

"Лучше меньше, да лучше" или практика выделения области аудита PCI DSS

22.01.2010

Статья посвящена тому, как определить границы области аудита, чтобы в будущем избежать трудноразрешимых проблем в процессе подготовки к сертификации.

Сергей Шустиков, руководитель направления менеджмента ИБ компании Digital Security, PCI QSA

Область соответствия и область аудита

Практика показывает, что у компаний, решивших привести свои информационные системы в соответствие требованиям стандарта PCI DSS, возникает большое количество вопросов относительно определения области аудита. Основной вопрос заключается в том, какие из информационных систем, входящих в информационную инфраструктуру компании, необходимо приводить в соответствие стандарту.

Для начала следует сказать, что есть разница между тем, какие системы должны соответствовать стандарту PCI DSS и тем, какие системы подлежат проверке в ходе QSA-аудита. Эти области не всегда совпадают.

Любая система, хранящая, обрабатывающая, либо передающая данные о держателях карт, должна соответствовать требованиям стандарта PCI DSS. Пусть даже если это PAN одной единственной карты. Эту область назовём термином «область соответствия».

Что касается области, подлежащей проверке на соответствие требованиям стандарта в ходе QSA-аудита, то для большинства организаций она совпадает с изолированной областью соответствия (средой данных о держателях карт, CDE). Назовём множество систем, подлежащее проверке, «областью аудита».

Однако для банков здесь не всё так просто. Позиция Совета PCI SSC изложена на его официальном сайте в разделе «Часто задаваемые вопросы». В ответе на вопрос «применим ли стандарт PCI DSS к эмитентам?» Совет сообщает следующее: «Стандарт PCI DSS применим ко всем сущностям, хранящим, обрабатывающим или передающим данные о держателях карт и все эти сущности должны соответствовать PCI DSS, включая эмитентов. Однако каждая международная платежная система применяет свою собственную программу управления соответствием PCI DSS, определяющую кто проверяет соответствие PCI DSS, уровни поставщиков услуг и торгово-сервисных предприятий, а также крайние сроки достижения соответствия. По своему усмотрению международные платежные системы могут потребовать у эмитентов проверить соответствие PCI DSS. Для уточнения детальных требований к проверке соответствия связывайтесь с международными системами».

Ответы международных платежных систем на вопрос о том, входит ли эмиссионная часть карточной инфраструктуры банка в область QSA-аудита, определенности не добавляют. Письма содержат общие слова о том, что все карточные системы должны соответствовать стандарту. При этом акцент ставится на слова «должны соответствовать», и без этого очевидные. От прямого ответа на конкретный вопрос о вхождении в область QSA-аудита эмиссионной части инфраструктуры международные платежные системы предпочитают уклоняться, оставляя за собой право выборочной проверки.

Сложившаяся на рынке практика QSA-компаний, причем как российских, так и западных, предполагает следующий подход: соответствовать должны все системы, так или иначе связанные с данными о держателях карт, но проверке соответствия стандарту PCI DSS подлежит только эквайринговая часть платежной инфраструктуры, если речь идет о банке. Граница между эквайринговой и эмиссионной частью, которую, к слову, бывает очень непросто провести, проходит по обработке «On-Us» транзакций. Поток данных эквайринговой «On-Us» транзакции проверяется на соответствие стандарту, а всё, что связано с процессом выпуска карт, остается за рамками аудита. Безусловно, подразумевается то, что эмиссионная часть отделена от эквайринговой корректно настроенным межсетевым экраном, иначе эмиссия попадет в область аудита по формальному признаку связанной системы.

Еще раз необходимо отметить, что эта проблема не стоит для торгово-сервисных предприятий и поставщиков услуг, обслуживающих данные о держателях карт для своих клиентов. В подобных организациях область аудита в большинстве случаев совпадает с изолированной областью соответствия.

Минимизация области соответствия

Приводить в соответствие требованиям стандарта необходимо всю область соответствия, к которой относятся все системы, хранящие, обрабатывающие и передающие данные о держателях карт. При правильном подходе эту область можно значительно сократить. Вывести из неё информационные системы можно двумя основными способами:

- исключение данных о держателях карт из отдельных систем, если это позволяют бизнес-требования;
- изоляция области соответствия при помощи межсетевых экранов.

Исключение данных о держателях карт из отдельных систем

Для начала следует составить перечень всех информационных систем, баз данных, общих сетевых ресурсов, хранилищ резервных копий, в которых так или иначе хранятся, обрабатываются и передаются данные о держателях карт. Далее необходимо понять, насколько обосновано с точки зрения бизнеса компании нахождение в них карточных данных.

Очень часто карточные данные встречаются в таких местах, где несложно обойтись и без них. Например, PAN может использоваться в качестве идентификатора клиента в дисконтных программах, или же он может играть роль ссылки при интеграции различных приложений. В подобных случаях PAN может быть заменен на ссылку, имя пользователя, номер счета и т. д. Основная сложность может быть

связана с тем, что такие варианты использования PAN широко практикуются приложениями, разработанными самостоятельно внутри организации, разработчики которых давно уже в ней не работают. Внесение даже самого незначительного изменения в такие приложения порой становится неразрешимой задачей.

Принимая решение лишить ту или иную систему карточных данных, следует помнить о хранящихся в архиве носителях резервных копий этой системы. И если после внесения соответствующих изменений информационная система, которая отныне никак не связана с карточными данными, смело может не рассматриваться с точки зрения PCI DSS, то резервные копии из её «прошлой жизни» продолжают оставаться носителями данных о держателях карт. С ними следует обращаться по всем правилам PCI.

Изоляция области соответствия и внедрение DMZ

После того, как в перечне остались только те системы, которым работа с карточными данными необходима с точки зрения бизнеса компании, необходимо подумать об их изоляции. Дело в том, что по правилам, определенным в стандарте, в область аудита входят все системы хранящие, передающие или обрабатывающие данные о держателях карт, а также связанные с ними системы. Под связанными понимаются системы, соединения с которыми не защищены корректно настроенными межсетевыми экранами.

Особенно остро проблема выделения карточных систем в отдельный сегмент стоит в банках, которые имеют масштабные информационные инфраструктуры, часто бывающие распределенными территориально.

Среду данных о держателях карт по требованиям стандарта PCI DSS следует отделить от внешнего мира при помощи демилитаризованной зоны (DMZ). DMZ должна обеспечивать отсутствие прямых маршрутов между внешней средой и средой данных о держателях карт. С целью минимизации затрат на обеспечение соответствия PCI DSS, рекомендуется размещать DMZ непосредственно на границе среды данных о держателях карт и остальной сети организации.

На рисунке 1 приведен пример не рекомендуемой схемы изоляции среды данных о держателях карт, когда DMZ устанавливается на входе каждого канала связи с внешней средой. Терминалы торговых сервисных предприятий и банкоматы могут подключаться к сети банка через его филиалы (каналы связи C-1, C-2 и C-3), и им требуется соединение с CDE. В этом случае на маршрутизаторе (межсетевом экране) R-2 потребуется открыть входящие соединения из сетей DMZ-1, DMZ-2, DMZ-3. Эти сети попадут в область аудита, так как будут являться связанными. Такое решение имеет право на жизнь, однако потребует от банка значительных ресурсов на достижение и поддержание соответствия. Филиалы, где расположены такие DMZ, придется приводить к соответствию PCI DSS, а аудитору придется их все обследовать в ходе QSA-аудита, что значительно повысит затраты банка.

Наоборот, внедряя DMZ непосредственно на границе DMZ и остальной локальной сети организации, мы можем вынести все офисы и филиалы за скобки аудита, как показано на рисунке 2. Доступ в CDE разрешен только из DMZ. При этом остальная сеть организации приравнивается к недоверенной и проходящий по ней трафик, содержащий данные о держателях карт должен быть зашифрован. Нарушение этого требования сразу же включит всю оставшуюся сеть компании в область аудита.

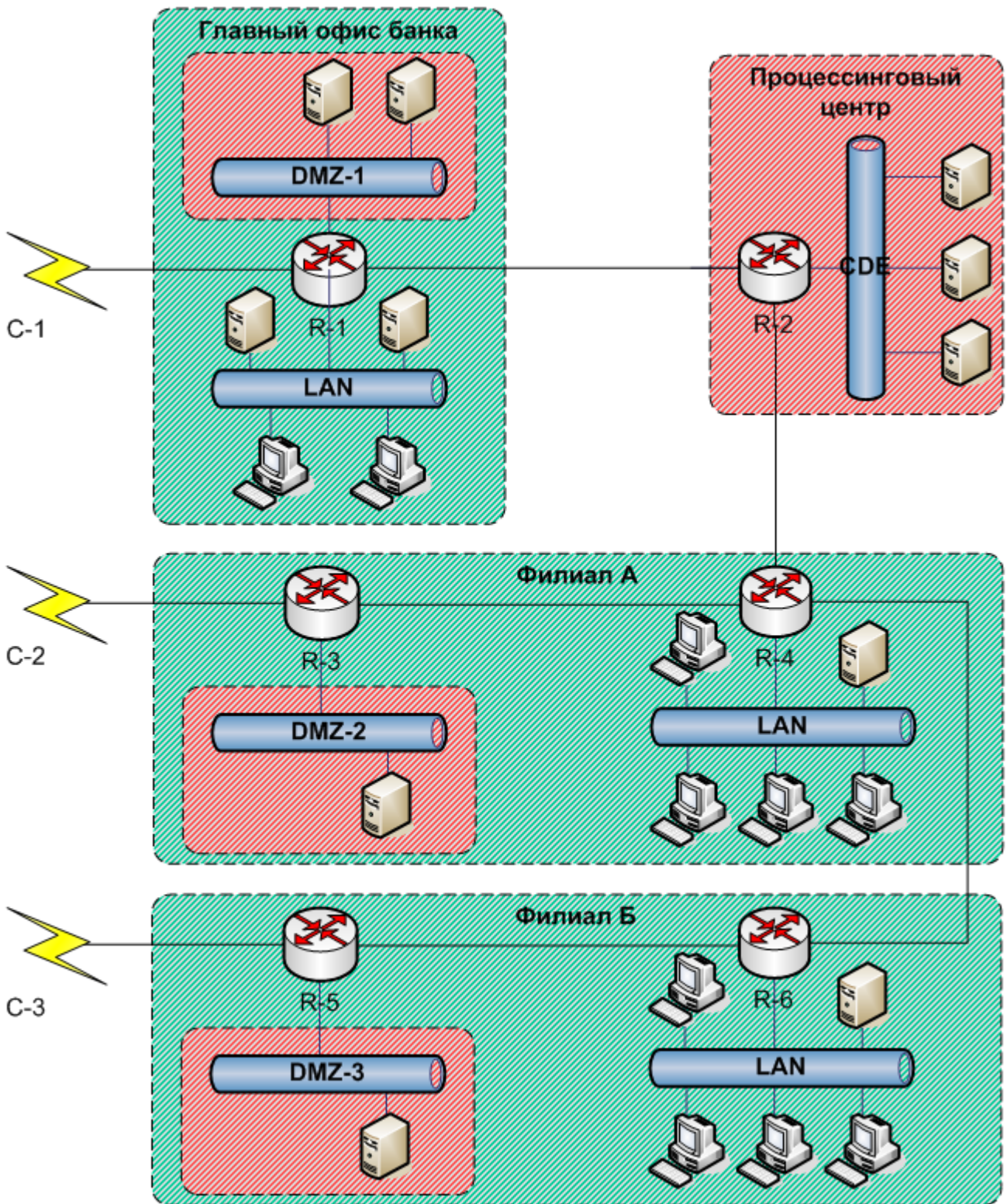


Рисунок 1. Не рекомендуемое решение

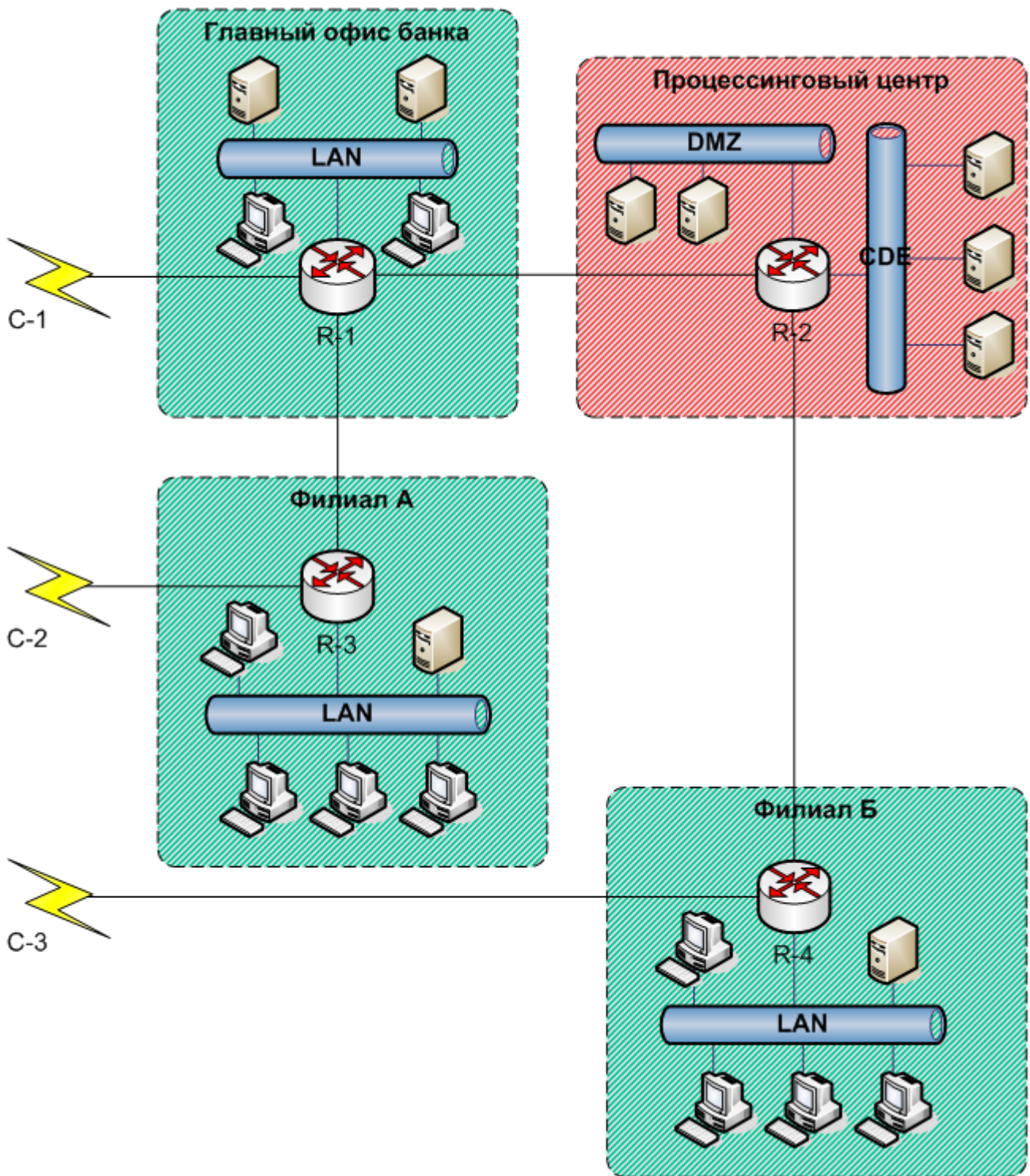


Рисунок 2. Рекомендуемое решение

Об авторе

Сергей Шустиков – руководитель направления менеджмента информационной безопасности компании Digital Security, PCI QSA. Специализируется на управлении безопасностью. Область профессиональных интересов охватывает разработку систем менеджмента информационной безопасности в соответствии с международными стандартами и проведение аудитов на соответствие требованиям международных и национальных стандартов индустрии защиты информации (PCI DSS, ISO 27001, СТО БР-ИББС-1.0).

Занимается научно-исследовательской деятельностью в области системного анализа методов управления в сфере информационных технологий и информационной безопасности. Преподает ряд специальных дисциплин на кафедре Безопасных Информационных Технологий Санкт-Петербургского Государственного Университета Информационных Технологий Механики и Оптики.

О стандарте PCI DSS

Стандарт PCI DSS (Payment Card Industry Data Security Standard) предназначен для обеспечения безопасности обработки, хранения и передачи данных о держателях платежных карт в информационных системах компаний, работающих с международными платежными системами Visa, MasterCard и другими. Стандарт разработан сообществом PCI Security Standards Council, в которое входят мировые лидеры на рынке платежных карт, такие как American Express, Discover Financial Services, JCB, MasterCard Worldwide и Visa International.

Под действие требований стандарта попадают банки, процессинговые центры, поставщики ИТ-услуг, торгово-сервисные предприятия, и иные организации, обрабатывающие транзакции по международным платежным картам. К части этих компаний международные платежные системы предъявляют требование о прохождении обязательного ежегодного аудита компанией, обладающей статусом QSA.

Текущая версия стандарта 1.2.1 выпущена в июле 2009 года.