4. Обеспечивать обработку и хранение больших объемов данных.

5. Обеспечивать обмен данными с удаленными подразделениями.

6. Предоставлять знакомые пользователям инструменты ввода бюджетных данных.

7. Обеспечивать ведение управленческого учета.

8. Обеспечивать разграничение прав доступа пользователей к данным и поддерживать регламент согласования и утверждения бюджетов.

9. Предоставлять инструменты для создания разнообразных аналитических отчетов. Бюджет по своей природе многомерен и анализируются доходы и расходы в разных разрезах: по центрам финансовой ответственности, видам деятельности, статьям бюджетов, проектам, продуктам и т. д. Не менее важно получение консолидированных отчетов и показателей. Аналитические отчеты должны поступать к руководству корпорации и филиалов оперативно, и желательно, чтобы пользователь мог их создавать, менять и т. д. самостоятельно, без программирования, чтобы не загружать IT-службу [2].

Таким образом, внедрение бюджетирования позволит оптимизировать финансовые ресурсы, поскольку предварительное планирование, анализ планов, просчет рисков, связанных с их реализацией, последующий контроль отклонений, анализ причин, вызвавших эти отклонения, а также влияние их на будущее приведет к минимизации затрат и увеличению прибыли.

Литература

1. Бюджетирование: шаг за шагом / Е. Ю. Добровольский [и др.]. – М. : Питер, 2009. – С. 448.
2. Iteam.ru – технологии корпоративного управления. – Режим доступа: http://iteam.ru.

НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Е. В. Чувашева, В. В. Костусева, В. Н. Агеева

Белорусский национальный технический университет, г. Минск

Научный руководитель Н. Н. Иванова

Платежные системы являются основой банковской и финансовой экономики. Практически любая финансовая операция приводит к осуществлению платежей и использованию платежных систем. В последние годы значимость платежных систем и контроля связанных с ними рисков резко возросла в результате существенного увеличения объемов банковских сделок на рынках валюты, финансов и ценных бумаг. Платежные системы также претерпели значительные технические усовершенствования и их оперативность возросла. Управление такими системами требует более высокого уровня квалификации, а также готовности к сбоям в них.

Наличие в стране платежной системы, которая удовлетворяла бы потребностям банков и их клиентов в безопасном обращении денежными средствами, является важным вопросом экономики любой страны. Платежные системы, которые функционируют должным образом, повышают финансовую стабильность и снижают стоимость расчетных операций, обеспечивают эффективное использование денежных ресурсов.

Существующая в настоящее время в Республике Беларусь платежная система обеспечивает потребности реального сектора экономики, банков и других финансовых институтов в своевременном и качественном проведении расчетов. Она сформировалась в конце 90-х гг., что позволило в полной мере использовать накопленный опыт других стран и учесть обязательные для ее успешного функционирования требования и принципы (рис. 1).

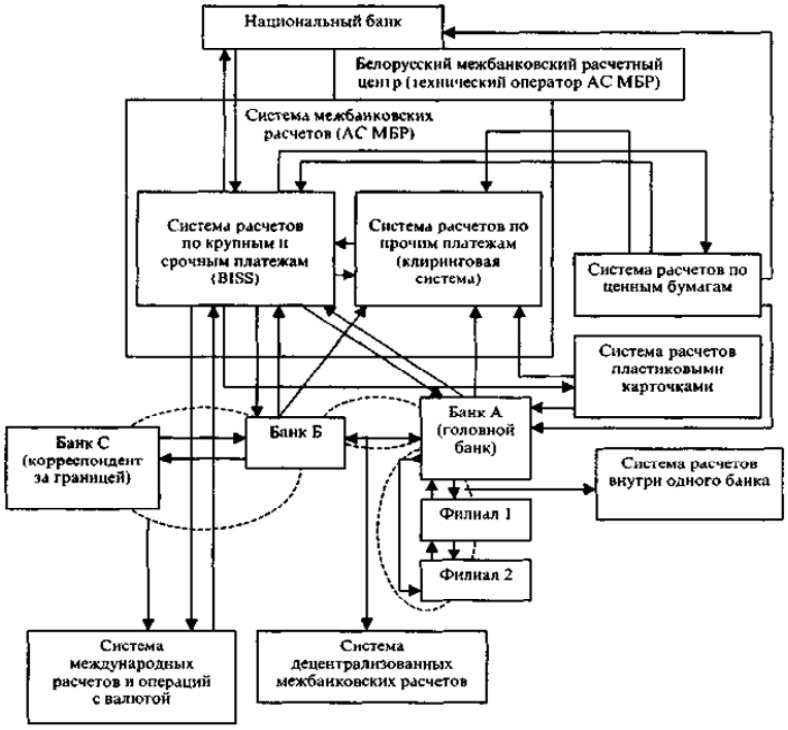

Рис. 1. Схема функционирования платежной системы Республики Беларусь

Платежная система Республики Беларусь регулируется двухъярусной законодательной структурой. Первый ярус включает в себя законодательные акты органов государственной власти, которые определяют порядок проведения межбанковских расчетов, а также определение порядка форм безналичного расчета. Второй ярус структуры, регулирующей платежи, охватывают нормативные документы, принятые Национальным банком в соответствии с Банковским кодексом Республики Беларусь от 25 октября 2000 г. № 441-З.

Кроме того, платежная система Республики Беларусь регулируется требованиями и положениями технических нормативных правовых актов. В 2009 г. принят технический регламент ТР 2008/009/BY «Банковская деятельность. Информационные технологии. Информационная совместимость программных и программно-технических средств платежной системы». Данный документ устанавливает требования к информационной совместимости программных и программно-технических средств, обеспечивающих взаимодействие участников платежной системы при выполнении банковских операций, в целях защиты имущества этих участников и предупреждения действий, вводящих в заблуждение пользователей относительно качества программных и программно-технических средств.

В ходе анализа действующих на территории Республики Беларусь НД и ТНПА было идентифицировано 18 технических кодексов установившейся практики и 10 государственных стандартов в области платежных систем и их безопасности. На международном уровне было выявлено 46 нормативных документа, в их числе стандарты 3-D Secure, PCI DSS и PA-DSS. Наиболее распространенным является стандарт PCI DSS, содержащий 12 обязательных требований безопасности, разработанных для защиты данных держателей карт (далее – ДДК). Данный стандарт применяется для всех организаций сферы обработки платежных данных: торгово-сервисных предприятий, процессинговых центров, банков-эквайеров, организаций, выпускающих платежные карты,

и поставщиков услуг, а также других организаций, которые хранят, обрабатывают или передают данные держателей карт и критичные аутентификационные данные.

Стандарт объединяет в себе требования ряда программ международных платежных систем по защите информации, в частности:

– Visa в Европе – Account Information Security (AIS);

– Visa в США – Cardholder Information Security (CISP);

– MasterCard – Site Data Protection (SDP).

В зависимости от числа обрабатываемых транзакций в год компании присваивается определенный уровень с соответствующим набором требований. Минимальный набор требований стандарта может быть расширен дополнительными регулирующими механизмами и методами сокращения рисков, а также требованиями национального законодательства. Кроме того, в соответствии с законодательством или нормативными требованиями может требоваться особая защита данных, идентифицирующих личность, или других элементов данных. PCI DSS не заменяет собой законы, правительственные распоряжения или иные требования законодательства.

Требования стандарта PCI DSS:

1. Установка и поддержка конфигураций межсетевых экранов для защиты ДДК.

2. Запрет на использование паролей к системам и других параметров безопасности по умолчанию, заданных производителем.

3. Защита хранимых ДДК.

4. Шифровка ДДК при передаче через сети общего пользования.

5. Защита всех систем от вредоносного ПО и регулярное обновление антивирусного ПО или программ.

6. Разработка и поддержка безопасных систем и приложений.

7. Ограничение доступа к ДДК в соответствии со служебной необходимостью.

8. Идентификация и аутентификация доступа к системным компонентам.

9. Ограничение физического доступа к ДДК.

10. Отслеживание и ведение мониторинга всего доступа к сетевым ресурсам и ДДК.

11. Регулярное тестирование систем и процессов безопасности.

12. Поддержка политики информационной безопасности.

Требования этого стандарта должны быть строго выполнены в процессинговых центрах, где обрабатываются данные платежных карт, и рекомендуются к выполнению банкам-эмитентам, выпускающим пластиковые карты.

Процесс внедрения PCI DSS подразделяется на следующие этапы: анализ исходного уровня соответствия; приведение к требуемому уровню соответствия; подтверждение соответствия; поддержка соответствия.

Процедуры подтверждения соответствия стандарту включают в себя ежегодное прохождение аудита, ежеквартальное сканирование сети на уязвимости и в некоторых случаях − заполнение листа самооценки (Self Assessment Questionauire). Для выполнения аудита и ежеквартальных сканирований своих сетей компании должны привлекать стороннюю организацию, имеющую статус Qualified Security Assessor (для аудита) и Approved Scanning Vendor (для сканирования сети). Данные статусы присваиваются советом PCI Security Standards Council. Для получения сертификата соответствия PCI DSS компания должна подготовить информационную систему, которая обрабатывает и хранит ДДК, к соответствию требованиям стандарта и пройти сертификационный аудит. Прохождение сертификации целесообразно разбить на два этапа.

На первом этапе проводится предварительный аудит, в рамках которого выявляются уязвимости информационной системы компании, вырабатываются рекомен-

дации по повышению текущего уровня защищенности информационной системы. Дополнительно должен быть проведен тест на проникновение, обязательный в соответствии с требованиями стандарта PCI DSS.

На втором этапе, после выявления всех несоответствий и их устранения согласно предоставленным рекомендациям, проводится итоговый сертификационный аудит. После проведения сертификационного аудита QSA аудиторы предоставляют отчеты в соответствующий орган по сертификации, который принимает решение о выдаче сертификата.

Стандарт PCI DSS предписывает ежегодное проведения теста на проникновение, причем под тестом на проникновение понимается проведение атак на сетевом уровне и уровне приложений на все публично доступные сервисы компании, а также «war-dialing» для проверки наличия возможности проникновения в корпоративную сеть компании по коммутируемым каналам связи. Тест на проникновение не ограничивается сканированием различными сканерами безопасности – это отдельно подчеркивается специалистами PCI SSC.

В Республике Беларусь сертификат соответствия требованиям PCI DSS впервые получен организацией «Приорбанк». В настоящее время данный сертификат имеют также организации «Белвнешэкономбанк», «Белгазпромбанк» и платежный сервис «Деньги Mail.Ru». Повсеместный переход от наличных денежных средств к безналичным расчетам обуславливает повышенный интерес финансовых организаций к внедрению системы менеджмента на соответствие стандарту PCI DSS. Получение сертификата соответствия стандарту PCI DSS гарантирует не только стремление организаций поддерживать высокий уровень безопасности для потребителей их услуг, но и дополнительные репутационные преимущества, заключающиеся в повышении доверия со стороны клиентов, партнеров и контрагентов.

ОБОСНОВАНИЕ ТЕХНИЧЕСКОЙ И ХОЗЯЙСТВЕННОЙ НЕОБХОДИМОСТИ РЕКОНСТРУКЦИИ ЖЕЛЕЗНОДОРОЖНЫХ СТАНЦИЙ

Е. Н. Шумская

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Республика Беларусь

Научный руководитель Л. М. Лапицкая

Железнодорожный транспорт является сложной производственно-экономической и социальной системой со своей внутренней, только ей присущей территориально-производственной и функциональной структурой. Главной задачей экономики железнодорожного транспорта является развитие в современных условиях теоретических основ изменения качества и методологии управления качеством и эффективностью транспортного производства. Развитие и согласование в условиях рыночной экономики взаимоувязанных функций и методов управления качеством транспортного производства должно быть направлено на выявление и использование резервов улучшения качества и повышения эффективности транспортного производства, разработку методов экономической оценки и стимулирования (мотивации) повышения качества транспортного производства [1, с. 78].

Научный потенциал отрасли, привлекаемых научных организаций стоит сконцентрировать на работах, входящих в следующие наиболее приоритетные направления: развитие ресурсосберегающих технологий; повышение доходов; развитие