Решения PostgresPro для выполнения требований PCI-DSS

Международный стандарт безопасности данных платежных карт PCI DSS предназначен для обеспечения защиты от несанкционированного доступа пользовательских платежных данных, которые хранятся, передаются и иным образом обрабатываются в организациях. Требования PCI DSS предъявляются ко всем системным компонентам, входящим или подключенным к информационной среде держателей карт, в том числе – к СУБД.

ООО «Постгрес Профессиональный», разработчик и правообладатель ПО класса СУБД на основе PostgreSQL в соответствии с реестровой записью №104 от 18.03.2016 в reestr.digital.gov.ru, является также обладателем лицензии ФСТЭК на деятельность по разработке и производству средств защиты конфиденциальной информации (см. reestr.fstec.ru/reg2). Наиболее полно средства защиты, разработанные или поддерживаемые ООО «Постгрес Профессиональный», и требования к которым устанавливаются стандартом PCI DSS, представлены в редакции СУБД Postgres Pro Certified.

Ниже в статье приведены примеры таких решений и механизмы их работы

Общие требования PCI DSS

Мониторинг	Проверка корректной работы средств защиты: МЭ, IDS/IPS, антивируса, системы контроля целостности, средств разграничения доступа.
Реагирование на отказы работы средств защиты	• восстановление механизма обеспечения безопасности; • определение причины отказа; • определение и решение любых проблем с безопасностью, возникших во время отказа механизма обеспечения безопасности; • внедрение нового средства безопасности (например, процесса или технического механизма) во избежание повторного возникновения причины отказа; • возобновление мониторинга механизма безопасности, желательно с временным его усилением для проверки эффективности работы механизма.
Изменение инфраструктуры	Контроль за изменением инфраструктуры, способной повлиять на область действия PCI DSS – добавление новой системы (накатывание стандарта конфигурации), вывод из эксплуатации, обновление документов/перечней. Своевременное применение стандартов конфигурации, обновление реестров, области действия.
Изменение организации	Формальное ревью области действия Стандарта и применимости требований вследствие изменении организационной структуры.
Периодический контроль	Проведение оценки соответствия с целью подтверждения того, что требования PCI DSS выполняются, а сотрудники следуют процессам обеспечения безопасности.
Технологический контроль	Контроль статуса поддержки ПО и железа. Своевременная замена/миграция на более современные средства.

Выдержка из Детальных требований PCI DSS и процедур проведения аудита

Построение и обслуживание защищенной сети и систем

> Требование 1. Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт *– неприменимо к СУБД*
>
> Требование 2. Не использовать пароли и другие системные параметры, заданные производителем по умолчанию *– частично применимо к СУБД*

Защита данных держателей карт

Требование 3. Обеспечить безопасное хранение данных держателей карт – *применимо к СУБД*

Требование 4. Обеспечить шифрование данных держателей карт при их передаче через сети общего пользования – *частично применимо к СУБД*

Программа управления уязвимостями

Требование 5. Защищать все системы от вредоносного ПО и регулярно обновлять антивирусное ПО – *неприменимо к СУБД*

Требование 6. Разрабатывать и поддерживать безопасные системы и приложения – *частично применимо к СУБД*

Внедрение строгих мер контроля доступа

Требование 7. Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью – *частично применимо к СУБД*

Требование 8. Определять и подтверждать доступ к системным компонентам – *частично применимо к СУБД*

Требование 9. Ограничить физический доступ к данным держателей карт – *неприменимо к СУБД*

Регулярный мониторинг и тестирование сети

Требование 10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт – *частично применимо к СУБД*

Требование 11. Регулярно выполнять тестирование систем и процессов обеспечения безопасности – *неприменимо к СУБД*

Поддержание политики информационной безопасности

Требование 12. Разработать и поддерживать политику информационной безопасности для всего персонала организации – *неприменимо к СУБД*

Механизмы выполнения Требования 2
(Не использовать пароли и другие системные параметры, заданные производителем по умолчанию**)**

- Изменение ВСЕХ логинов/паролей, установленных по умолчанию, для всех систем
- Изменение логинов/паролей, установленных по умолчанию, для беспроводных устройств
- Изменение настроек, установленных по умолчанию, способных повлиять на безопасность
- Разработка стандартов конфигурации для ВСЕХ компонентов с учетом положений лучших практик, рекомендуемых настроек безопасности производителей
- Поддержание стандартов конфигураций в актуальном состоянии
- Один сервер – одна функция
- Шифрование неконсольного административного доступа
- Инвентаризация, учет всех компонентов, систем, входящих в область действия стандарта
- Документирование всех требований (политик) и процессов (регламенты) по изменению настроек согласно требованиям раздела 2

Решения PostgresPro для выполнения Требований 2

- Настройка парольных политик через Профили postgrespro.ru/docs/enterprise/16/sql-createprofile

- Контроль целостности конфигурации СУБД postgrespro.ru/docs/enterprise/16/pg-integrity-check
- Регистрация изменений конфигурации СУБД postgrespro.ru/docs/enterprise/16/runtime-config-logging
- Криптозащита трафика между клиентом и сервером postgrespro.ru/docs/enterprise/16/ssl-tcp

Механизмы выполнения Требования 3
(Обеспечить безопасное хранение данных держателей карт [ДДК])

- Установление необходимости, причин и срока хранения ДДК
- Разработка методов удаления данных, срок хранения которых истек
- Запрет хранения Критичных аутентификационных данных [КАД] после авторизации
- Маскирование PAN при его отображении в случае отсутствия необходимости видеть весь PAN
- Защита PAN во всех местах его хранения (усечение, шифрование, токенизация, хэширование)
- Документирование требований к средствам/методам защиты PAN
- Запрет использования пароля от учетной записи в качестве ключа шифрования раздела диска или всего диска
- Защита ключей шифрования
- Управление жизненным циклом ключей шифрования
- Документирование всех требований (политик), процессов (регламенты) , настроек согласно требованиям раздела 3

Решения PostgresPro для выполнения Требований 3

- Возможно удаление данных по фильтру postgrespro.ru/docs/enterprise/16/dml-delete или с помощью статического маскирования postgrespro.ru/docs/enterprise/16/pgpro-anonymizer ; для 17-й версии Enterprise редакции разработан функционал Information Lifetime Management (перенос устаревших или редко используемых данных в другое табличное пространство)
- Единственные КАД, которые можно хранить — это номер карты Primary Account Number [PAN], и то исключительно в зашифрованном виде. В текущем версии поддерживаются базовые криптографические функции postgrespro.ru/docs/enterprise/16/encryption-options , для 17-й версии Enterprise редакции разработан функционал Transparent Data Encryption [TDE]
- Политики динамического маскирования позволяют на лету частично скрывать PAN postgrespro.ru/docs/enterprise/16/pgpro-anonymizer
- В TDE разработаны механизмы работы с секретами (ключами) защитного преобразования данных (шифрования) – иерархия, места хранения (в том числе – внешнее для мастер-ключа), ротация, вызов неактивных ключей

Механизмы выполнения Требования 4
(Обеспечить шифрование данных держателей карт при их передаче через сети общего пользования)

- Использование стойких криптопротоколов при передаче ДДК через общедоступные сети
- Безопасная настройка беспроводных сетей в случае передачи по ним ДДК (например IEEE 802.11i)
- Запрет передачи ДДК через пользовательские технологии обмена сообщениями (месенджеры, эл.почта, чаты)
- Документирование всех требований (политик), процессов (регламенты), настроек согласно требованиям раздела 4

Решения PostgresPro для выполнения Требований 4

- Криптозащита трафика между клиентом и сервером postgrespro.ru/docs/enterprise/16/ssl-tcp

Механизмы выполнения Требования 6
(Разрабатывать и поддерживать безопасные системы и приложения)

- Внедрение процесса обнаружения уязвимостей из открытых источников и их ранжирование (анализ информации из открытых источников, а не результатов сканирования / ASV / пентеста)
- Внедрение патч-менеджмента (обновления/патчи). Тестирование обновлений, документирование влияния обновления на безопасность системы, разработка процедуры отката для каждого обновления, согласование внесения изменения в производственную среду.
- Установка обновлений безопасности, закрывающих критичные уязвимости (согласно принятой методике ранжирования) на всех компонентах в течение одного месяца со дня выхода патча.
- Внутренняя и сторонняя разработка ПО в соответствии с требованиями PCI DSS, лучших практик.
- Разделение сред разработки, тестирования, производственной среды.
- Запрет использования боевых данных в качестве тестовых
- Процесс анализа кода (код-ревью) сотрудником, не участвовавшим в написании проверяемого кода (вручную или автоматически)
- Предотвращение появления потенциальных уязвимостей на этапе написания кода. Обучение разработчиков, разработка с учетом методов безопасного программирования
- Необходимо разрабатывать и тестировать ПО под последние версии ОС (со всеми патчами), с использованием последних версий библиотек
- Установка Web-application firewall [WAF] перед платежным веб-приложением или проведение пен.теста веб-приложения как минимум раз в год и после каждого релиза.
- Документирование всех требований (политик), процессов (регламенты), настроек согласно требованиям раздела 6. Документирование принятых в компании методов борьбы с уязвимостями при разработке.

Решения PostgresPro для выполнения Требований 6

- ООО «Постгрес Профессиональный» сотрудничает с ФСТЭК РФ по формированию базы данных уязвимостей bdu.fstec.ru/search/index?q=postgres , с сообществом по выпуску заплаток безопасности postgresql.org/support/security и оперативно предоставляет их заказчикам (в том числе – с выпуском внеочередных сертифицированных релизов). Подробности – в Release Notes, пример – на postgrespro.ru/blog/news/5969695
- ООО «Постгрес Профессиональный» является обладателем лицензии ФСТЭК на деятельность по разработке и производству средств защиты конфиденциальной информации (см. reestr.fstec.ru/reg2). Все разработки проходят через статический и динамический анализ кода с учетом появления новых версий ОС
- Одна приобретенная лицензия на процессор СУБД PostgresPro в продуктивной среде дает право на использование еще одной процессорной лицензии в среде разработки и еще одной процессорной лицензии в среде тестирования. Для тестирования можно использовать данные, полученные с помощью статического маскирования postgrespro.ru/docs/enterprise/16/pgpro-anonymizer

Механизмы выполнения Требования 7
(Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью)

- Управление доступом к компонентам и данным согласно концепции Разделения полномочий (Segregation of Duties [SoD]) / матрице доступа

- Внедрение процесса выдачи доступа по заявкам
- Внедрение на всех системах средств контроля доступа с установкой запрещающего правила по умолчанию.
- Документирование всех требований (политик), процессов (регламенты), настроек согласно требованиям раздела 7.

Решения PostgresPro для выполнения Требований 7

- Дополнительно к базовым механизмам предоставления доступа Postgres SQL (позволяющих управлять доступом вплоть до ячейки – см. postgrespro.ru/docs/enterprise/16/user-manag, postgrespro.ru/docs/enterprise/16/sql-createrole , postgrespro.ru/docs/enterprise/16/sql-grant , postgrespro.ru/docs/enterprise/16/sql-revoke , postgrespro.ru/docs/enterprise/16/ddl-rowsecurity) реализован функционал Разграничения прав между привилегированными пользователями СУБД postgrespro.ru/docs/enterprise/16/sod-separation-of-duties и Ограничения доступа администратора СУБД к данным postgrespro.ru/docs/enterprise/16/restrict-dbms-admin-data-access . Доступ в защищенную схему запрещен по умолчанию.
- Для 17-й версии Enterprise редакции разработан функционал Поиска избыточных привилегий. Использование прав определяется по статистике; отчёт показывает, какие права пользователя использовались, какие не использовались, напрямую ли были получены эти права либо же через какую-то обобщающую роль

Механизмы выполнения Требования 8
(Определять и подтверждать доступ к системным компонентам)

- Внедрение процесса управления идентификацией: выдача уникальных идентификаторов, запрет использования групповых и разделяемых учетных записей, блокировка учетных записей при идентификации согласно политике
- Внедрение процесса управления учетными записями – создание, блокировка, удаление, изменение.
- Управление учетными записями поставщиков услуг при их удаленном доступе.
- Требования к средствам аутентификации, в т.ч. паролям и парольным фразам, 2ФА. Запрет использования групповых и разделяемых паролей.
- Создание инструкций по использование каждого метода аутентификации
- Ограничение доступа к БД с ДДК, использование хранимых процедур, запрет прямых запросов для пользователей, использование учетных записей приложений
- Документирование всех требований (политик), процессов (регламенты), настроек согласно требованиям раздела 8.

Решения PostgresPro для выполнения Требований 8

- Управление учетными записями реализовано через роли postgrespro.ru/docs/enterprise/16/database-roles
- Парольные политики и условия блокировки учетных записей задаются через Профили postgrespro.ru/docs/enterprise/16/sql-createprofile
- Поддерживаются различные методы аутентификации postgrespro.ru/docs/enterprise/16/client-authentication
- Аутентификация клиентов управляется конфигурационным файлом **pg_hba.conf** postgrespro.ru/docs/enterprise/16/auth-pg-hba-conf . В нем можно настроить ограничение доступа к БД с ДДК

Механизмы выполнения Требования 10
(Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт)

- Обеспечить регистрацию событий на всех компонентах:
  - любой доступ к ДДК
  - все действия root
  - любой доступ к журналам событий
  - использование механизмов идентификации, расширение полномочий, изменения учетных записей с правами суперпользователя и администратора;
  - инициализация журналов, остановка или приостановка ведения журналов
  - создание и удаление объектов системного уровня
- Настроить параметры журналирования. Хранить журналы 1 год.
- Установить центральный сервер сбора журналов событий.
- Установить единый источник времени и настроить на синхронизацию с ним все компоненты
- Ограничить доступ к журналам [SoD]
- Анализировать все события на предмет аномалий или подозрительной активности
- Документирование всех требований (политик), процессов (регламенты), настроек согласно требованиям раздела 10.

Решения PostgresPro для выполнения Требований 10

- Настройка регистрации событий, связанных с работой сервера СУБД, описана в https://postgrespro.ru/docs/enterprise/16/runtime-config-logging , а событий, связанных с безопасностью – в https://postgrespro.ru/docs/enterprise/16/pg-proaudit
- По умолчанию только владелец сервера СУБД может читать и писать в журнальные файлы (см. параметр "log_file_mode").