щено законодательством и влечет административную, а в установленных случаях и уголовную ответственность. Важно отметить, что несоблюдение законодательства о лицензировании, лицензионных требований и условий являются нарушением и влекут за собой приостановление, прекращение действия лицензии.

УДК 389.1

НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Гиль Н.Н., Чувашева Е.В., Костусева В.В.
Белорусский национальный технический университет
Минск, Республика Беларусь

Наличие платежной системы, удовлетворяющей потребностям банков и их клиентов в безопасном и эффективном переводе денежных средств, является важным элементом экономики любой страны. Должным образом функционирующие платежные системы повышают финансовую стабильность, снижают стоимость расчетных операций, обеспечивают эффективное использование денежных ресурсов, повышают ликвидность финансовых рынков и способствуют проведению монетарной политики.

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 годов, что позволило в полной мере использовать накопленный опыт других стран и учесть обязательные для ее успешного функционирования требования и принципы (рисунок 1).

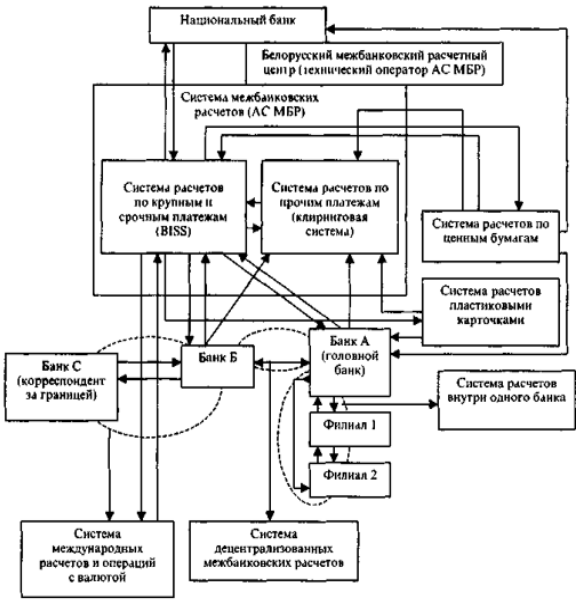

Рисунок 1 – Схема функционирования платежной системы Республики Беларусь

Платежная система Республики Беларусь регулируется двухъярусной законодательной структурой. Первый ярус включает в себя законода-тельные 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 году 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 обра-

ботки 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 тран-закций 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, выпускающими пластиковые карты.

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 рекомендации 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 «Белвнешэкономбанк», «Белгазпромбанк» и платежный сервис Деньги Mail.Ru. Повсеместный переход от наличных денежных средств к безналичным расчетам обу-

славливает 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, партнёров и контрагентов.

УДК 624.014:620.179.16

К ВОПРОСАМ ИССЛЕДОВАНИЯ НАПРЯЖЕНИЙ В НЕСУЩИХ ЭЛЕМЕНТАХ ПРОМЫШЛЕННЫХ СООРУЖЕНИЙ

Демченко М.А., Филиппова М.В.
Национальный технический университет Украины «Киевский политехнический институт»
Киев, Украина

В современном строительстве используется новейшие технологии, которые требуют все большего использования металлических и бетонных конструкций в промышленных сооружениях, срок эксплуатации, которых закладывается проектной группой, и не превышает 20-25 лет. Поэтому, существует необходимость всесторонней диагностики данных сооружений с целью выявления и устранения возможных дефектов в процессе эксплуатации. Процессу разрушения конструкции характерны определенные условия его возникновения, а именно локализация зон напряжения на отдельных участках конструкционных элементов [1,2]. Причина возникновения таких зон может быть различной, начиная от дефектов материала, из которого изготовлены элементы конструкции, в результате механической обработки - формирование элементов конструкций и заканчивая невыполнение условий эксплуатации, указанных в технической документации.

Среди всех конструктивных элементов комплекса промышленного сооружения наибольшему воздействию нагрузки подвергаются межэтажные перекрытия, перекрытия потолка, те что имеют пролет между опорными элементами. Именно в точках наибольшего прогиба происходит концентрация напряжений, как растяжения, так и сжатия, о чем свидетельствует конструкция балочных элементов. Увеличение напряжения в других зонах элемента в сочетании с дефектность металла образуется новые концентраторы напряжения.

Дефект в материале конструкционного элемента может возникнуть в любой момент его жизненного цикла. С этой целью проводится входной контроль металлопродукции. Качество поверхности металла проверяют на соответствие требованиям нормативной технической документации на поставку визуально без применения увеличительных приборов. Рекомендуемый объем контроля составляет 5% от партии. В некоторых случаях контролю поверхности подвергают 100% продукции.

Дефекты стальных конструкций и их соединений возникают в результате ошибок проекта, низкого качества стали и металлопроката, неудовлетворительного контроля при изготовлении, низкого качества монтажных работ и неправильной эксплуатации.

Методы контроля напряженно-деформированного состояния металлических конструкций разделяются на такие 3 группы:

– визуально-оптический и измерительный контроль (ГОСТ 23479-79 «Контроль неразрушающий. Методы оптического вида»);

– механический метод прямого и косвенного контроля;

– неразрушающие методы контроля.

Визуально-оптический и измерительный контроль основан на получении первичной информации о контролируемом объекте при визуальном наблюдении или с помощью оптических приборов и средств измерений. Внешний осмотр позволяет проверить качество выполнения швов в процессе сварки и качество готовых сварных соединений. Как правило, внешним осмотром контролируют все сварные изделия независимо от применения других видов контроля. Визуальный контроль во многих случаях достаточно информативен и является наиболее дешевым и оперативным методом контроля.

Визуальный метод контроля позволяет обнаруживать неоднородности, отклонения размера и формы от заданных более 0,1 мм при использовании приборов с увеличением до 10х. Этот метод напрямую указывают наличие зон концентрации напряжений, в дальнейшем могут привести к разрушению.

Механический метод прямого и косвенного контроля. Косвенные методы обычно дают возможность только качественно оценить напряжен-