deiteriy

Секция 5
Выполнение требований PCI DSS

Метод приоритетного подхода

Стандарт PCI DSS содержит 288 проверочных процедур, которые должны дать положительный результат при том или ином варианте подтверждения соответствия организации его требованиям.*

В ответ на закономерный вопрос: «С выполнения какого требования стандарта лучше начинать его внедрение?» Советом PCI SSC был разработан документ под названием «Приоритетный подход к выполнению требований стандарта PCI DSS».

Приоритетный подход рекомендует выполнять требования в шесть этапов:

1. Удаление КАД и ограничение хранения ДДК.
2. Защита периметра, внутренних и беспроводных сетей.
3. Обеспечение безопасности приложений, БД и ОС.
4. Мониторинг и контроль доступа.
5. Защита хранимых данных.
6. Внедрение системы менеджмента информационной безопасности.

* - вариантами подтверждения соответствия стандарту PCI DSS являются: заполнение листа самооценки (SAQ), выполнение внутреннего ISA-аудита и выполнение внешнего QSA-аудита.

Этап 1. Удаление КАД и ограничение хранения ДДК

Согласно требованиям раздела 3 стандарта PCI DSS, критичные аутентификационные данные (КАД), к которым относятся TRACK, CVV2, PIN или PIN-block, после авторизации транзакции хранить запрещается. Единственным исключением является хранение КАД эмитентом для обеспечения возможности авторизации транзакции.

Номера карт (PAN), относящиеся к данным о держателях карт (ДДК), хранить можно, при этом они должны быть защищены в соответствии с требованием 3.4 стандарта PCI DSS.

Из конкретных мер по обеспечению безопасности платежной индустрии это требование является наиболее важным во всем стандарте PCI DSS. Оно направлено на снижение наиболее высоких рисков, связанных с утечкой данных, обладая которыми можно выполнить транзакцию по карте.

Если критичные аутентификационные данные сохраняются после авторизации, их необходимо удалить и настроить компоненты информационной инфраструктуры таким образом, чтобы исключить возможность сохранения КАД в будущем.

Номера карт могут потребоваться организации в её бизнес-процессах, а их хранение несет меньший риск, чем хранение КАД. Однако их при хранении следует защищать, а срок хранения ДДК должен быть ограничен бизнес-требованиями организации.

«Если тебе это больше не нужно – не храни это» –
золотое правило обеспечения безопасности индустрии платежных карт.

Этап 1. Удаление КАД и ограничение хранения ДДК

Иногда найти, где именно в информационной инфраструктуре организации спрятались КАД и ДДК бывает очень непросто. Задача несколько облегчается тем, что у каждого вида ДДК или КАД есть свои излюбленные места:

1. **PAN** - обитает практически везде, но особенно предпочитает:
   - таблицы баз данных с журналами транзакций;
   - файлы протоколирования событий приложений фронт-офиса;
   - хранилища данных и журналы, связанные с системами электронной коммерции;
   - таблицы баз данных бэк-офиса;
   - журналы протоколирования событий на банкоматах (ATM), их контрольная лента;
   - в розничных магазинах – системы поддержки программ лояльности и журналы протоколирования операций контрольно-кассовой техники;
   - служебная почта сотрудников call-центра и технической поддержки;
   - АБС банка;
   - архивы бумажных документов о выдаче персонализированных карт;
   - автоматизированные системы риск-менеджмента и фрод-мониторинга.

Этап 1. Удаление КАД и ограничение хранения ДДК

2. **CVV2** - в особенности любит все, что связано с электронной коммерцией:
   - хранилища данных и журналы, связанные с платежными системами Интернет-магазина;
   - Лог-файлы входящих запросов веб-серверов (например, Apache).
   - таблицы баз данных бэк-офиса.

   Если организация не занимается Интернет-эквайрингом, то найти у неё в информационной инфраструктуре CVV2 почти невозможно.

3. **TRACK** - он есть везде, где есть кард-ридер:
   - таблицы баз данных с журналами card-present транзакций;
   - файлы протоколирования событий приложений фронт-офиса;
   - журналы протоколирования событий на банкоматах (ATM), их контрольная лента;
   - в розничных магазинах – в журналах встроенных в кассовое решение POS-приложений;
   - системы персонализации карт.

4. **PIN/PIN-блок** - в открытом виде PIN практически не встречается, зато в виде шифрограммы (PIN-блок) является верным спутником TRACK там, где есть card-present транзакции:
   - файлы протоколирования событий старых приложений фронт-офиса;
   - таблицы баз данных с журналами card-present транзакций старых приложений.

Этап 2. Защита периметра, внутренних и беспроводных сетей

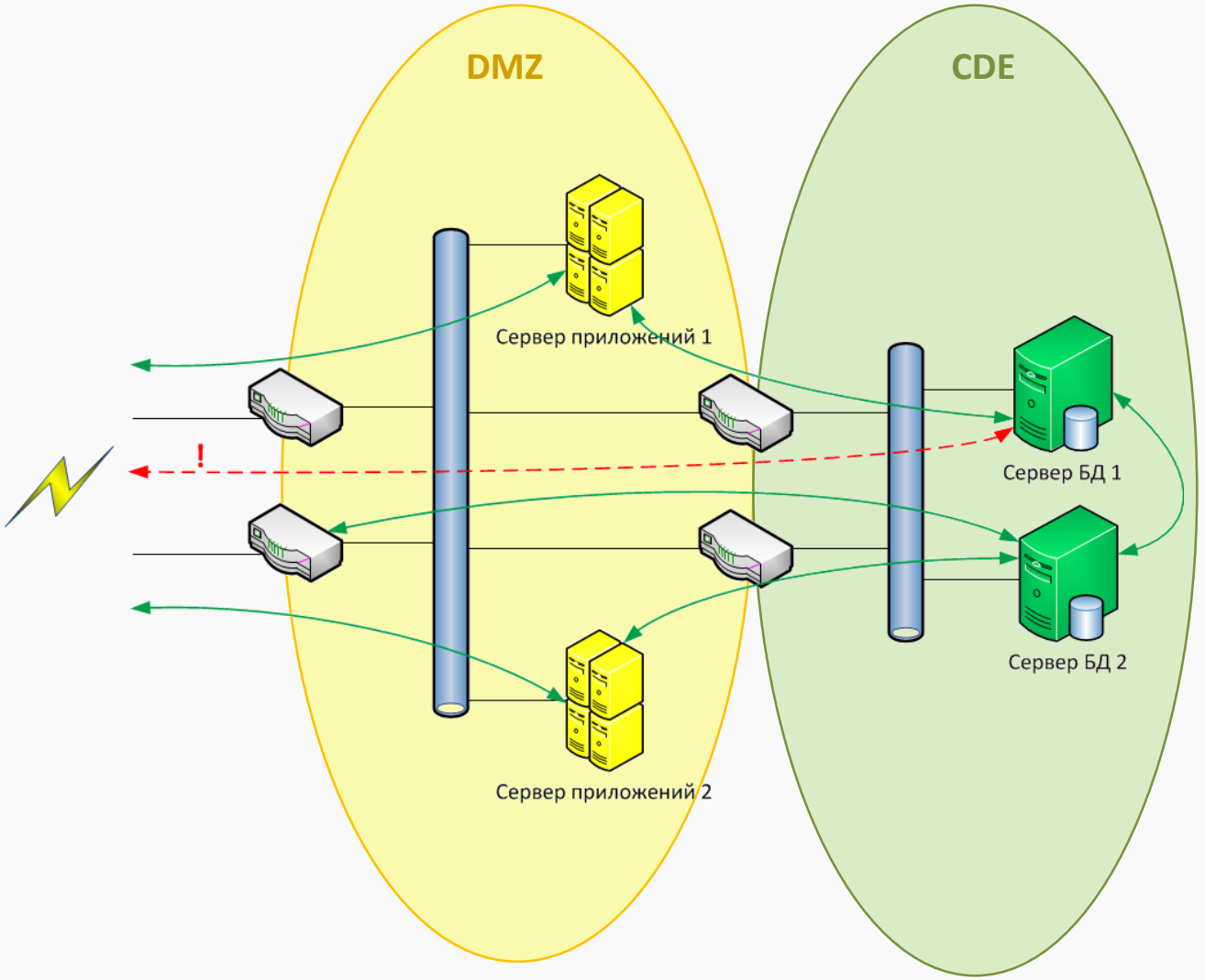
Атаки по сети являются наиболее распространенным способом компрометации данных злоумышленниками. Кроме того, во время передачи по сетям данные особенно уязвимы. Следующим по приоритету этапом будет защита внешнего периметра сети, внутренних и беспроводных сетей организации.

На этом этапе следует решить три задачи:

- защитить вычислительную сеть организации путем корректной настройки маршрутизаторов и межсетевых экранов, а также организации выделенного защищенного внутреннего (Cardholder Data Environment, CDE) и пограничного DMZ-сегмента* сети;
- обеспечить учет и контроль конфигураций компонентов информационной инфраструктуры, для этого разработать стандарты конфигурации компонентов информационной инфраструктуры;
- обеспечить безопасность передаваемых ДДК путем шифрования каналов связи, по которым они передаются (можно применять широкий спектр решений от различных VPN до SSL).

* - основное правило организации CDE и DMZ таково: все компоненты, хранящие ДДК, должны быть расположены в CDE, при этом все внешние соединения должны иметь возможность устанавливать соединения только с компонентами, расположенными в DMZ. Все соединения из CDE во внешнюю среду должны также иметь возможность устанавливать соединения только с компонентами в DMZ.

Этап 2. Защита периметра, внутренних и беспроводных сетей



Этап 3. Обеспечение безопасности приложений, БД и ОС

Компоненты прикладного уровня на сегодняшний день являются самыми уязвимыми с точки зрения информационной безопасности. Следующим этапом будет защита платежных приложений и баз данных, а также операционных систем, на которых они установлены.

На этом этапе следует решить четыре задачи:

- наладить процесс безопасной поддержки информационной инфраструктуры, внедрив процедуры управления изменениями. Хорошей практикой будет внедрение такого элемента из руководства ITIL-ITSM как база данных управления конфигурациями Configuration Management Database (CMDB). Необходимо обеспечить регулярное обновление программного обеспечения, как минимум – установку критических патчей. Если в организации ведется разработка программного обеспечения, следует выделить под неё отдельную среду разработки, не связанную с производственными системами.
- настроить механизмы аутентификации пользователей приложений, баз данных и операционных систем, внедрив строгую парольную политику;
- разработать и внедрить организационные процедуры управления логическим и физическим доступом к данным. Лучшим вариантом будет внедрение метода управления доступом, основанного на ролях пользователей в бизнес-процессах (Role-Based Access Control, RBAC);
- внедрить средства антивирусной защиты информационной инфраструктуры.

Этап 4. Мониторинг и контроль доступа

После того, как информационная инфраструктура организации стала относительно защищена, следует внедрить механизмы объективного контроля защищенности, а также различные системы мониторинга безопасности.

На этом этапе следует решить три задачи:

- настроить аудит и протоколирование событий и действий. Это означает, что по возможности все компоненты информационной инфраструктуры должны вести лог-файлы своей активности, связанной с безопасностью информационной инфраструктуры, использованием механизмов аутентификации, использованием административных привилегий, а также доступом к данным о держателях карт. Рекомендуемым, но не обязательным решением будет внедрение централизованной системы сбора логов и управления событиями.
- внедрить средства контроля информационной безопасности – сканеры уязвимостей, системы обнаружения и предотвращения вторжений, системы контроля беспроводных сетей, межсетевые экраны уровня приложений, системы контроля целостности файлов;
- разработать и внедрить регулярные процедуры использования всего вышеперечисленного, определить ответственных лиц и форму регистрации записей о выполнении. Также следует разработать планы реагирования на инциденты и события информационной безопасности.

Этап 5. Защита хранимых данных

Информационная инфраструктура защищена и можно приступить к защите самих данных о держателях карт, хранящихся в её ядре – среде данных о держателях карт (Cardholder Data Environment, CDE).

После того, как были удалены все критичные аутентификационные данные, хранимые данные о держателях карт представлены только номером карты (PAN).

При хранении номера карты следует применять один из методов защиты согласно требованию 3.4 стандарта PCI DSS:

- шифрование;
- маскирование (1234 56xx xxxx 7890);
- однонаправленная хеш-функция*;
- токенизация**.

* – при наличии доступа одновременно к маскированному и хешированному номеру одной и той же карты, для злоумышленника не составит большого труда восстановить исходный PAN.

** – токен – уникальный идентификатор транзакции или карты, используемый вместо PAN.

Этап 6. Внедрение системы менеджмента ИБ

Информационная безопасность – это процесс, который имеет начало, но не имеет конца, и им необходимо управлять. Для закрепления внедренных методов защиты данных о держателях карт следует внедрить процессы информационной безопасности, выполняемые на практике в строгом соответствии с документированными процедурами. Хорошим решением здесь будет следование рекомендациям таких стандартов, как ISO 27001 и СТО БР ИББС-1.0.

Структура нормативных документов (документированных процедур) по информационной безопасности в первую очередь должна быть адекватной размерам, организационной структуре и бизнес-процессам организации. Различаются одно-, двух- и трехуровневые структуры нормативных документов по информационной безопасности.

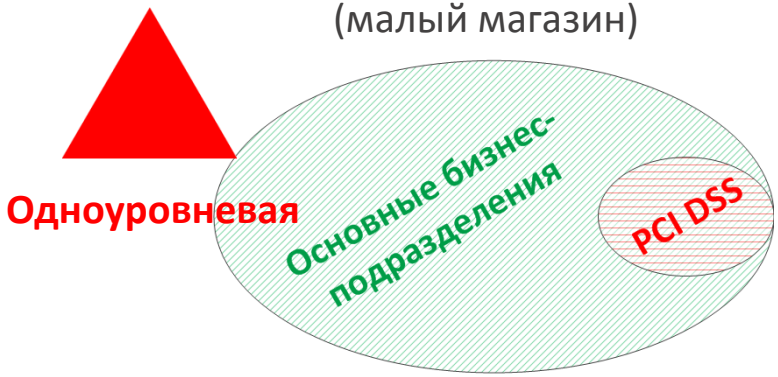
Одноуровневая – содержит минимально необходимые инструкции и стандарты конфигурации. Может вестись в виде записей в системе JIRA или на движке WIKI.

Двухуровневая – содержит общий руководящий документ, такой как Политика ИБ, определяющий требования руководства организации к этому процессу, плюс документированные процедуры, инструкции и стандарты конфигурации.

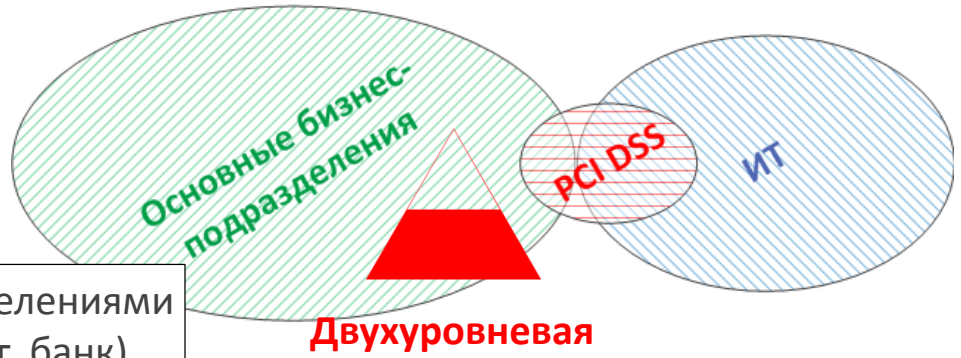
Трехуровневая – помимо Политики ИБ и низкоуровневых процедур и инструкций, описывающих процесс детально, содержит также промежуточный уровень регламентов (частных политик), описывающих требования к каждому из процессов ИБ и дающих возможность распределенного контроля за обеспечением ИБ в крупной организации.

Этап 6. Внедрение системы менеджмента ИБ

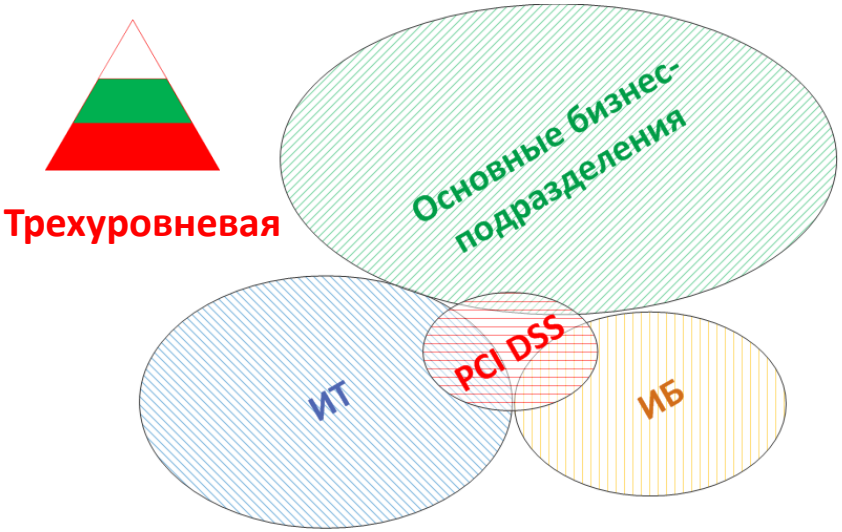
В компании без выделенных ИТ и ИБ подразделений (малый магазин)



В компании с выделенным ИТ-подразделением (средний магазин, платежный шлюз)



В компании с выделенными ИТ- и ИБ-подразделениями (крупный магазин, крупный поставщик услуг, банк)



Причины применения компенсационных мер

Наиболее распространёнными причинами применения компенсационных мер на сегодня являются:

- зависимость бизнес-процессов организации от устаревшего, неподдерживаемого производителем программного обеспечения или оборудования;
- нехватка производственных мощностей и невозможность их оперативного увеличения в силу архитектурных особенностей;
- существенные бюджетные ограничения;
- до недавнего времени – отсутствие в России хостинг-провайдеров, сертифицированных по стандарту PCI DSS.

Требования к компенсационным мерам

Компенсационная мера должна быть направлена на защиту данных о держателях карт от того же риска, от которого защищает выполнение заменяемого ею требования стандарта.

Компенсационная мера должна снижать риск в той же степени, что и требование стандарта.

Выполнение существующих требований стандарта PCI DSS не может являться компенсационной мерой. Однако, компенсационной мерой может являться применение средств защиты, предусмотренных существующими требованиями стандарта в тех областях информационной инфраструктуры, в которых их применение не требуется по стандарту.

Компенсационная мера не должна противоречить другим требованиям стандарта PCI DSS.

Обоснованность компенсационной меры и её соответствие описанным требованиям проверяется аудитором в рамках ежегодного подтверждения соответствия организации PCI DSS.