OPERA версия 4.0+ Руководство PABP и соблюдение Стандарта Защиты Данных PCI

Общая информация

Об Этом Документе

Настоящий документ представляет собой краткое руководство, содержащее информацию о соблюдении **MICROS Systems, Inc.** стандарта безопасности данных индустрии платежных карт, утвержденного **Visa USA,** в части соответствия Программе безопасности данных держателей карт **(CISP).** Этот документ относится исключительно к программному продукту ***OPERA Version 4.0+ Enterprise Solution software***, в т.ч. **Opera Property Management, Opera Limited Service (Xpress), Opera Xpress Lite (Lite)** и **Opera Reservation System.**

О соответствии Программе CISP

Когда клиенты расплачиваются с помощью банковской карточки в точках продаж или совершают покупки через интернет, по телефону или электронной почте, они хотят быть уверенными в безопасности своего банковского счета. Вот почему **Visa** в США и **VISA** в Европе внедрили Программу Безопасности Данных Держателей Карт **(CISP).** Запущенная в июне **2001** года, эта программа призвана защитить данные держателей карт **Visa** —независимо от места—и обеспечить поддержание самого высокого **1-**го уровня информационной безопасности со стороны членов-участников, торгово-сервисных предприятий и провайдеров услуг.

Более подробно о соответствии Программе **CISP** читайте на вэб-сайте **Visa USA:** **http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html**

О защите данных индустрии платежных карт

Соответствие Программе безопасности данных держателей карт **(CISP)** требуется со стороны всех торгово-сервисных предприятий и провайдеров услуг, которые хранят, обрабатывают или передают данные о держателях карт **Visa.** Эта программа касается всех каналов оплат, включая розничную торговлю через торговые точки, заказы товаров по электронной почте/телефону и интернет-коммерцию. . Чтобы соответствовать Программе **CISP,** торгово-сервисные предприятия и провайдеры услуг должны соблюдать Стандарт безопасности данных индустрии платежных карт **(PCI-DSS),** определяющий единый подход к обеспечению безопасности конфиденциальных данных для всех платежных брендов карточного рынка. Этот представляет собой результат совместного сотрудничества между **Visa** и **MasterCard** и призван создать общие для индустрии требования безопасности, включая требования **CISP.** Другие карточные бренды, ведущие бизнес в США, также одобрили Стандарт **PCI-DSS** и реализовали его в своих программах. Взяв за основу Стандарт **PCI-DSS,** Программа **CISP** предлагает инструменты и меры защиты против утечки информации и компрометации карт для всей индустрии **PCI.**

[1] **Reprinted from "Cardholder Information Security Policy", <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>.**

Стандарт **PCI-DSS,** описанный ниже**,** включает двенадцать основных требований**,** которые детализируются дополнительными требованиями**:**[2]

Стандарт **PCI-DSS** является результатом совместного сотрудничества между **Visa, MasterCard, AMEX, Discover** и **JCB,** целью которого было создать общие для индустрии требования безопасности**.** Другие карточные бренды**,** ведущие бизнес в США**,** также одобрили Стандарт **PCI-DSS** и реализовали его в своих программах**.**
Эти нижеописанные **12** требований положены в основу Программы **CISP Visa.**

Стандарт PCI-DSS

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

---

[2] **Reprinted from "CISP_overview.pdf", <http://usa.visa.com/download/business/accepting_visa/support_center/cisp_overview.pdf?it=c|/business/accepting_visa/ ops_risk_management/cisp%2Ehtml|CISP%20Overview>.**

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**
• Умение работать с периферийными устройствами **MICROS**

OPERA версия 4.0+ и Стандарт Защиты Данных PCI

Стандарт Защиты Данных PCI

В то время как **MICROS** признает важность поддержания безопасности и целостности данных о держателях платежных карт, некоторые параметры Стандарта **PCI DSS** и **с**оответствия **CISP** остаются исключительной ответственностью клиента. Настоящий раздел содержит описание **12** пунктов Стандарта **PCI-DSS.** Информация в этом разделе касается только соответствия программного продукта **OPERA V4.0** Стандарту **PCI DSS**

Полное описание Стандарта **PCI-DSS** можно найти на вэб-сайте **Visa USA** в разделе **"Cardholder Information Security Plan"**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

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.[3]

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 Плана безопасности данных о держателях платежных карт**,** разработанных **Visa.**

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 **Visa USA**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

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.[4]

---

[3] **"Payment Card Industry Standard Audit Procedures.doc", p. 5, V. 1.0, December 15, 2004.<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.**

https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm

[4] **"Payment Card Industry Security Audit Procedures.doc", p. 10, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.**

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 **CISP**; 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.

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 **Visa USA** раздел **"Cardholder Information Security Policy"**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

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.[5]

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.**

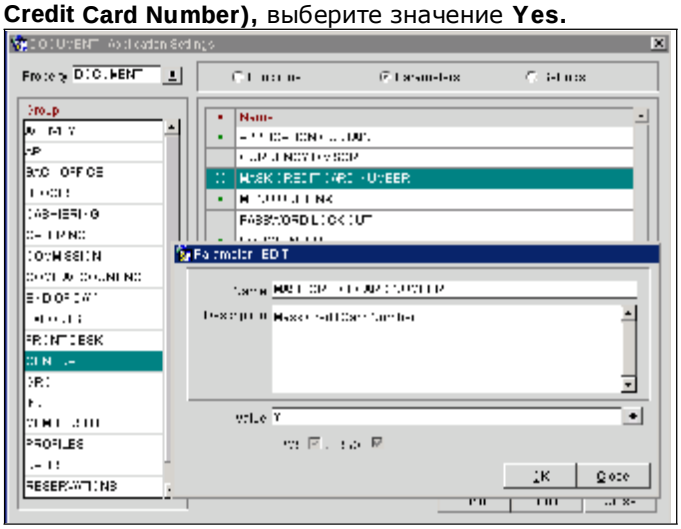
При апгрейде с версии **Opera 2.0**, пожалуйста, ознакомьтесь с разделом "Руководство для проведения апгрейда с предыдущей версии **Opera" (***внизу этого документа***)**, в котором рассказывается о том, как выполнить апгрейд до новой версии, используя надежный инструмент очистки данных, и полностью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

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

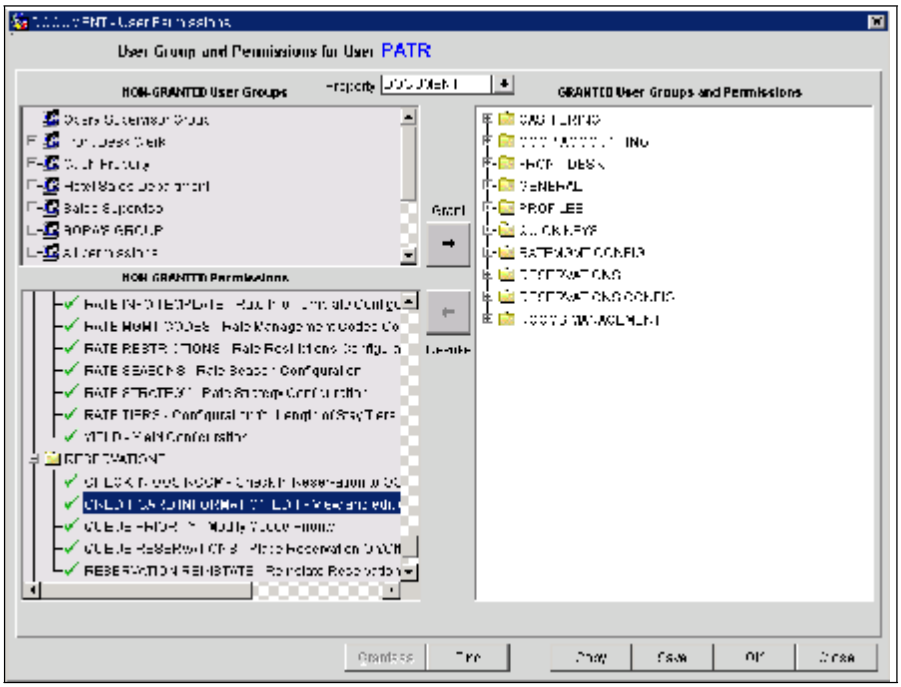
[5] **"Payment Card Industry Security Audit Procedures.doc", p. 13, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.**

Опционные настройки

- **Setup>Application Settings:** Откройте **General>MASK CREDIT CARD NUMBER (Mask Credit Card Number),** выберите значение **Yes.**



- **Setup>User Configuration>Users>Permissions:** В **RESERVATIONS> CREDIT CARD INFORMATION EDIT (**Проверьте и измените номер кредитной карты и дату истечения срока действия**)** выберите **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 **Visa USA** раздел **"Cardholder Information Security Policy"**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

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.[6]

MICROS рекомендует предварительно шифровать всю передаваемую через интернет конфиденциальную информацию, используя такой надежный тип шифрования, как например, **VPN** или **SSL;** 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 **SSL.** 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 **SSL** соединение 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 на вэб-сайте **Visa USA** раздел **"Cardholder Information Security Policy"**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

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.[7]

В соответствии со стандартом **PCI-DSS Visa USA, 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", ознакомьтесь на вэб-сайте **Visa USA** с разделом **"Cardholder Information Security Policy"**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

---

[6] **"Payment Card Industry Security Audit Procedures.doc", p. 18, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.**

[7] **"Payment Card Industry Security Audit Procedures.doc", p. 20, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.**

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.[8]

Для обеспечения программной целостности и безопасности **MICROS** использует отдельные среды для разработок и для производства. Обновляемые патчи, в т.ч. 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 т.ч. процедуры изменений конфигураций систем и программ, а также установка доступных обновлений безопасности, зависят от специфической практики и политики сайта.

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", читайте на вэб-сайте **Visa USA** раздел **"Cardholder Information Security Policy"** **http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html**

Внедрение строгих мер контроля доступа

7. Ограничить доступ к данным служебной необходимостью

Доступ к критическим данным предоставляется только авторизованным пользователям.[9]

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 **Visa USA** раздел **"Cardholder Information Security Policy»**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

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.[10]

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.

---

[8] **"Payment Card Industry Security Audit Procedures.doc", p. 21, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.**

[9] **"Payment Card Industry Security Audit Procedures.doc", p. 26, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.**

[10] **"Payment Card Industry Security Audit Procedures.doc", p. 27, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.**

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**
- 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 **SSL (**О конфигурации сервера **Opera** для доступа по протоколу **HTTPS**, читайте **"OperaV403 – Configure Opera for SSL".pdf)** или используйте сетевую инфраструктуру, как например, защищенная **VPN** или что-то подобное.

Подробнее о Шаге **8** Стандарта **PCI-DSS** "Привязать уникальный идентификатор каждому, у кого есть доступ к ПК", читайте на вэб-сайте **Visa USA** раздел **"Cardholder Information Security Policy"**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

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.[11]

В соответствии со стандартом **PCI-DSS Visa USA, 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", читайте на вэб-сайте **Visa USA** раздел **"Cardholder Information Security Policy»**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

Регулярный мониторинг и тестирование сети

10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях 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.[12]

---

[11] **"Payment Card Industry Security Audit Procedures.doc", p. 33, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.**

[12] **"Payment Card Industry Security Audit Procedures.doc", p. 37, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.**

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 на вэб-сайте **Visa USA** раздел **"Cardholder Information Security Policy"**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

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.[13]

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", читайте на вэб-сайте **Visa USA** раздел **"Cardholder Information Security Policy"**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

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.[14]

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", читайте на вэб-сайте **Visa USA** раздел **"Cardholder Information Security Policy"**
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

---

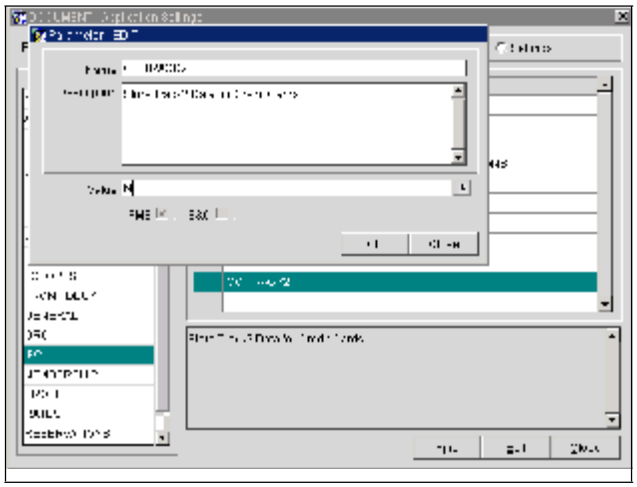
[13] **"Payment Card Industry Security Audit Procedures.doc", p. 41, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.**

[14] **"Payment Card Industry Security Audit Procedures.doc", p. 44, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.**

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



II. Обновление Базы Данных

Для обновления базы данных выполните следующие шаги:

1. **C**оздание 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. **С**копируйте все файлы из каталога **d:\oracle\oradata\opera,** в каталог бэкапа

c. **С**копируйте 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**