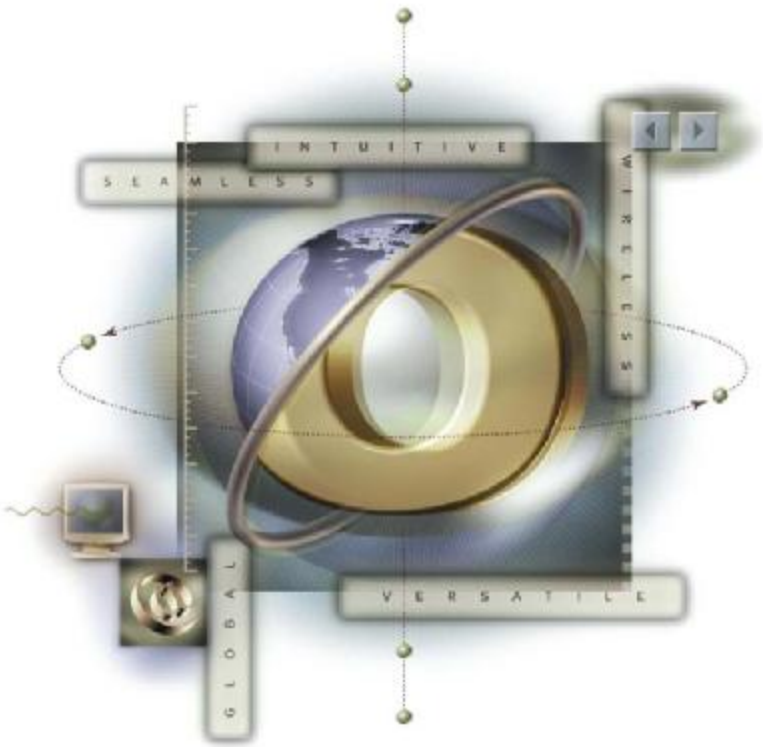
micros | FIDELIO



Opera Hotel Edition

ORACLE

ПО OPERA : Реализация стандарта PA-DSS

V5.0+

Август 2009

Авторское право

MICROS Systems, Inc.
Fidelio Technologies Inc.
2640 Golden Gate Parkway, Suite 211
Naples, FL 34105
Voice: (239) 643-7999 / Fax: (239) 643-7911

Документ: 1470 ПО **Opera :** Реализация стандарта **PA-DSS**

Автор:
Соавторы:

Содержание

ОБЩАЯ ИНФОРМАЦИЯ 4

Об этом Документе 4

О Совете по развитию стандартов информационной безопасности индустрии платежных карт 4

О стандарте безопасности данных индустрии платежных карт **(PCI DSS)** 4

Для кого предназначен этот документ 6

Необходимые предварительные знания 6

OPERA ВЕРСИЯ 5.0+ И СТАНДАРТ ДАННЫХ ПЛАТЕЖНЫХ ПРИЛОЖЕНИЙ 7

Стандарт безопасности данных платежных приложений 7

Построение и обслуживание защищенной сети 7

Защита данных о держателях карт 8

Опционные настройки 8

Опционные настройки 9

Программа управления уязвимостями 10

Внедрение строгих мер контроля доступа 10

Регулярный мониторинг и тестирование сети 11

Поддержание политики информационной безопасности 12

Руководство для апгрейда с предыдущей версии **Opera** 12

Внедрение и поддержание политики хранения данных 13

Интерфейсы с третьими сторонами 15

Общая Информация

Об этом Документе

Настоящий документ представляет собой краткое руководство, содержащее информацию о соответствии **MICROS Systems, Inc.** требованиям, предъявляемым Советом по развитию стандартов безопасности данных индустрии платежных карт **(PCI-SSC)** к платежным приложениям **(PA-DSS).** Этот документ относится исключительно к программному продукту ***OPERA** версии **5.0+ Enterprise Solution***, в т.ч. **Opera Property Management, Opera Limited Service (Xpress), Opera Xpress Lite (Lite), Operetta** и **Opera Reservation System.** Этот документ ежегодно распространяется среди всех клиентов или передается при апгрейде программного продукта.

О Совете по развитию стандартов безопасности данных индустрии платежных карт[1]

Совет по развитию стандартов безопасности данных индустрии платежный карт **-** это открытый планетарный форум, запущенный в **2006** году, задачей которого стали разработка, контроль, обучение и просвещение в вопросах, связанных со стандартами безопасности данных индустрии платежных карт, а именно: Стандартом безопасности данных **(DSS),** Стандартом безопасности данных для платежных приложений **(PA-DSS)** и Требованиями к устройствам ввода ПИН-номера **(PED).**

Все пять членов-учредителей пришли к соглашению о том, что стандарты безопасности данных **PCI DSS –** это технические требования, которым должны соответствовать все используемые ими программы информационной безопасности. Каждый член-учредитель также признает, что гарантии качества **(QSA)** и списки утвержденных поставщиков **(ASV),** сертифицированных Советом **PCI-SSC,** отвечают условиям соответствия стандарту **PCI DSS.**

Совет **PCI-SSC** зарегистрирован в США, штате Дэлавер, как корпорация с ограниченной ответственностью **(LLC),** учредителями которой стали **American Express, Discover Financial Services, JCB International, MasterCard Worldwide** и **Visa Inc.** Все эти пять платежных брендов принимают одинаковое участие в управлении Советом, имеют в нем равную долю акций и сообща делят ответственность за работу организации. Другие держатели акций данной индустрии также приглашаются присоединиться к этой группе для обсуждения предлагаемых добавлений или изменений существующих стандартов.

О Стандарте безопасности данных индустрии платежных карт **(PCI DSS)**[2]

Стандарт безопасности данных индустрии платежных карт **(PCI DSS) –** это набор всеобъемлющих требований, призванный повысить безопасность данных платежных счетов. Стандарт разработан платежными брендами-учредителями Совета: **American Express, Discover Financial Services, JCB International, MasterCard Worldwide** и **Visa Inc. Inc. International** с целью облегчить повсеместное внедрение согласованных мер информационной защиты во всем мире.

PCI DSS – это всеобъемлющий стандарт безопасности данных, включающий требования к управлению безопасностью, политике, процедурам, архитектуре сети, конструированию программ и другим важным мерам защиты. Этот всеобъемлющий стандарт призван помочь организациям проактивно защищать данные счетов своих клиентов.

Совет **PCI-SSC** будет и впредь, по мере необходимости, повышать стандарт **PCI DSS,** включая в него любые новые или измененные требования, необходимые для снижения рисков информационной безопасности платежным приложений, продолжая при этом широко-масштабное внедрение этого стандарта.

По мере развития стандарта, его будут оценивать Консультативный Комитет и другие организации-участники. Поощряется вклад всех основных держателей акций на этапах создания и обсуждения предлагаемых дополнений и изменений стандарта **PCI DSS.**

[1] **https://www.pcisecuritystandards.org/about/index.shtml**
[2] **https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml**

Главное в стандарте **PCI DSS –** это набор принципов и соответствующих требований, вокруг которых группируются элементы **DSS:**[3]

Построение и обслуживание защищенной сети

Требование 1: Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт

Требование 2: Не использовать настройки системных паролей и других параметров безопасности данных, заданных производителем по умолчанию

Защита данных о держателях карт

Требование 3: Обеспечить безопасное хранение данных о держателях карт

Требование 4: Обеспечить шифрование данных о держателях карт при их передаче через открытые сети общего пользования

Программа управления уязвимостями

Требование 5: Использовать и регулярно обновлять антивирусные программы

Требование 6: Разрабатывать и поддерживать системы и приложения безопасности

Внедрение строгих мер контроля доступа

Требование 7: Ограничить доступ к данным держателей карт служебной необходимостью

Требование 8: Привязать уникальный идентификатор всем, у кого есть доступ к ПК

Требование 9: Ограничить физический доступ к данным держателей карт

Регулярный мониторинг и тестирование сети

Требование 10: Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт

Требование 11: Регулярно тестировать системы и процессы информационной безопасности

Поддержание политики информационной безопасности

Требование 12: Поддерживать политику информационной безопасности

[3] **pcisecuritystandards.org**

Для кого предназначен этот документ

Этот документ предназначен для следующей аудитории:

- Клиенты **MICROS**
- Установщики/Программисты **MICROS**
- Дилеры **MICROS**
- Служба Поддержки Клиентов **MICROS**
- Обучающий персонал **MICROS**
- Персонал **MIS**

Необходимые предварительные знания

Данные документ рассчитан на аудиторию, имеющую следующие знания или навыки:

- Умение работать с ПК
- Понимание базовых сетевых концепций
- Опыт работы с ОС на платформах, поддерживаемых **OPERA**
- Знакомство с программным продуктом **OPERA**
- Знакомство с периферийными устройствами, необходимыми для работы с **MICROS**

OPERA версия **5.0+** и Стандарт данных для платежных приложений

Стандарт безопасности данных для платежных приложений

В то время как **MICROS** признает важность поддержания безопасности и целостности данных о держателях платежных карт, некоторые параметры Стандарта **PCI DSS** и Совета **PCI-SSC** остаются исключительной ответственностью клиента. Настоящий раздел содержит описание **12** пунктов Стандарта **PCI DSS.** Информация в этом разделе касается только соответствия программного продукта **OPERA V5.0** Стандарту **PCI DSS.**

Полное описание Стандарта **PCI-DSS** можно найти на вэб-сайте Совета **PCI-SSC** **<http://pcisecuritystandards.org>.**

Построение и обслуживание защищенной сети

1. Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт

Межсетевые экраны - это средства вычислительной техники, контролирующие разрешенный входящий сетевой трафик, а также трафик между сегментами локальной сети разного уровня критичности. Все системы должны быть защищены от неавторизованного доступа через интернет, будь то электронная коммерция, удаленный доступ своих работников через браузер или корпоративная почта. Часто кажущиеся малозначимыми каналы связи с внешней средой могут представлять собой незащищенные пути доступа к ключевым системам. Межсетевые экраны – это основные механизмы обеспечения безопасности любой компьютерной сети.

MICROS настоятельно рекомендует хранить все системы с конфиденциальной информацией **(**серверы, базы данных, беспроводные точки доступа, и пр.**)** за межсетевыми экранами для защиты этих данных и с целью соответствия Стандартам Совета **PCI-SSC.**

Чтобы быть уверенными в том, что конфигурация ваших сетевых экранов настроена в соответствии с Шагом **1** Стандарта **PCI DSS** "Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт", ознакомьтесь с вэб-сайтом Совета **PCI-SSC** **<http://pcisecuritystandards.org>**

2. Не использовать настройки системных паролей и других параметров безопасности данных, заданных производителем по умолчанию

Хакеры (как на стороне, так и внутри компании) для взлома систем часто прибегают к использованию паролей и других настроек , заданных производителями по умолчанию. Эти пароли и настройки хорошо известны в определенных сообществах и легко находятся через открытые источники информации.

MICROS рекомендует клиентам при установке систем поменять все дефолтовые пароли, включая те, что предназначены для операционных систем, беспроводных точек доступа, серверов, баз данных и пр. В **Opera** есть две дефолтовых учетных записи, пароли которых необходимо поменять, чтобы соответствовать комплексным требованиям к паролям, выдвигаемым Советом **PCI-SSC**; это учетная запись пользователя приложения: **SUPERVISOR** и учетные записи баз данных: **SYS, SYSTEM, OPERA, OXI, OXIHUB** и **OUTLN.**

Помимо этого, отдел **IT** и**/**или ответственные лица должны создать Пользователя Службы Поддержки **(Opera Support User) с**о всеми необходимыми полномочиями.

Стандарт **PCI-DSS** однозначно запрещает использование типовых или дефолтовых имен пользователей или паролей для входа в любой раздел платежной системы, включая учетные записи **Windows.** Любой доступ к любым разделам платежной системы должен предоставляться при условии ввода уникального и надежного имени пользователя и пароля со всеми необходимыми полномочиями.

Более подробно о Шаге **2** Стандарта **PCI DSS** "Не использовать настройки системных паролей и других параметров безопасности данных, заданных производителем по умолчанию", читайте на вэб-сайте Совета **PCI-SSC** **<http://pcisecuritystandards.org>**

Защита данных о держателях карт

3. Обеспечить безопасное хранение данных

Шифрование – это лучший механизм защиты, потому что даже если кто-то взломает все другие механизмы защиты и получит доступ к зашифрованным данным, он не сможет их прочитать, не имея ключа шифрования. Шифрование - пример принципа многоуровневой защиты.

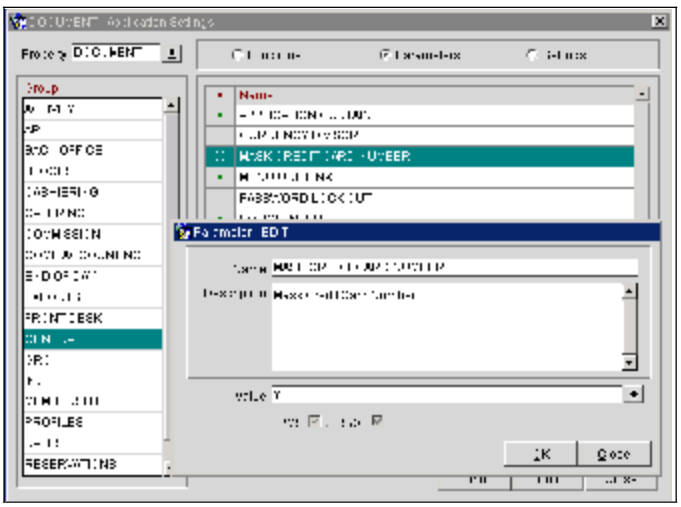
MICROS Systems Inc. использует маскировку данных кредитных карт и **128**-битное шифрование по алгоритму **Triple-DES** для хранения персонального номера учетной записи **(PAN),** имени учетной записи и даты истечения срока действия, что обеспечивает хранение данных кредитных карт в соответствии со Стандартом безопасности данных **PCI-DSS.**

При апгрейде с версии **Opera 2.0**, пожалуйста, ознакомьтесь с разделом "Руководство для проведения апгрейда с предыдущей версии **Opera**" **(***внизу этого документа***)**, в котором рассказывается о том, как выполнить апгрейд до новой версии, используя надежный инструмент очистки данных, и полностью удалить из **Opera** все старые данные кредитных карт.

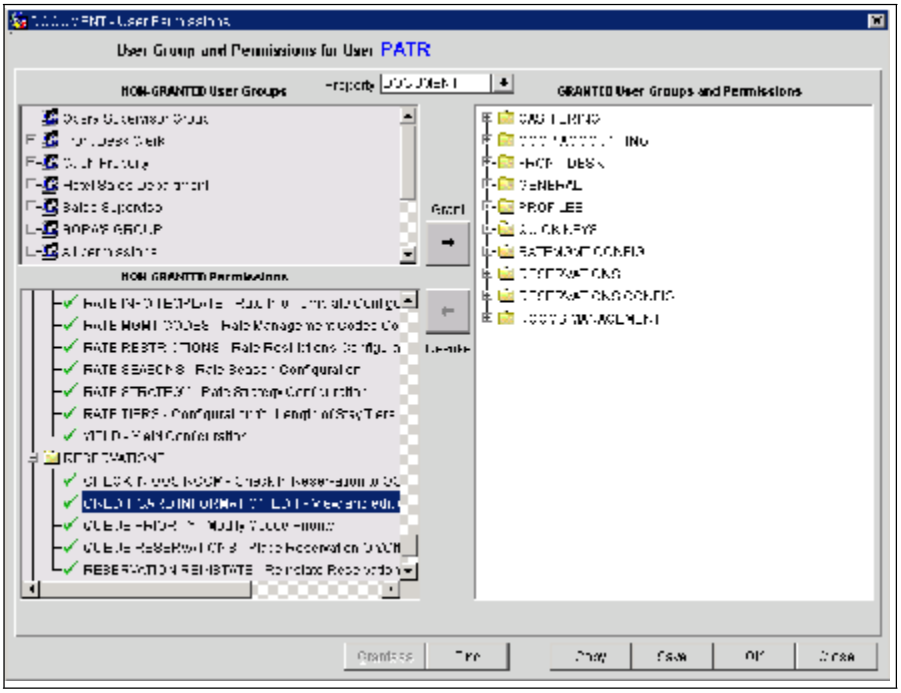
Чтобы соответствовать Шагу **3** Стандарта **PCI DSS,** пожалуйста, сконфигурите следующие опции маскировки данных кредитных карт:

Опционные настройки

- **Setup>Application Settings: Set General>MASK CREDIT CARD NUMBER (Mask Credit Card Number) to Yes.**



- **Setup>User Configuration>Users>Permissions: Set RESERVATIONS> CREDIT CARD INFORMATION EDIT (**Проверьте и измените номер кредитной карты и дату истечения срока действия**) to Non-Granted** для всех пользователей, кроме тех, кому положено знать. Таким пользователеям можно дать разрешение **Granted.**



***Прим: Для обеспечения соответствия Шагу 3** Стандарта PCI DSS, сохраняйте эти опции в той конфигурации, которая показано выше.*

Более подробно о Шаге **3** Стандарта **PCI DSS** "Обеспечить безопасное хранение данных", читайте на вэб-сайте Совета по развитию стандартов информационной безопасности индустрии платежных карт **<http://pcisecuritystandards.org>**

4. Обеспечить шифрование данных о держателях карт при их передаче через открытые сети общего пользования

Конфиденциальная информация, при передаче ее через интернет, должна зашифровываться, так как хакеру легко и просто перехватить и/или перенаправить такие данные.

MICROS рекомендует предварительно шифровать всю передаваемую через интернет конфиденциальную информацию, используя такой надежный тип шифрования, как например, протокол **SSLv3**; это касается всех беспроводных передач данных, электронной почты и сервисов, например, **Telnet** и **FTP.**

Опционные настройки

MICROS настоятельно рекомендует при использовании вэб-интерфейса **MICROS** с кредитными картами настраивать соединение по протоколу **SSLv3.** Для его конфигурации, выполните следующее. Выберите **Configuration > Setup > Property Interfaces > Credit Card Setup > General Parameters.** В открывшейся форме вы увидите раздел для конфигурации **URL** подключения. Убедитесь в том, что **URL** начинается с названия протокола **HTTPS,** который обеспечивает надежное **SSLv3 со**единение с производителем до передачи данных кредитных карт.

Более подробно о Шаге **4** Стандарта **PCI-DSS** "Обеспечить шифрование данных о держателях карт при их передаче через открытые сети общего доступа", читайте вэб-сайт Совета по развитию стандартов информационной безопасности индустрии платежных карт **<http://pcisecuritystandards.org>**

Программа управления уязвимостями

5. Использовать и регулярно обновлять антивирусные программы

Много уязвимостей и вредоносных вирусов попадает в сеть через электронную почту. Чтобы защититься от них, антивирусные программы должны быть установлены на всех почтовых системах и рабочих столах.

В соответствии со стандартами Совета по развитию стандартов информационной безопасности индустрии платежных карт **(PCI-SSC), MICROS** настоятельно рекомендует постоянно использовать и регулярно обновлять антивирусные программы. Конфигурация некоторых серверов OPERA требует специальных антивирусных настроек; эти настройки подробно описываются в соответствующих инструкциях.

Чтобы убедиться в том, что ваша антивирусная программа настроена в соответствии с Шагом **5** Стандарта **PCI DSS** "Использовать и регулярно обновлять антивирусные программы", озакомьтесь с вэб-сайтом Совета **PCI – SSC** <http://pcisecuritystandards.org>

6. Разрабатывать и поддерживать системы и приложения безопасности

Злоумышленники используют уязвимости в защите для проникновения в системы. Многие из этих уязвимостей устраняются обновлениями безопасности, выпускаемыми производителем, поэтому все системы должны обновляться актуальными программными патчами, защищающими от злоумышленных действий работников, сторонних хакеров и вирусов. Что касается приложений, являющихся продуктом собственных рабработок, то здесь многочисленных уязвимостей можно избежать, используя стандартные процессы разработки систем и защитное кодирование.

Для обеспечения программной целостности и безопасности **MICROS** использует отдельные среды для разработок и для производства. Обновляемые патчи, в том числе обновления безопасности, доступны на вэб-сайте **MICROS** <http://www.micros.com>. В то время как **MICROS** прилагает все возможные усилия к тому, чтобы соответствовать Шагу **6** Стандарта **PCI DSS**, некоторые параметры, в том числе процедуры изменений конфигураций систем и программ, а также установка доступных обновлений безопасности, зависят от специфической практики и политики того или иного сайта.

MICROS также настоятельно рекомендует при установках на оперативной системе **Windows XP** отключать функциональность Точек Восстановления Системы.

Чтобы убедиться в том, что ваш сайт разрабатывает и поддерживает системы и приложения безопасности в соответствии с Шагом **6** Стандарта **PCI DSS** "Разрабатывать и поддерживать системы и приложения безопасности", ознакомьтесь с содержанием вэб-сайта Совета **PCI – SSC** <http://pcisecuritystandards.org>

Внедрение строгих мер контроля доступа

7. Ограничить доступ к данным служебной необходимостью

Доступ к критическим данным предоставляется только авторизованным пользователям.

MICROS признает важность контроля доступа к данным и осуществляет этот контроль, предоставляя доступ в зависимости от уровня должности работника. Этот механизм позволяет ограничить доступ к конфиденциальной информации необходимым для выполнения должностных обязанностей объемом знаний и защитить пароли.

Более подробно о Шаге **7** Стандарта **PCI DSS** "Ограничить доступ служебной необходимостью", читайте на вэб-сайте Совета **PCI – SSC** <http://pcisecuritystandards.org>

8. Привязать уникальный идентификатор каждому, у кого есть доступ к ПК

Такая привязка гарантирует, что действия с критическими данными и системами выполняются известными и авторизованными пользователями и могут отслеживаться.

MICROS признает важность привязки уникального идентификатора каждому работнику, имеющему доступ к компьютеру. Два разных пользователя **OPERA** не могут иметь одинаковый идентификатор, что позволяет отслеживать действия каждого при условии, что сайт клиента поддерживает должную конфигурацию и ограничивает уровни привилегий работников служебной необходимостью. В то время как **MICROS** прилагает все возможные усилия к тому, чтобы соответствовать Шагу **8** Стандарта **PCI DSS**, некоторые параметры, в т.ч. аутентификация пользователя, удаленный доступ к сети и управление паролями для производственно-технического персонала и администраторов, а также для всех системных компонентов, зависят от специфической практики и политики того или иного сайта.

Для соответствия Шагу **8** Стандарта **PCI DSS**, мы рекомендуем сделать следующее.

- Убедитесь в том, что поле "Дней до даты истечения срока действия пароля" на экране **Edit User** настроено на значение, не превышающее **90**.
- Убедитесь в том, что длина паролей пользователей насчитывает не менее **7** знаков.
- Убедитесь в том, что пароли пользователей содержат как буквенные, так и цифровые символы.
- Кодируйте все пароли при передаче данных, используя кодировку, как например, протокол **SSLv3. Micros** НАСТОЯТЕЛЬНО рекомендует всегда использовать **SSLv3. (**О конфигурации сервера **Opera** для доступа по протоколу **HTTPS**, читайте **"Opera – Configure Opera for SSL".pdf)**

Подробнее о Шаге **8** Стандарта **PCI DSS** "Привязать уникальный идентификатор каждому, у кого есть доступ к ПК", смотрите вэб-сайт Совета по развитию стандартов информационной безопасности индустрии платежных карт **<http://pcisecuritystandards.org>.**

9. Ограничить физический доступ к данным о держателях карт

Любой физический доступ к данным или системам с данными о держателях карт создает условия для доступа к устройствам или информации, с возможностью удалить систему или бумажную копию документа, и должен быть надлежащим образом ограничен.

В соответствии со стандартом Совета **PCI-SSC, MICROS** настоятельно рекомендует ограничивать физический доступ к данным о держателях карт.

Чтобы убедиться в том, что ваш сайт настроен в соответствии с Шагом **9** Стандарта **PCI DSS** "Ограничить физический доступ к данным о держателях карт", ознакомьтесь с вэб-сайтом Совета **PCI-SSC <http://pcisecuritystandards.org>.**

Регулярный мониторинг и тестирование сети

10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт

Механизмы ведения записей о событиях, а также возможность отслеживать действия пользователей совершенно необходимы. Наличие записей во всех средах позволяет провести тщательное расследование и проанализировать инциденты. Определить причину инцидентов, если отсутствуют записи событий, очень трудно.

MICROS включает в **OPERA** всеобъемлющую аудиторскую утилиту, позволяющую привилегированным пользователям отслеживать события в **OPERA.** Появление структур с открытой базой данных означает, что любой пользователь с системным уровнем доступа к серверу базы данных **(Oracle)**, имеет также доступ к системным компонентам, а следовательно, его вход и действия протоколируются, как описано в Шаге **10** Стандарта **PCI DSS.** В соответствии со стандартом Совета **PCI-SSC, MICROS** настоятельно рекомендует вести записи событий на сервере базы данных.

Чтобы убедиться в том, что ваш сайт соответствует Шагу **10** Стандарта **PCI DSS** "Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт", смотрите вэб-сайт Совета **PCI-SSC <http://pcisecuritystandards.org>.**

11. Регулярно тестировать системы и процессы информационной безопасности

Уязвимости то и дело обнаруживаются хакерами/разработчиками, а также появляются вместе с новыми программными продуктами. Системы, процессы и написанные на заказ программы необходимо часто тестировать, чтобы быть уверенными в их защищенности по мере того, как идет время и вносятся изменения.

В соответствии со стандартами Совета по развитию стандартов информационной безопасности индустрии платежных карт **(PCI-SSC), MICROS** настоятельно рекомендует регулярно тестировать системы и процессы безопасности.

Чтобы убедиться в том, что системы и процессы безопасности вашего сайта настроены в соответствии с Шагом **11** Стандарта **PCI-DSS** "Регулярно тестировать системы и процессы информационной безопасности", откройте вэб-сайт Совета **PCI-SSC** **<http://pcisecuritystandards.org>.**

Поддержание политики информационной безопасности

12. Поддерживать политику информационной безопасности

Строгая политика информационной безопасности задает нужный тон в компании в целом и дает работникам представление о том, что от них ожидается. Все работники должны быть осведомлены о конфиденциальности данных и своей ответственности по их защите.

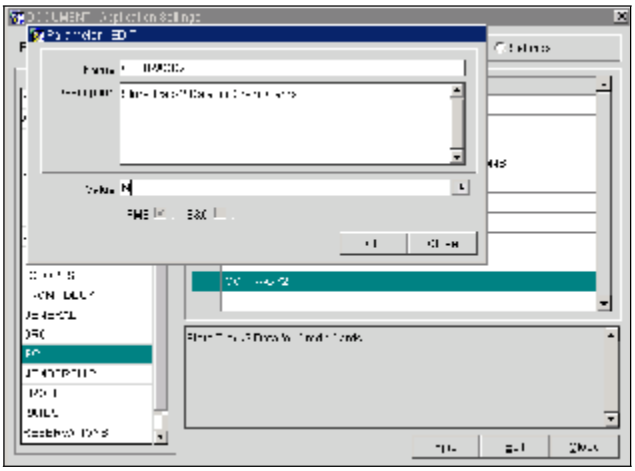
В соответствии со стандартами Совета **PCI-SSC, MICROS** настоятельно рекомендует поддерживать политику информационной безопасности.

Чтобы убедиться в том, что ваша политика информационной безопасности настроена в соответствии с Шагом **12** Стандарта **PCI DSS** "Поддерживать политику, направленную на информационную безопасность", откройте вэб-сайт Совета **PCI-SSC** **<http://pcisecuritystandards.org>.**

Руководство для апгрейда с предыдущей версии **Opera**

I. Отключение функциональности Дорожки 2

Чтобы соответствовать требованиям Совета **PCI-SSC,** при апгрейде с предыдущей версии до версии **Opera 4.0,** сначала в предыдущей версии надо выключить параметр **CC_TRACK2.**



В результате будут удалены данные **2**-ой дорожки из базы данных **Opera.** Чтобы отключить этот параметр в версии **Opera 3.0,** выберите **Setup > Application Settings,** и, как показано ниже, выставите для параметра **IFC Group Application** значение **No.**

II. Обновление Базы Данных

Для обновления базы данных выполните следующие шаги:

1. Создание новой схемы **Oracle 10g** для **Opera 4.0.**
   a. Используйте установочный диск для установки базы данных **Opera V4.0.3.**
   b. Удалите схему **Opera** из базы данных, подключившись к **SQLPLUS** под **SYS.**
      i. Удалите каскадное расположение окон **Opera** пользователя.
2. Экспорт схемы **Opera** из Базы Данных **9i.**
   a. Для экспорта схемы используйте **Opera_SMT.**
3. Импорт схемы **Opera** в объект **10g**
   a. Используйте **Opera_SMT,** чтобы импортировать схему двойным кликом по **EXE,** сгенеренному с помощью Экспорта.
4. Апгрейд схемы **Opera** до версии **4.0**
   a. Запустите мега-патч **Executable** для соответствующей версии. **Executables** доступны на вэб-сайте **Micros.** Загрузите файл, соответствующий версии **9i**
5. Полный бэкап
   a. Закройте базу данных
   b. Скопируйте все файлы из каталога **d:\oracle\oradata\opera,** в каталог бэкапа
   c. Скопируйте файл **initopera.ora** из каталога **d:\oracle\1020\database (**или каталога **d:\oracle\admin\opera\pfile),** в каталог бэкапа.
6. Удалите все файлы **Oracle 9i** с помощью надежного инструмента очистки данных **(**Выбор этих инструментов носит случайный характер, и мы не может рекомендовать тот или иной**).**
   - **http://www.clean-space.com/privacy/about/secure-wipe.html**
   - **http://www.softsea.com/review/EZ-Wipe.html**
   - **http://tucows.menanet.net/fileremove95_default.html**

Внедрение и поддержание политики хранения данных

Стандарт **PCI-DSS** гласит: "Храните данные о держателях карт в минимальном объеме. Разработайте политику хранения и удаления данных. Ограничьте объем и длительность хранения служебной необходимостью, юридическими и/или нормативными требованиями, как это задокументировано в политике хранения данных. Разработка и внедрение Политики Хранения Данных **(DRP) -** важный фактор глобальной безопасности вашей среды.

Политика хранения данных создает важный фундамент, помогающий управлять данными организации. Создание Политики – комплексная задача, требующая тщательного

исследования и содействия со стороны квалифицированных юристов. Границы вашей **DRP** должны выходить за рамки Стандарта **PCI-DSS.** Вы должны работать в тесном контакте с юристами, чтобы обеспечить соблюдение законов и государственных нормативных актов, имеющих отношение именно к вашему типу организации.

После внедрения своей Политики Хранения Данных **(DRP),** вам следует заключить договор с утвержденной Советом **PCI-SSC** организацией на проведение оценочной экспертизы на соответствие вашей **DRP "**Требованиям и Процедурам Оценки безопасности данных в индустрии платежных карт**", V. 1.2, О**ктябрь**, 2008**г. Контролирующая организация должна проверить, насколько ваша Политика Сохранения Данных **(DRP)** соответствует Требованию **#3** стандарта **PCI DSS** в части хранения данных платежных карт.

Интерфейсы с третьими сторонами

Интерфейсы с третьими сторонами нужны для установления взаимоконтакта между неким продуктом **MICROS Systems, Inc. (MICROS)** и продуктами некоей третьей стороны, которые не разрабатывались и не контролировались **MICROS (**Продукты не**-MICROS).** Эти продукты, не имеющие отношения к **MICROS,** могут соответствовать, а могут и не соответствовать Стандарту безопасности данных для платежных приложений индустрии платежных карт **(PA-DSS). MICROS** настоятельно рекомендует всем торгово-сервисным предприятиям, занимающимся написанием интерфейсов между продуктами **MICROS,** участвующими в обработке платежей, и продуктами не**-MICROS,** заручиться гарантией того, что продукты обеих сторон **– MICROS** и не-М**ICROS –** соответствуют требованиям стандарта **PA-DSS.**