшие действия на основании своего вывода по каждой из транзакций. В основе таких систем могут находиться модели, построенные с использованием алгоритмов машинного обучения, выполняющих задачу классификации.

Компания Hitachi разработала инновационную технологию FingerVein как способ идентификации клиента-владельца счета с помощью метода отслеживания линий. Суть метода заключается в том, что программа сканирует цифровое изображение для темных пятен вен на отпечатках пальцах руки. Данная технология обеспечивает простоту использования геометрии кисти с гораздо более высокой точностью, меньшими размерами считывателей и меньшим количеством контактов. Система FingerVein сканирует вены на пальцах, а затем сопоставляет их с заранее установленными шаблонами.

Результаты исследования и их обсуждение

П. Семикова выделяет лимитированные банковские продукты (продукт, объем или количество выпуска, которого, строго квотируется (например, акции, облигации, кредитные соглашения и др.) и нелимитированные банковские продукты (продукт, объем или количество выпуска, которого, не зависит от каких-либо квот (например, пластиковые, расчетные и кредитные карты, банковские счета и т.п.) [4, с. 34].

На конкурентном рынке многие банки стараются расширить не только продуктовую линейку и совершенствовать условия по их обслуживанию, но и применить технологические решения, для быстроты проведения той или иной операции. Одним из подобных технологических новшеств стало развитие системы «электронных очередей» в банках, которое существенно снизило время и моральное напряжение клиентов.

Система безконтактных платежей payWave была представлена банками второго уровня Казахстана в 2013 году, а летом 2014 года такая система уже работала посредством мобильных телефонов [5].

В казахстанских банках, а также в АО «Казпочта» клиенты могут провести переводы денежных средств через следующие системы: Система Всемирного почтового союза, Золотая корона, Faster, Contact, Быстрая Почта, WesternUnion, Migom, InterBanking, Блиц, Анелик, Лидер, MoneyGram, Unistream, CoinstarMoneyTransfer, IntelExpress и т.д.

Общее количество переводов денег, осуществленных на территории Республики,

составило 42,1% от общего объема, и 33,4% от общей суммы проведенных переводов через СДП. Количество денежных переводов, которые были отправлены за рубеж, составили 77,9% и 86,6% соответственно, что объясняется их активным применением для осуществления трансграничных платежей как схожего услугам банков по осуществлению платежей посредством счетов, открытых на основе корреспондентских отношений с банками- нерезидентами.

С помощью СДП за рубеж было проведено 1 785,0 тыс. операций на сумму 238,8 млрд. тенге в 2019 году. В общей сложности динамика изменения размеров платежей за 2019 годстабильная по сравнению с предыдущим годом по количеству на 12,0% и по сумме переводов - на 16,9%.

Банки Казахстана и АО «Казпочта» предоставляют клиентам услуги по различным системам перевода. Таблица 1 наглядно демонстрирует количество и суммы переводов, которые были отправлены за рубеж.

Таблица 1

Переводы денег в Республике Казахстан в 2019 году, отправленные за рубеж в разрезе систем денежных переводов.

Система	Кол-во (тыс. транзакций)	Доля от общего кол- ва, в %	Сумма (млн. тенге)	Доля от общей суммы, в %
Золотая корона	697,3	39,1%	83 265,6	34,9%
WesternUnion	276,5	15,5%	44 959,0	18,8%
Contact	253,5	14,2%	36 047,8	15,1%
Юнистрим	177,9	10,0%	26 160,7	11,0%
Блиц	122,1	6,8%	13 754,6	5,8%
Система Всемирного почтового союза	83,7	4,7%	3 343,0	1,4%
Faster	70,7	4,0%	7 026,7	2,9%
Быстрая почта	45,7	2,6%	9 118,2	3,8%
MoneyGram	20,7	1,2%	3 480,5	1,5%
Лидер	17,0	1,0%	5 164,7	2,2%
Анелик	11,0	0,6%	5 387,7	2,3%
Почтовые международные переводы	7,2	0,4%	291,5	0,1%
InterBanking	0,9	0,05%	587,5	0,2%
InterExpress	0,3	0,02%	50,7	0,02%
Migom	0,09	0,005%	144,3	0,1%
Восточный Экспресс	0,004	0,0002%	2,9	0,001%
Система Киберплат	0,5	0,03%	35,9	0,02%
Общий итог	1 785	100,0%	238 821,2	100,0%
Примечание – составлено автором на основе источника [6]				

Основное количество отправленных переводов с помощью СДП проведено в долларах США, основная масса которых по объему составила 62,1% и по сумме 73,6%.

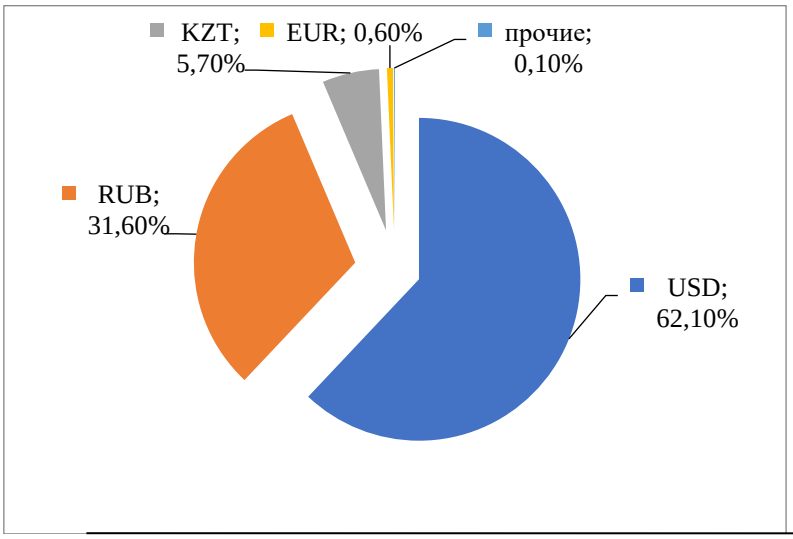

Рисунок 1 - Доля отправленных переводов за рубеж от общего количества отправленных переводов по Республике Казахстан

Примечание - составлено автором на основе [6]

Вместе с тем растут число мошеннических случаев с банковскими картами и количество украденных с электронных счетов денег. Например, в 2018 году в банках второго уровня Республики Казахстан подобным образом было украдено 190 млн. тенге, что на 44% больше, чем в 2017 году, а число зарегистрированных дел о мошенничестве с банковскими картами за первую половину 2019 года выросло в 8 раз по сравнению с тем же периодом 2018 года [7]. Более того, по прогнозам Group-IB, число атак в сфере банковских карт продолжит расти. Это говорит о необходимости своевременного реагирования на мошеннические действия в банковской сфере и об актуальности поиска подходов к решению данной задачи.

В Европейском докладе за 2019 год о преступности связанной с банкоматами, инциденты мошенничества, связанные с банкоматами, снизились на 26 % по сравнению с 2018 г., хотя связанные потери выросли на 13%, т.е. произошло снижение атак мошенничества с банкоматами на 26 %, с 21 346 в 2018 году до 15 702 в 2019 г. Это падение было в основном обусловлено сокращением на 95% TRF – мошенничеств (мошенничество, связанное со снятием наличных денежных средств в банкомате) и сокращением захвата наличных денежных средств на 31%. Было зарегистрировано 5631 карта с инцидентами на скимминг (skimming), что снизилось на 3 % по сравнению с 5822 картами в 2018 году.

Потери, связанные с мошенничеством с банкоматами, поднялись на 13 % по сравнению с 2018 (с 248 млн. Евро до 280 млн. Евро). Этот рост был в основном обусловлен ростом в 18% в международных потерях при скимминге (с 201 млн. Евро до 238 млн. Евро). Большинство таких потерь было зарегистрировано в США и в Азиатско-Тихоокеанском регионе. Внутренние потери при скимминге упали на 9% за тот же период.

Рост международных потерь при скимминге не наблюдается в Европейских странах, где широко реализовано блокирование региональных карт, так же известное как гео– блокирование. Использование активной магнитной полосы на европейских EMV -картах продолжает делать карты более уязвимыми к скимингу, поэтому гео - блокорование значительно снижает риск успешного мошенничества.

Физические атаки, связанные с банкоматами, упали на 6 % по сравнению с 2018 г. (с 2102 до 1980 случаев). Это частично объясняется снижением применения газовых и взрывоопасных атак на 11%. Было зарегистрировано 619 таких нападений, которые снизились с 696 в 2018 г. Девять стран сообщили о таких атаках, пять из которых с более 40000 установленными банкоматами.

В 2019 году после первых в Западной Европе собрана статистика по вредоносным программам использованных в банкоматах. Это были программы с атаками на «обналичивание» или «срывание джекпота (всего банкомата)". В 2019 году было зарегистрировано 51 таких инцидентов, связанных с потерями в 1,23 млн. Евро [8].

В таблице 2 представлено краткое изложение криминальной статистики мошенничества с банкоматами в Европе по основным направлениям.

Таблица 2

Общая криминальная статистика мошенничества с банкоматами в Европе

Наименование	2015	2016	2017	2018	2019	% +/-2018/2019
Мошеннические атаки, связанные с банкоматами:						
Общее количество опубликованных инцидентов	12,383	20,244	22,45	21,346	15,702	-26%
Общее количество опубликованных потерь, млн.Евро	268	234	265	248	280	13%
Физические атаки, связанные с банкоматами:						
Общее количество опубликованных инцидентов	2,062	1,818	1,92	2,102	1,98	-6%
Общее количество опубликованных потерь, млн.Евро	33	28	19	23	27	17%
Примечание - составлено автором на основе источника [8]						

Кроме скимминга, в число мошенничества с карточками включаются также «приклеивание» карточки к кард-ридеру (англ. trapping, swapping), «проглатывание», подмена значения номинала купюр или страницы авторизации банкомата (англ. jamming), кража личной информаций с помощью рассылки электронных писем (англ. fishing).

Меньше происходят внутренние целевые кибер-атаки, когда информация реквизитов карты присваивается по каналам связи системы. В этот момент мошеннику достаточно взломать систему или происходит разглашение внутренней информации (иногда с задействованными сотрудниками самого банка). Немаловажен профессионализм и компетентность Департамента безопасности (внешняя защита), а также прохождение сертификаций ISO 27000, PCI DSS (внутренняя защита). С целью блокировки другого

программного обеспечения используются следующие решения: «IntrusionProtection», «AccessProtection» компании «WincorNixdorf» и так далее.

Для работы самой простой системы защиты немаловажно ответственное обращение владельца с картой, а именно:

-бумажник не должен являться местом для хранения ПИНкода;

-карточка не должна передаваться в третьи руки;

-фискальный чек в местах торговли должен стать обязательным после совершения операции;

-блокировка карты при утере;

-отправка ПИНкода по электронной почте в открытом виде либо посредством SMS сообщений.

Основной задачей банков, а также компаний, которые отвечают за обеспечение безопасности – создание условии по защите информации клиентов и банковского оборудования.

Вместе с тем, интеграция во Всемирную торговую организацию (ВТО) и Единое экономическое пространство (ЕЭП), имея свои положительные стороны, образует условия предстоящего процесса расширения прав и свободы рынка финансовых услуг. Дальнейшее форсирование конкуренций на финансовом рынке, будет способствовать повышению качества и увеличению видов предлагаемых услуг. А также, необходимо отметить увеличение степени незащищенности отечественного финансового сектора к внешним потрясениям, роста так называемых рисков «заражения», которые при воплощении неудачного сценария развития, могут привести к выводу капитала и средств заемщиков, вкладчиков из коммерческих банков, а также привести к так называемому кредитному сжатию. При возникновении подобных ситуаций финансовой системе лучше не способствовать формированию новых рисков или увеличению диапазона действующих рисков в экономике страны. При данном подходе необходимо выработать наилучшую систему регулирования, при которой результаты воплощения рисков будут сведены к минимуму, а условия не будут чрезмерными и ослабляющими финансовый сектор.

С целью предотвращения мошенничества с банкоматами нами предложено внедрение и развитие новой услуги для клиентов банков Казахстана – внедрение биометрических банкоматов банками второго уровня. К примеру, известный научно-технический журнал IEEE Spectrum содержит статью об использовании систем биометрической идентификации на момент проведения платежей в банкоматах коммерческих банков Японии [9].

На сегодняшний день, благодаря биометрическим системам, около 80 000 банкоматов в Японии имеют возможность быть защищенными от краж. На основе опыта внедрения данных банкоматов сканеров Hitachi и Fujitsu, которые используются с помощью сканирования рисунка кровеносных сосудов руки, крупные банки таких стран как Бразилия, Польша и Турция также обратились к их внедрению. В Европе, по данным Европейской группы по обеспечению безопасности банкоматов, кража из банкомата посредством копирования данных с банковской карточки и иного мошенничества составили 67 миллионов Евро во второй половине 2019 года. Мошенничеств и взломов банкоматов в Соединенных Штатах Америки, где еще преобладает карточка с простой и относительно небезопасной магнитной кодовой полоской намного больше. Точные цифры глобальных потерь невозможно найти, но по данным эксперта отдела безопасности McAfeeRobertSiciliano, по крайней мере 2 млрд долларов США теряется каждый год.

Компании Hitachi и Fujitsu на протяжении нескольких лет работают над проектом коммерческого внедрения биометрических систем - у каждой компании свои методы воплощения проекта, различные подходы просвечивания руки: только пальцев, как сканируют сканеры компании Hitachi или ладони в целом.

Ряд банков Японии отказываются от ПИН кодов, некоторые банки готовы предложить клиентам избавится от банковских карт и вовсе. Подобные достижения толкают к наиболее амбициозным и футуристическим видениям исследователей, когда клиент сможет купить конфеты или рубашку в магазине, с помощью сканирования ладони у датчика. Такая схема сейчас все еще научно-фантастическая, и технические трудности такой биометрической системы будут приостанавливать развитие авторизации карточек. Но факт тот, что инженеры начинают решать эти проблемы и это является еще одним признаком того, что мировое сообщество приближается к еще одной вехе в человеческой культуре: новообразованная степень абстракции в многовековой виртуализации денег. Это не показательная технология, но это плюс. Биометрический модуль легко интегрируется в машину, и клиенты радикально не меняют свое поведение. После того как банковская карточка вставлена, появляется экран строка, чтобы приложить палец в пластиковую впадину, встроенную в банкомат. Инфракрасный свет, расположенный рядом, светит с обеих сторон выреза, а камера ниже записывает полученное изображение вен в пальце, который сравнивается с вашими зарегистрированными данными. Если данные сходятся, то экран отображает подтверждение в течение одной секунды, и клиент может ввести свой PIN-код и продолжить операцию. Банк Киото начал биометрическую программу в 2005 году, и по сей день в нем зарегистрировано около трети его 3000000 клиентов.

Когда-то банк решил присоединиться к биометрической системе, методично сравнивая возможные технологии с точки зрения безопасности, точности и простоты использования. Кроме того, были рассмотрены другие варианты

включая сканеры отпечатков пальцев и голоса, лица и радужной оболочки глаза. Считыватель отпечатков пальцев, возможно, казался очевидным выбором: технология очень зрелая и сканеры отпечатков пальцев дешевы и просты в использовании. Но проблема оказалась в том, что они недостаточно безопасны - отпечатки пальцев легко подделать. Известен печальный случай в Малайзии, когда несколько лет назад банда воров отрезала палец владельцу автомобиля MersedesBenz, где использовалась система отпечатков пальцев для распознавания во время зажигания.

По нашему мнению, распознование по венам более безопаснее и удобнее, несмотря на то, что распознавание по голосу или по лицу являются дешевым и простым способом в использовании: насморк или плохое освещение может повлиять на их точность. Что касается распознавания по радужной оболочке глаза, то, камеры анализируют сложные микроструктуры в этой части глаза. Такие системы являются довольно безопасными и очень точными, но они требуют от пользователей правильного расположения головы и держать свои глаза открытыми. Этот процесс аутентификации является также слишком медленным, так как есть занятые банковские клиенты, которые быстро хотят получить деньги и продолжить день. Проводить сканирование вен намного быстрее и точнее. Нет возможности получить результат от вырванной вены или вырубленной руки.

Системы Hitachi и Fujitsu действуют по одинаковому принципу. Кровь течет по кровеносной системе, которая содержит белок гемоглобина и переносит кислород из легких, оседая в тканях по всему телу. Кровь, которая доставляется в сердце по венам, содержит дезоксигемоглобин, который поглощает свет в ближний инфракрасный диапазон. Остальная часть ткани руки пропускает инфракрасные лучи сквозь, создавая изображение темных линии.

Отличие систем двух компании в том, что сканеры Fujitsu предполагают сканирование ладони целиком, в отличие от сканеров Hitachi, сканирующих пальцы.

В компании Hitachi, эта технология была создана в исследовательской лаборатории компании по диагностической визуализации. Затем ею заинтересовался отдел финансовых услуг Hitachi, где аналитики решили, что это может быть полезным в банковской сфере. Но, изображения, полученные с помощью оборудования медицинской бригады, не были достаточно отчетливы, для надежного опознавания лиц, поэтому они были подвержены компьютерной обработке.

В таблице 3 отражен итоговый результат о необходимости и успешности внедрения технологии в разбивке по органам человека.

Таблица 3

Сравнительный анализ внедрения технологии по органам человека.

	Сетчатка глаза	Голос	Лицо	Отпечатки пальцев	Вены
1	2	3	4	5	6
Легкий в использовании					
Дешевый во внедрении					
Верный результат					
Безопасный					
Примечание - составлено автором на основе источника [10]					

Таблица 2 показала, что распознавание по венам человека, является легким в использовании, дешевым во внедрении и безопасным, с помощью которого можно получить верный результат.

Как подвести итог биометрической системы идентификации: когда дело доходит до точности опознания лица или голоса, то биометрической системы опознания недостаточно. С точки зрения безопасности, система опознания не может быть «обманута» копиями, фотографиями или записями.

В одном из кампусов Центральной научно-исследовательской лаборатории Hitachi, на окраине Токио, главный научный исследователь АкиоНагасака проецировал рисунок серого пальца с изображением вен на экране, указав, что типичных методов изображения фильтрации недостаточно, чтобы извлечь образцы вены. Здесь не используется классический метод как при определении отпечатков пальцев, который в сравнении является крошечным. Обычно используется в анализе отпечатков пальцев, который сравнивает крошечные, отличительные черты в отпечатке (они на самом деле называются "мелочи"). Вместо того, чтобы реагировал рисунок, команда Hitachi разработала метод отслеживания линии [PDF], в которой программа сканирует цифровое изображение для темных пятен, а затем пытается следовать за ними, пиксель за пикселем, чтобы увидеть, образование линии. Когда программа выполняется достаточное количество раз, она выдает картину вен.

Команда работала в миниатюризации оптической системы с датчиком CMOS, который собирает изображения - датчиками нового поколения 15 миллиметров в длину и 10 мм в ширину, размером в ноготок. Другое открытие - это конструкция, излучающая свет по обе стороны пальца, с помощью датчика CMOS. Кроме того, исследования показали, что клиентами идея сбора данных для биометрических опознании не особо положительно воспринята, объясняя, что в случае взлома хакерами этих данных, клиент не способен

будет заменить эти данные в будущем, соответственно обслуживание по счетам в банке будет приостановлено. В связи с чем, компанией Hitachi была разработана система match-on-card, согласно которой банковская карта клиента содержит биометрический шаблон, а изображение, полученное с помощью датчика в банкомате схоже с картой. Компания Fujitsu использует аналогичную систему, поэтому биометрическая информация клиентов всегда под контролем. Если карта украдена, даже самые умелые хакеры не смогут иметь доступ к биометрическим данным. Это потому, что карты настраиваются для принятия входящих данных от датчика банкомата, а не передавать данные во внешнюю среду.

В лаборатории Кавасаки, научным руководителем биометрии создано квадратное устройство. Над выемкой в устройстве необходимо держать руку и при нажатии тремя пальцами светится зеленый, это позволяет крошечному датчику в выемке, собрать данные вен в ладони, в то время как датчики в пластине одновременно собирают отпечатки трех пальцев. Компания Fujitsu представила эту "смешанную" систему в прошлом году.

Такая сложная система не является необходимой в банкоматах, которые в настоящее время используют биометрическую систему распознания вен. Эти системы основаны для проверки на соответствие с одним биометрическим шаблоном, хранящимся на банковской карте пользователя. Но если клиент желает воспользоваться банковской картой и PIN-кодом или использовать биометрическую систему в продуктовом магазине, то клиенту нужна система, которая может сравнить данные клиента с биометрическим шаблоном из программы. Особенность этой системы должна быть быстрота (в течении 1-2 секунды) и точность получения личных биометрических данных, после чего отключиться, чтобы избежать утечки информации.

На сегодняшний день банкомат с функцией сканирования капилляров является дополнением пластиковых карт с PIN-кодом, хотя в ближайшем будущем планируется замена карточек, это значит, что производить оплату можно приставив руку к банкомату. Данная система будет являться полноценной биометрической платежной системой, т.е. новым уровнем абстракций в платежной системе. Подобная система значительно сложнее, по сравнению с её текущей работой, потому как происходит полное распознание личности взамен простой верификации личности. В компании Fujitsu был проведен эксперимент, рассчитанный на 5 млн. пользователей, результатом которого было корректное распознание человека системой за 1,34 секунды в среднем. Скорость получения результата объяснена перенаправлением системой всех данных каждого отпечатка пальцев, вен ладони в одну общую систему распознания. После чего, посредством метода удаления похожих результатов получают нужный эскиз, наряду с действием которого работают 7 серверов лаборатории Fujitsu.

Внедрение технологии - это не единственная задача. Нужно сначала привлечь и банки, и клиентов, к тому, чтобы они доверили свои деньги и биометрические данные этой системе. Все банки, которые приняли биометрические системы, в Турции и Бразилии, и в настоящее время используют эту систему и ушли так далеко, что не прибегают к ПИН-кодам.

OgakiKyoritsuBank, являясь японским банком, в сентябре 2012 года первый на мировом рынке запустил биометрическую платежную систему, которая подразумевала поднесение руки к сканеру, введение PIN-кода и даты рождения без наличия пластиковой карточки достаточным для снятия денег в банкомате. Подобные меры, по ускорению и защищенности платежных процедур, были предприняты японскими банками в связи с природными катастрофами в 2011 году, которые порядка десятка тысяч человек оставили без каких-либо документов и банковских карточек.

Применяемые в Японии сканеры рекомендуют использовать не только в банкоматах, но и в торговых автоматах. К примеру, клиенту, желающему приобрести бутылку минеральной воды в торговом автомате достаточно приложить ладонь в сканер и получить свой выбор [4, с.36-41].

Из европейских банков Банк BPH SA (коммерческий банк Польши) стал первым банком, внедрившим систему распознавания клиентов, которая базируется на биометрическом распознании кровеносных сосудов пальца, произведенных компанией Hitachi, в работе своих банковских отделений.

Как основной метод для подтверждения личности в банковских отделениях банка BPH, расположенных на территории Польши, внедрены биометрические технологии FingerVein с января 2013 года [11].

Биометрическая идентификация клиентов - одна из самых инновационных и современных технологий на рынке банковских услуг.

Помимо технических аспектов, сопряженных с внедрением решения и объединением ИТ - систем в банк BPH SA, важнейшей задачей было подготовить клиентов к работе с данной технологией. На сегодняшний день, клиенты с радостью используют эту технологию и рады упрощению процедуры подтверждения личности, а также удобству, которое дает это решение. Несмотря на сложности при внедрении: недостаток сетевой инфраструктуры, несоответствие ИТ-систем, строгое требование к безопасности главной задачей было создание инновационного биометрического считывателя FingerVien на базе технологии Ethernet, которая бы соответствовала высочайшим стандартам банковской безопасности. При этом была: удобной и простой.

Банк BPH SA стал вторым проектом по внедрению технологии FingerVein, который осуществил вместе с Hitachi. До этого биометрика

была внедрена только в банкоматы и небольшие банки, действующие в корпоративном секторе.

Для выявления экономической эффективности биометрических банкоматов для банков была составлена таблица 4.

Таблица 4

Основные показатели для расчета экономической эффективности внедрения биометрических банкоматов

Первоначальные инвестиции	Текущие доходы банка в месяц	Текущие расходы банка в месяц
1	2	3
Стоимость биометрического банкомата	Доход, получаемый от расчетно-кассового обслуживания предприятий	Расходы на аренду площади, если банкомат находится вне территории банка
Стоимость сервера	Доход, получаемый от предприятий за выпуск пластиковых карточек	Заработная плата сотрудников, обслуживающих биометрические банкоматы
Место администратора в Департаменте карточных продуктов банка	Доход, получаемый от снятия наличности, в т.ч. заработной платы сотрудников предприятий.	Расходы по налогам на заработную плату сотрудников
Площадь, для выдачи наличных денег	Доход от вложения среднедневных остатков на карт-счетах в кредиты	Коммунальные услуги
	Доход, полученный за использование овердрафтов, револьверных кредитов и т.д.	Приобретение наличности
		Начисление процентов на среднедневные остатки на карт-счетах
		Расходы на возможный ремонт
Примечание – составлено автором		

Как видно из таблицы 4, для расчета экономической эффективности автором представлены три составляющие: первоначальные инвестиции, текущие доходы банка от внедрения биметрических банкоматов и текущие расходы банка в месяц. Необходимо отметить, что при внедрении биометрических банкоматов наблюдается сокращение выпуска пластиковых карточек, в связи с наличием данных клиента Банка. Таблица подытожена следующей формулой:

$$Cr = Pi / (Bi - Be) \quad (1)$$

где,

Cr – текущий результат;

Pi – первоначальные инвестиции;

Bi – доходы банка в месяц;

Be – расходы банка в месяц.

Формула составлена из расчета индивидуального применения банками второго уровня. В данном случае, целесообразно отметить идею маржиналистского подхода, состоящую из того, что стоимость товара определена не затратами труда на его производство, а его полезным эффектом, получаемым потребителем. С учетом маржиналистского подхода, потребителем выступает как банк, так и сам клиент.

Исходя из данного подхода, можно сделать вывод, что каждое дополнительное потребление товара, приносит дополнительную полезность, возникающую от прироста размера потребления, который равен единице определенного блага. В посткризисный период, такой подход считаем наиболее объективным при внедрении биометрических банкоматов, причиной которого является потребительское равновесие. Суть потребительского равновесия в выборе одного товара из нескольких при ограниченной сумме денег, при этом все потребители ссылаются на собственное ощущение, с целью максимизировать общую полезность от товаров, которые входят в этот состав. Величина спроса может изменяться в связи с влиянием меняющихся цен на размер реального дохода. Что является эффектом дохода. Размер увеличенной суммы дохода может способствовать установлению дополнительного банкомата, спрос на который будет расти при росте дохода.

Выводы или заключение

Таким образом, инновационные технологии FingerVein способны поднять не только экономику казахстанского банка, но и имидж банка, а также несут в себе огромные перспективы для развития не только банковской сферы, но и экономики в целом.

Несмотря на дороговизну установки биометрического банкомата, полезным эффектом является минимизация мошеннических операций, повышение доверия населения к банкоматам и банкам в целом, минимизация текущих расходов по обслуживанию банкоматов (списание средств, по причине мошенничества), а также развитие платежной системы в экономике.

Внедрение нововведения - биометрического банкомата для развития инновационных технологий в банковской сфере позволит создать конкурентную среду в сфере банковских продуктов

и услуг; сконцентрировать занятость банковских сотрудников во фронт-офисах без отвлечения на консультации, текущего обслуживания клиентов; обеспечить оптимизацию и совершенствование банковских операций; конкурентоспособность банковских продуктов и услуг не только на отечественном, но признание на мировом рынке; **предотвратит мошенничество с банкоматами и увеличит безопасность счетов клиентов**.

Список литературы

1. Technology and Innovation in Financial Services: Scenarios to 2020. World Economic Forum. – Switzerland, 2017. – 87p.

2. Карминский А.М., Жданова О.Р. Современные тенденции банковских инноваций //Маркетинг і менеджмент інновацій. - 2018. - №2. – С.106-118.

3. ИвановаО.В. Классификация банковских инноваций //Вестник ВГУ. серия: Экономика и управление. - 2018. - № 1. - С.163-166.

4. Семикова П. Банковские инноваций и новыйбанковский продукт / П. Семикова // Банковские технологии. - 2015. - № 11.

5. Галат И. 5 банковских технологий, которых пока нет в Казахстане.[Электронный ресурс]. URL:http://vlast.kz/article/5_bankovskih_tehnologij_kotoryh_poka_net_v_kazahstane-6541.html (дата обращения 24.02.2020).

6. ImramziyevaM.Ya. Internet banking development in commercial banks of Kazakhstan //4th International Conference on Science and technology. – London: Sciero, 2020. - P.107-114.

7. Коррупция и мошенничество уничтожают банки Казахстана // [Электронный ресурс]. URL: http://forbes.kz/finances/markets/korruptsiya_i_moshennichestvo_unichtojayut_banki_kazahstana (дата обращения 01.02.2020).

8. European ATM Related Fraud Incidents fall 26%, although Skimming Losses rise. [Электронный ресурс].URL: https://www.european-atm-security.eu/european-atm-related-fraud-incidents-fall-26-although-skimming-losses-rise/ (дата обращения 09.03.2020).

9. Strickland E. Blood and money // Spectrum, IEEE . – 2012. – Vol.49, №6. – P. 36 - 41.

10. Технология FingerVein в Bank BPH. // март 2018.// [Электронный ресурс].URL: http://www.hitachi.ru/март 2018. (дата обращения 01.02.2020).

11. Испанский банк «LaCaixa» представил бесконтактный банкомат. Информационный [Электронный ресурс].URL: http://www.penki.lt/Tekhnologii-i-bezopasnost/Ispanskiy-bank-La-Caixa-predstavil-beskontaktny-bankomat. 11.04.2011. (дата обращения 27.02.2020).

УДК 338.242.2

ОЦЕНКА ЭФФЕКТИВНОСТИ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

[1]Анастасия Юрьевна Селиванова,
[2]Сергей Владимирович Слабинский
[1]Уральский федеральный университет, Екатеринбург, Россия,
[2]Уральский федеральный университет, Екатеринбург, Россия

EVALUATING THE EFFECTIVENESS OF INNOVATION ACTIITIES ENTERPRISES IN THE FIELD OF INFORMATION TECHNOLOGY

[1]Anastasia Yuiryevna Selivanova,
[2]Sergey Vladimirovich Slabinskiy
[1]Ural Federal University, Yekaterinburg, Russia,
[2] Ural Federal University, Yekaterinburg

АННОТАЦИЯ

В статье представлена эволюция терминов «эффект» и «эффективность, рассмотрены подходы к понятию «эффективность инновационной деятельности», изучены их достоинства и недостатки. Представлена авторская трактовка данного термина. Дан анализ отрасли информационных технологий на современном этапе, а также тенденции развития и перспективы. Проведено исследование различных инструментов оценки эффективности инновационной деятельности. Разработана авторская методика оценки, отличительной особенностью которой является использование комплексного системного подхода.

ABSTRACT

The article presents the evolution of the terms "effect" and "efficiency", the article considers approaches to the concept of "innovation efficiency", and examines their advantages and disadvantages. Authors present their interpretation of this term An analysis of the information technology industry at the present stage, as well as development trends and prospects is given. A study of various tools for evaluating the effectiveness of innovation activities was conducted. The author's assessment methodology has been developed, the distinctive feature of which is the use of a comprehensive system approach.