Студенческий Вестник Электронный научно-технический журнал Октябрь 2017 года

ФРОД – МОНИТОРИНГ КАК СРЕДСТВО ЗАЩИТЫ БАНКОВСКИХ ТЕХНОЛОГИЙ

А.В. Носаль, **Л.В.Олехнович**

В статье рассмотрено и предложено для развития в банковской сфере Республики Беларусь новое средство защиты банковских технологий – фрод-мониторинг, которое имеет своей целью исследование всей банковской информации на предмет обнаружения мошеннических действий. На основе реального опыта эксплуатации этого решения, полученного зарубежными банковскими специалистами, данное средство позволит осуществлять мониторинг, выявление и блокировку мошеннических транзакций в режиме реального времени, предотвращая таким образом финансовые и имиджевые потери банка от данного вида преступлений.

Ключевые слова: дистанционное банковское обслуживание, платежные карточки, фрод-мониторинг,

Дистанционное банковское обслуживание позволяет банкам улучшить качество, расширить спектр предлагаемых услуг и географию их предоставления за счет организации удаленной, оперативной, удобной системы обслуживания клиентов, увеличить прибыль, обеспечить высокий уровень конкурентоспособности и повысить инвестиционную привлекательность на финансовом рынке.

На протяжении последнего десятилетия банковские платежные карточки прочно вошли в сферу обращения и в банковском деле карточный бизнес занял лидирующие позиции. Развитие карточной сферы оказывает непосредственное влияние на состояние банковской системы Республики Беларусь [1].

Так, в платежной системе Республики Беларусь в 2016 г. совершено 393,4 млн. платежей на сумму 20 599 млн руб. По сравнению с 2015 г. в 2016 г. количество платежей в платежной системе Республики Беларусь увеличилось на 61 млн единиц, или на 18 %, а сумма возросла на 5 128 млн руб., или на 33 %.

За период 2011–2016 гг. динамика платежного оборота в платежной системе Республики Беларусь представлена в рисунке 1 [1].

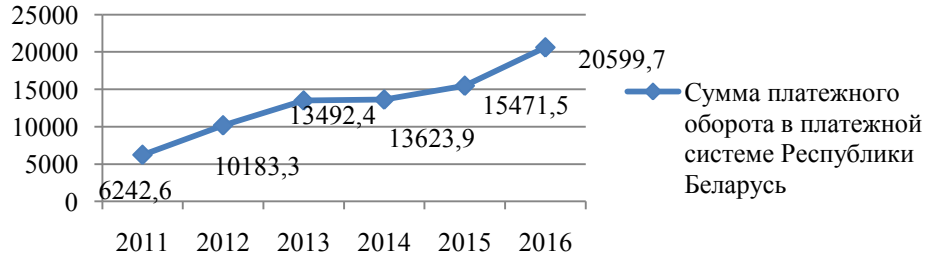

Рис.1. Динамика платежного оборота за 2011– 2016 гг., млн.р

В 2016 г. рост платежного оборота по сумме платежей обусловлен ростом эмиссии банками платежных карточек, количества организаций торговли (сервиса), оснащенных платежными терминалами, платежных терминалов в организациях торговли (сервиса), банкоматов, инфокиосков и увеличением объемов безналичных операций, проведенных с помощью банковских платежных карточек на 114,9 млн. ед., ростом объема платежей, проведенных посредством АИС «Расчет».

Динамику банковских платежных карточек в течении последних шести лет можно проследить на рисунке 2.

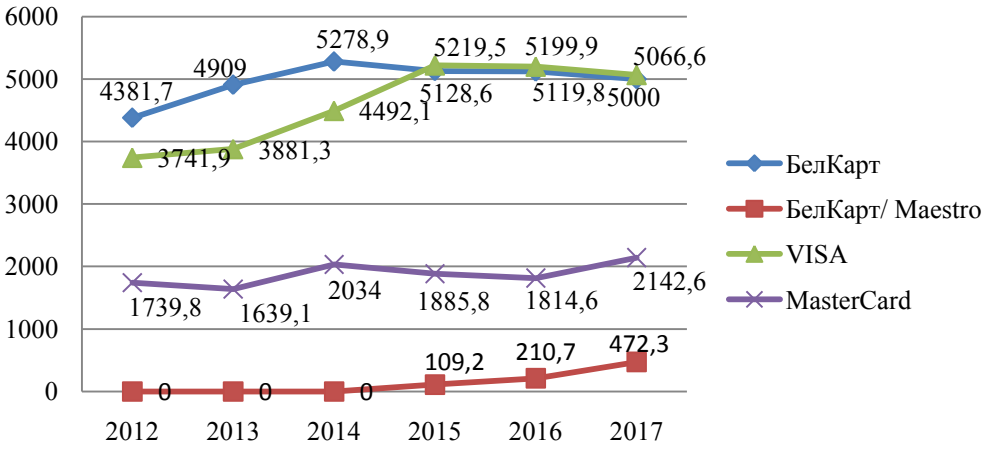

Рис.2. Динамика изменения эмиссии банковских платежных карточек в Республике Беларусь, ед.

Лидером по количеству используемых карточек в Беларуси являются Visa и БЕЛКАРТ (в обращении более 10 млн. ед.). В 2016 году с использованием банковских платежных карточек на территории Беларуси было совершено около 1,1 млрд операций на сумму почти 39 трлн. р [2].

В таблице 1 представлены показатели развития объектов инфраструктуры обслуживания банковских платежных карточек за 2014-2017 гг. [1].

***Таблица* 1. Инфраструктура обслуживания банковских платежных карточек**

Дата	Объекты программно-технической инфраструктуры, ед.				
	количество организаций торговли (сервиса), оснащенных платежными терминалами	платежные терминалы в организациях торговли (сервиса)	платежные терминалы в пунктах выдачи наличных	банкоматы	инфокиоски
01.01.2014	49 539	73 627	7 448	4 088	3 586
01.01.2015	64 764	91 784	7 646	4 362	3 670
01.01.2016	79 107	111 724	7 505	4 414	3 519
01.01.2017	109 380	139 608	7 373	4 386	3 394

За период 2014-2016 гг. обеспечены опережающие темпы прироста количества объектов инфраструктуры по сравнению с темпами прироста эмиссии карточек.

В таблице 2 представлены данные по операциям использования платежных карточек,совершенных на территории Республики Беларусь. [1].

Из представленных данных видно, что наибольший удельный вес по количеству операций принадлежит безналичным платежам: в 2014 г. – 72,0 %, в 2015 г. – 76,4 %, в 2016 г. – 79,8 %. Наличные платежи имеют меньший удельный вес: в 2014 г. – 74,1 %, в 2015 г. – 68,3 %, в 2016 г. – 61,4 %. Однако доля по сумме проведенных операций принадлежит наличным платежам. В целом по состоянию на 01.01.2017 г. было произведено 1 098 943,6 тыс. операций на сумму 38 946,5 млн. руб.

Таблица 2. **Операции с использованием банковских платежных карточек**

Дата	Наличные операции, млн. руб.				Безналичные операции, млн. руб.			
	количество	доля	сумма	доля	количество	доля	сумма	доля
2013	233 119,1	31,6	18715,4	78,5	504 652,7	68,4	5120,2	21,5
2014	231 322,3	28,0	22522,0	74,1	595 708,9	72,0	7856,0	25,9
2015	222 427,2	23,6	23567,1	68,3	719 480,7	76,4	10920,0	31,7
2016	221 579,1	20,2	23918,9	61,4	877 364,6	79,8	15027,5	38,6

С развитием рынка розничных безналичных платежей умножилось и число способов мошенничества с платежными карточками. Махинации с платежными карточками распространяются в основном на кредитные карточки, поскольку при использовании дебетовой карточки всегда проводится авторизация, то есть делается запрос в платежной системе о подтверждении полномочий предъявителя карточки и его финансовых возможностях.

На сегодняшний день из известных видов мошенничеств “лидирует” полная подделка карты. На заготовки полностью подделанных карточек наносятся логотип эмитента, поле для проставления подписи, точно воспроизводятся все степени защиты. В данном случае используются подлинные реквизиты существующих карт.

Другой распространенный вид преступлений – незаконное использование подлинных карточек. Сюда относятся операции с украденной или утерянной карточкой, изготовление продавцом дополнительных копий платежных квитанций, которые в дальнейшем используются для снятия денег со счетов.

Банки вынуждены искать все новые и новые способы борьбы с мошенничеством. Застой в области защиты очень опасен, поэтому технологии защиты необходимо постоянно совершенствовать, а внедрять - быстро и в широких масштабах, это очень непросто. Однако темп роста злоупотреблений по карточкам вынуждает всех участников "карточного" бизнеса решать эту проблему.

Таким образом, преступность в сфере платежных карточек развивается параллельно с самой индустрией карточек. Поэтому необходимо искать пути решения данных проблем и направления успешного развития рынка банковских платежных карточек.

Современные условия экономического развития требуют выстраивания эффективной системы борьбы с мошенничествами в банках. В настоящее время большую популярность приобретает современный механизм контроля банковских технологий – фрод–мониторинг.

Фрод–мониторинг – это обязательная составляющая превентивных мер по борьбе с мошенничествами, причем как с внешней стороны (клиенты, злоумышленники), так и внутри банка. Это мониторинг всей информации, входящей и исходящей, на предмет обнаружения мошеннических действий.

В Европе более половины ведущих банков передают данную функцию на аутсорсинг. Для оценки клиентских запросов на предмет мошенничеств принято обращаться к специализированным компаниям. Во-первых, подобные организации, как правило, консолидируют информацию по нескольким банкам, что позволяет уберечь от опасности тех, на кого атака пока не началась. Во-вторых, специализированные организации имеют в своем штате высококвалифицированных аналитиков, которые по результатам анализа всех данных о мошенничествах делают прогнозы по развитию схем атак и предлагают конкретные меры противодействия. Однако при этом возникают различные риски, работа партнера влияет на бизнес банка. Некачественный сервис может привести к негативным последствиям, вплоть до перерывов в работе. Также проблема банковской тайн является не менее актуальной. Однако практика показывает, что подобный подход эффективен. В

России пока все банки выстраивают свою систему фрод–мониторинга, независимо от того, осуществляют внедрение самостоятельно, силами ИТ и службы безопасности, либо силами квалифицированных специалистов вендора или его российского партнера [3].

Общая схема работы практически любого механизма фрод–мониторинга представлена на рисунке 3.

«Зеленая» метка отмечает транзакции с низкой вероятностью возникновения мошеннической операции. «Желтой» меткой отмечаются транзакции, в которых шанс возникновения мошеннической операции выше среднего, и для проведения платежа потребуются дополнительного внимания. «Красной» отмечаются транзакции, которые с наибольшей вероятностью могут оказаться мошенническими, и при их проведении потребуется документальное подтверждение аутентичности владельца карты[3].

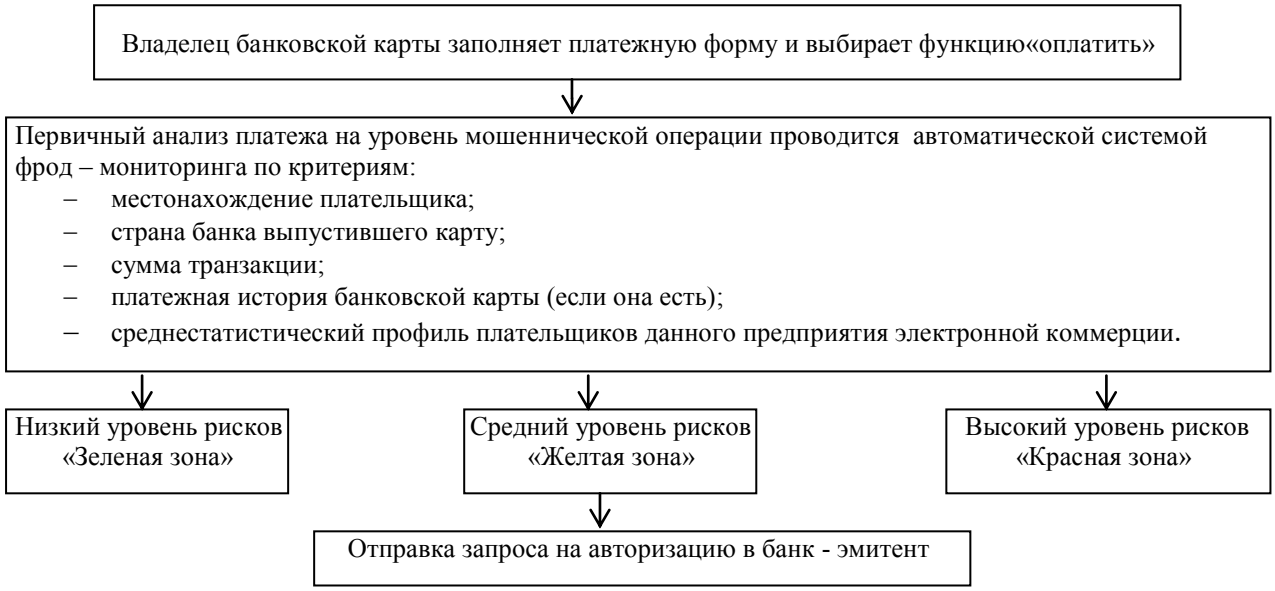

Рис. 3. Архитектура модуля фрод – мониторинга

Банки уделяют особое внимание совершенствованию систем обеспечения безопасности в сегменте защиты средств клиентов от противоправных посягательств, совершаемых с использованием банковских карт, терминального оборудования и других средств электронного бизнеса.

В целях реализации эффективных мер защиты от противоправных посягательств на денежные средства банка и клиентов, необходимы :

- построение эффективной системы защиты банка и клиентов от киберугроз на основе внедрения процесса «Противодействие внешнему и внутреннему мошенничеству»
- внедрение систем фрод-мониторинга в различных сегментах банковской деятельности.

Внедрение решения фрод-мониторинга несет в себе определенные трудности, и первая из них – это интеграция с различными системами внутри банка, ведь такое решение влияет на действия всех сотрудников банка.

Большинство банков уже осознали необходимость создания подобных систем по борьбе с мошенничествами. Но технической и технологической подготовки к внедрению этой формы контроля пока нет. Большинство автоматизированных банковских систем не имеет необходимой информации и необходимых инструментов для интеграции с системой фрод-мониторинга. Дистанционные каналы банковского обслуживания требуют доработки, они не могут качественно предоставить информацию об источнике сообщения

– используемом рабочем месте клиента, самом клиенте . Во многих банках до сих пор нет качественно работающей системы риск-менеджмента, которая бы могла переводить риски в деньги. Некоторым проще использовать варианты страхования убытков, чем бороться с рисками превентивными методами.

Сервисная поддержка фрод-мониторингу нужна точно так же, как и любой автоматизированной системе, как и любому программному обеспечению. Это банки частично могут делать собственными силами, даже если решение внедрено специализированной компанией. Немаловажным является оперативное реагирование на изменения и актуализация данных. Фрод-мониторинг должен быть постоянно обучающейся системой. В данном случае банку предстоит решить, может ли он это делать самостоятельно, либо ему потребуется помощь вендора или партнера. В редких случаях службы безопасности сами могут контролировать «рынок мошенничества», поскольку это требует больших затрат рабочего времени. Например, есть ресурсы, где хакеры вывешивают данные о взломе систем, раскрытых счетах клиентов, и др. Система фрод-мониторинга должна быть постоянно в таком состоянии, чтобы она могла противодействовать атакам со стороны мошенников [5].

Литература

1. Статистические данные // Официальный сайт Национального банка Республики Беларусь [Электронный ресурс]. – 2017. – Режим доступа: http:// www.nbrb.by.– Дата доступа: 30.09.2017.

2.Официальный сайт Белорусского телеграфного агентства [Электронный ресурс]. –2017. – Режим доступа: http://www.belta.by.– Дата доступа: 30.09.2017.

3. *Митричев И.* Фрод-мониторинг меняет процесс обслуживания клиентов в банке, к этому надо быть готовым / *И. Митричев* / [Электронный ресурс].– 2012. –Режим доступа: http://bankir.ru.– Дата доступа: 30.09.2017.

4. *Голенищев А.* Система фрод-мониторинга глазами банка. / *А. Голенищев* // Банковская розница. – 2009.– № 8 с. 35-40.

5.*Голенищев, А.* О клиентоориентированном фрод-мониторинге / *А. Голенищев* / [Электронный ресурс].– 2017. –Режим доступа: https://bosfera.ru.– Дата доступа: 30.09.2017.

Носаль Анастасия Валерьевна
Студентка экономического факультета группы ФК-141
Белорусско-Российский университет, г. Могилев
Тел.: +375(29)241-05-21.
E-mail: anastasiya_nosal@mail.ru
Олехнович Лариса Владимировна
Старший преподаватель кафедры «Финансы и бухгалтерский учет»
Белорусско-Российский университет, г. Могилев
Тел.: +375(29) 745-86-50
E-mail: larisa.olekhnovitch@yandex.ru