Однако на ряду с достоинствами инвестирования в фонды банковского управления следует помнить о рисках, связанных с отсутствием гарантированной доходности и, как следствие, невозможностью точно спрогнозировать результаты инвестирования; невысокая транспарентность по сравнению с паевыми инвестиционными фондами.

Таким образом, несмотря на наличие на финансовом рынке Республики Беларусь традиционных видов финансовых инструментов вложения средств, все большую финансовую привлекательность приобретают новые финансовые институты и способы умножения капитала, к таким институтам относят и фонды банковского управления. На данный момент функционирование фондов банковского управления в Республике Беларусь приостановлено. Зарубежный опыт свидетельствует, что фонды банковского управления приобретают все большую привлекательность по сравнению с другими институтами коллективных инвестиций. Преимуществами фондов банковского управления являются их высокая надежность, ликвидность, доходность, широкий выбор финансовых инструментов для инвестирования; недостатками – риски, связанные с отсутствием гарантированной доходности и низкой транспарентностью.

Литература:

1. О проведении эксперимента по созданию фондов банковского управления: Указ Президента Респ. Беларусь, 3 марта 2010 г., № 131 // Консультант Плюс: Беларусь [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2014. – Дата доступа: 07.05.2014.

2. Профиль рынка ОФБУ // Информационный портал Investfands.ru [Электронный ресурс]. – 2014. Режим доступа: http://pif.investfunds.ru/analitics/ofbu. – Дата доступа: 07.05.2014.

***Т.Ю. Равинская***
*ЗАО «Дельта Банк»*
*(Республика Беларусь, Минск)*

## МОШЕННИЧЕСТВО И ГРАММОТНОСТЬ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ПЛАТЕЖНЫХ ИНСТРУМЕНТОВ

В решение вопросов безопасности платежей вовлечены тысячи людей, обсуждаются на многочисленных конференциях, в сотнях периодических и интернет изданий по всему миру, принимаются законопроекты, постоянно совершенствуется IT инфраструктура и вместе с тем, тема неисчерпаема, каждый новый шаг в развитии экономики, госу-

дарства, общества, международных отношений влечет за собой хотя бы одно «но», и это «но» — информационная безопасность, безопасность в сфере платежных инструментов и как следствие возникает потребность в выработке направлений и механизмов противодействия угрозам при использовании платежных инструментов.

Наиболее распространенные угрозы можно сгруппировать следующим образом: банкоматное мошенничество; мошенничество в торговых точках с целью компрометации карт; создание фиктивных торговых точек для совершения операций по поддельным картам; интернет-мошенничество: электронная коммерция, платежи, пополнение счетов, переводы с карты на карту и др.; мошенничество в системах дистанционного банковского обслуживания; фальшивые кредитовые (возвратные/refund) операции; проникновение (взлом) процессиновых и датацентров: кража данных по картам, кража персональных данных, манипулирование лимитами и блокировками и др.; подмена СИМ-карт и другие виды мошенничества с мобильными приложениями; подлимитные мошеннические операции; БИН-атаки; социальная инженерия.

При этом наиболее визуально восприимчивый вид мошенничества – это мошенничество при использовании банкоматов: скимминг; захват карты, наличных; вредоносное программное обеспечение; взломы, ограбления, взрывы, кража банкоматов; поддельные банкоматы; социальная инженерия (phishing, vishing).

Во-первых, очередь безопасность платежей при использовании платежных карт (реквизитов) обеспечивается регулированием на республиканском уровне: Указ Президента от 23.09.2010г. №485 об утверждении Государственной программы по борьбе с преступностью и коррупцией на 2010-2012г.; Межведомственная рабочая группа по противодействию мошенничеству в области электронных платежей (распоряжение Председателя Правления Национального банка Республики Беларусь (далее – НБ РБ) от 31.12.2010г. №1056); План совместных действий государственных органов и участников финансового рынка по развитию в Республике Беларусь (далее – РБ) системы безналичных расчетов по розничным платежам с использованием современных электронных платежных инструментов и средств платежа на 2013-2015гг. (Постановление Совета Министров РБ и НБ РБ от 01.04.2013г. от №246/4); Подкомитет «Платежные карты, электронные деньги и иные инструментарии» комитета по безналичным расчетам (распоряжение Председателя Правления НБ РБ от 15.04.2013г.№140); 19.02.2014 Постановлением Правления НБ РБ от № 92, приняты рекомендации в соответствии с которыми, Банкам необходимо возмещать денежные средства клиента в случае отсутствия информации о нарушении держателями платежных карточек порядка их

использования и (или) мошенничестве с их стороны (принцип «нулевой ответственности).

Во-вторых, банки (эмитенты и эквайеры платежных карт) применяют большое количество организационно-технических мер для обеспечения безопасности платежей, а именно: микроплатежи; геоблокирование карт, либо установления лимитов, на отдельные страны и регионы; системы мониторинга операций (on-line, off-line); использование лучших практик, технических решений и рекомендации экспертного сообщества; завершение перехода на EMV (чиповые) технологии; методики оценки рисков использования электронных средств платежа (карт) и внедрение их во внутренние политики безопасности; обучение персонала и держателей карт правилам безопасного использования электронных средств платежа; осуществление внутреннего контроля за соблюдением внедряемых технических и административных решений; совершенствование механизмов межбанковского взаимодействия с целью противодействия мошенничеству, выявления точек компрометации карт и новых схем мошенничества (форум безопасности АРЧЕ; National Merchant Alert Service (NMAS), European Fraud Sharing Group (EFSG); InterBank Exchange (IBE) и др.)

В-третьих, необходимые достаточные меры безопасности при осуществлении операций при использовании платежных карт требуется применять и держателям карт, а именно: не передавать карточку другому лицу; не оставляйте карточку в тех местах, где информация о карточке может быть доступна посторонним лицам; не сообщать конфиденциальные данные карты; хранить карточку отдельно от ПИН-кода, наличных и документов; использовать услугу SMS-оповещения; перед проведением операции в банкомате (инфокиоске) осматривать его на наличие подозрительных предметов; не упускать карточку из поля зрения при проведении операций в магазинах, ресторанах, гостиницах и т.п. Немаловажно выполнение простых рекомендаций при совершении операций с сети Internet: убедиться в подлинности Web-сайта перед вводом платежных реквизитов: в рамке окна браузера должен быть значок в виде замка; Web-адрес должен начинаться с https://; web-адрес или имя владельца закрашено зеленым; использовать специально открытую карту для расчетов в Internet; выбирать крупные и хорошо известные, проверенные сайты; не использовать ПИН при заказе товаров и услуг через Internet или по телефону; не возвращать денежные средства на свою платежную карту с незащищенного сайта.

Для эффективного обеспечения безопасности при использовании платежных инструментов требуется единая сбалансированная политика, как государства, так и всех участников рынка безналичных платежей.