Таким образом, использование Интернет-банкинга является перспективным инновационным направлением развития банковского обслуживания в Республике Беларусь.

Литература:

1. Саксельцева Е.Г. Возможности применения зарубежных банковских технологий безналичных расчетов в российской практике //Расчеты и операционная работа в коммерческом банке, 2006 г. №1. с. 33-45

2. Оакли А. Белорусские банки объединяют пространства интернет-банкинга //Компьютерные вести [Электронный ресурс] - №32, 2007. - Режим доступа: http://kv.by/index2007322101.htm

3. Бурмусь А. Эпистолярная связь //Дело. 2007 г. N9. с. 24-26.

Ганкевич С.Л., Ших Т.В.

БГЭУ, ФФБД, группа ДФК-3, 4 курс

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ

Банковская карта, как известно, инструмент безналичных расчетов, предназначенный для совершения физическими лицами, в том числе уполномоченными юридическими лицами, операций с денежными средствами, находящимися у банка-эмитента. Если злоумышленник получает саму карту, ее данные или реквизиты, подделывает ее, то он имеет возможность совершать мошеннические операции со счетом в банке, средством доступа к которому является данная карта.

Мошенническая операция — это операция с использованием банковской карты или ее реквизитов, не инициированная или не подтвержденная ее держателем.

Классификация видов мошенничества: утерянные и украденные карты; неполученные карты; поддельные карты; карта не присутствует;

несанкционированное использование персональных данных держателя карты и информации по счету; другие виды мошенничества.[2]

Основными способами компрометации банковской карты являются: скимминг — несанкционированное считывание и сохранение данных с магнитной полосы карты; фишинг — получение у держателя карты информации о реквизитах карты и (или) ПИН-коде путем обмана; установка специальных технических средств на терминальные устройства с целью фиксирования вводимого держателем карты ПИН-кода; подглядывание реквизитов карты и (или) ПИН-кода злоумышленником; разглашение информации со стороны работников банка.[1]

Международные платежные системы (МПС) Visa и MasterCard приняли стандарты мониторинга транзакций для обеспечения контроля рисков, связанных с мошенничеством: Visa regional operation regulations (Май 2007); MasterCard security rules and procedures (Январь 2006). Эти стандарты предусматривают контроль авторизационных и клиринговых транзакций. Для обеспечения безопасности МПС созданы специальные программы.[2]

В 2004 г. был разработан единый набор требований к безопасности данных — Payment Card Industry Data Security Standard (PCI DSS), который включал требования ряда программ по безопасности таких платежных систем, как VISA, MasterCard, American Express, JCB. Стандарт PCI DSS v1.1 определяет требования безопасности для защиты информации, относящейся к платежной карте, и должен использоваться тогда, когда номер карты хранится, обрабатывается или передается. Стандарт устанавливает требования по следующим шести категориям: построение и обеспечение безопасности сети; защита данных о держателях карт; обеспечение программы менеджмента уязвимостей; реализация строгих механизмов контроля доступа; регулярный мониторинг и тестирование сетей; обеспечение политики информационной безопасности.[3]

В РБ опыта предотвращения мошенничества пока мало. Принимаемые меры противодействия все еще носят разрозненный характер и не

применяются повсеместно. Нескоординированные шаги по борьбе с мошенничеством могут дать лишь временный результат. Решить проблему можно только комплексно. Значительная роль в деле обеспечения безопасности банковских карт принадлежит соответствующим службам платежных систем.

Литература

1. Безмалый В. Мошенничество в Интернете.//Компьютер Пресс №10, 2009, с 52-55.

2. Платежные карты. Бизнес-энциклопедия. – М.: Маркет ДС, 2008. – 760 с.

3. Рудакова О.С. Банковские электронные услуги: Учеб. пос., 2009. – 400 с.

Демидюк О.В., Римицан А.А.
БГЭУ, ФФБД, группа ДФК-3, 4 курс

РАДИОЧАСТОТНАЯ ИДЕНТИФИКАЦИЯ ТОВАРОВ КАК АЛЬТЕРНАТИВА ШТРИХОВОМУ КОДИРОВАНИЮ

Современная система идентификации объектов должна соответствовать уровню развития информационных технологий и минимизировать риск человеческого фактора. Сегодня ускорение идентификации товаров требуется везде. Появившаяся в конце прошлого века технология штрихового кодирования уже не в состоянии решить проблему быстрой и надежной идентификации. Технология штрих-кодирования имеет достаточную информативность, низкую стоимость, простоту, эффективность. Но при этом обладает и рядом недостатков: этикетки штрих-кода недолговечны, считываются при определенных условиях видимости, чувствительны к внешней среде. Также мала скорость считывания.

Высокий уровень скорости идентификации товаров происходит, когда на каждой единице груза размещается значительное количество информации, которая может самостоятельно, по запросу или без него, передаваться в