9700 HMS версия 3.20 Соответствие Требованиям платежного бренда Visa к платежным приложениям

Общая Информация

Об этом Документе

Настоящий документ представляет собой краткое руководство, содержащее информацию о соответствии MICROS Systems, Inc. Стандарту Защиты Данных Индустрии Платежных Карт (PCI DSS) и Требованиям к Платежным Приложениям, утвержденным платежным брендом Visa (PABP). Этот документ относится исключительно к программному продукту *MICROS 9700 версии 3.20 Hospitality Management System.*

О соответствии требованиям PCI

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 был введен Стандарт Защиты Данных Индустрии Платежных Карт **(PCI DSS).** Эта программа призвана защищить данные о держателях карт —независимо от места нахождения этих данных— и обеспечить поддержание самого высокого уровня стандарта информационной безопасности со стороны членов-участников, торгово-сервисных предприятий и провайдеров услуг[1].

Более подробно о соответствии требованиям **PCI** читайте на вэб-сайте Совета по развитию стандартов информационной безопасности индустрии платежных карт **(PCI SSC),** https://www.pcisecuritystandards.org/.

1. Reprinted from “Cardholder Information Security Program”, <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>.

О стандарте Защиты Данных PCI

Соответствие стандарту индустрии платежных карт **(PCI)** требуется со стороны всех торгово-сервисных предприятий и провайдеров услуг, которые хранят, обрабатывают или передают данные о держателях карт. Эта программа касается всех каналов оплат, включая розничную торговлю через торговые точки, заказы товаров по электронной почте/телефону и интернет-коммерцию. Чтобы соответствовать требованиям **PCI**, торгово-сервисные предприятия и провайдеры услуг должны соблюдать Стандарт **PCI-DSS**, определяющий единый подход к обеспечению безопасности конфиденциальных данных для всех платежных брендов карточного рынка. Этот стандарт представляет собой результат совместного сотрудничества индустрии **PCI** и и призван создать общие для индустрии требования безопасности, включающие требования **PCI**.

Взяв за основу Стандарт **PCI-DSS**, индустрия **PCI** разработала и предлагает инструменты и меры защиты против утечки информации и компрометации карт для всей своей индустрии.
Стандарт **PCI-DSS**, описанный ниже, включает двенадцать основных требований, которые детализируются дополнительными требованиями:[2]

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:

- Установщики/Программисты **MICROS**
- Дилеры **MICROS**
- Служба Поддержки Клиентов **MICROS**
- Обучающий персонал **MICROS**
- Персонал **MIS**
- Пользователи **9700**

Необходимые предварительные знания

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

- Умение работать с ПК
- Понимание базовых сетевых концепций
- Опыт работы с **Microsoft Windows 2000** или **Windows 2003**
- Знакомство с программным продуктом **9700 HMS**
- Опыт работы с периферийными устройствами **MICROS**

9700 HMS версия 3.20 и Стандарт Защиты Данных PCI

В то время как **MICROS Systems Inc.** признает важность поддержания безопасности и целостности данных о держателях платежных карт, некоторые параметры Стандарта **PCI-DSS** и того, что касается соблюдения требований **PCI**, остается исключительной ответственностью клиента. Настоящий раздел содержит описание **12** пунктов Стандарта **PCI-DSS**. Информация в этом разделе касается только соответствия программного продукта 9700 HMS версии 3.20 Стандарту защиты данных индустрии платежных карт (PCI).

Поскольку платежное приложение должно работать в условиях защищенной сети, 9700 HMS не вмешивается в использование **NAT**, **PAT**, сетевого устройства фильтрации трафика, анти-вирусной защиты, установку патчей и обновлений, а также шифрование.

Более подробно о Стандарте **PCI DSS** читайте на вэб-сайте Совета **PCI SSC**, https://www.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.[3]

В соответствии со Стандартом **PCI DSS**, **MICROS Systems Inc.** настаивает на том, чтобы все объекты, в т.ч. те, что работают с беспроводными сетями, установили и поддерживали межсетевые экраны для защиты данных. Сконфигурите вашу сеть так, чтобы базы данных и беспроводные точки доступа *всегда* располагались за межсетевыми экранами и не имели прямого доступа к Интернету.

Персональный защитный экран в виде ПО должен быть установлен на всех переносных и персональных компьютерах работников, где есть прямой выход в интернет, например, на ноутбуках, используемых работниками для доступа к сети организации. Работники не должны иметь возможности изменять конфигурационные настройки защитного экрана.

3. "Payment Card Industry (PCI) Data Security Standard.doc", p. 4, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

С целью соблюдения Стандарта **PCI DSS, MICROS Systems Inc.** настаивает на том, чтобы серверы, базы данных, беспроводные точки доступа и любые среды с конфиденциальными данными на всех объектах находились за межсетевыми экранами. Конфигурация межсетевого экрана должна ограничивать соединения между серверами общего пользования и любыми системными компонентами, хранящими данные о держателях карт, включая любые беспроводные соединения.

Конфигурация межсетевого экрана должна учитывать размещение базы данных во внутренней сети, отделенной от демилитаризованной зоны **(DMZ)** вэб-сервером. Демилитаризованная зона может использоваться для отделения Интернета от систем хранения данных о держателях карт.

В целях соблюдения требований **PCI, 9700 HMS** не настаивает на том, чтобы сервер базы данных и вэб-сервер были одним и тем же сервером.

Чтобы убедиться в том, что ваш межсетевой экран настроен в соответствии с Требованием **1** Стандарта **PCI DSS, "**Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт**»,** читайте вэб-сайт Совета **PCI SSC** https://www.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.[4]

Установки предыдущих версий **9700 3.x** предполагали создание четырех дефолтовых учетных записи**: "9700cfg" "csremote" "micros"** и **"m9700." MICROS Systems, Inc.** ранее советовала удалять, переименовывать или отключать эти дефолтовые учетные записи. Теперь, чтобы обеспечить полную безопасность и соответствие требованиям **PCI,** в программе **9700 v. 3.20** эти учетные записи изменены или удалены.

Старые учетные записи **"micros"** и **"csremote"** больше не будут использоваться и создаваться. Они удалены из процедуры установки, так как в случае ненадежного удаления могли вступать в противоречение с требованиями **PCI.** При апгрейде до **9700 v. 3.20** с предыдущей версии, эти учетные записи будут отключены после завершения процедуры апгрейда.

Старая учетная запись **"m9700"** будет отключена после завершения процедуры установки**/**апгреда до **9700 v. 3.20.**

4. "Payment Card Industry (PCI) Data Security Standard.doc", p. 5, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Учетная запись **"9700cfg"** используется для удаленного входа в Удаленную Консоль Управления **(RMC).** Эта учетная запись будет отключена после завершения процедуры установки**/** апгрейда до **9700 v. 3.20.** Если в системе **9700** используется функциональность транзакций по платежным картам**,** то эта учетная запись должна быть удалена**,** а опции безопасности на уровне домена должны быть включены во время установки**/**апгрейда **9700,** как показано ниже.

Более подробное описание можно найти в документе *9700 Secure Default Account Handling*

MICROS Systems, Inc. не рекомендует использовать учетные записи администратора**,** типа **"sa",** для доступа к базе данных и входа в приложение**.** Клиентам и дилерам**/**специалистам по системной интеграции рекомендуется всегда привязывать надежные пароли к подобным дефолтовым учетным записям**,** даже если эти учетные записи не используются**.** Позднее**,** эти дефолтовые учетные записи должны быть отключены или перестать использоваться.

Надежные системные пароли и пароли для входа в приложение должны использоваться всегда**,** когда это возможно**. MICROS Systems, Inc.** настаивает на том**,** чтобы клиенты и дилеры**/** специалисты по системной интеграции всегда создавали соответствующие требованиям Стандарта **PCI DSS** комплексные пароли для входа в платежное приложение**.** Более подробно о том**,** как создавать пароль в соответствии с требованиями **PCI** для входа в Консоль Управления Предприятием **(EMC),** читайте на стр. 13.

При использовании беспроводных сред измените дефолтовые настройки производителей**,** включая**,** но не ограничиваясь**,** следующим**:** ключи к беспроводным протоколам защиты данных **(WEP),** дефолтовый идентификатор беспроводной сети **(SSID),** дефолтовые пароли и строки имени и пароля **SNMP.** Отключите **SSID broadcasts** и включите технологию **Wi-Fi** защищенного доступа **(WPA2)** для шифрования и аутентификации

Более подробное описание можно найти в документе *MICROS Wireless Networking Best Practices: A Payment Application Best Practices (PABP) Implementation Guide Supplement.*

Все вне**-**консольные входы под администратором должны шифроваться с использованием технологий **SSH, VPN** или **SSL/RLS (**протокол **TLS),** независимо от целей**:** будь то управление через интернет или другое**.** Ни **Telnet,** ни **rlogin** никогда не должны использоваться для администрирования**.**

Более подробно о Требовании **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** https://www.pcisecuritystandards.org/.

Защита данных о держателях карт

3. Защита данных о держателях карт

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 платежных карт и **128-**битное шифрование по алгоритму **Triple-DES** для обеспечения хранения данных карт в соответствии со Стандартом безопасности данных **PCI-DSS.**

Для защиты данных и в соответствии с требованиями **PCI,** производственные системы **9700 HMS** никогда не должны располагаться непосредственно в Интернете, а между системой **9700 HMS** и корпоративными интернет-шлюзами всегда должен быть межсетевой экран.

9700 HMS не позволяет распечатывать назашифрованные данные платежных карт в чеках гостей, а также отображать их на рабочих станциях, в квитанциях клиентов и журналах, что соответствует Требованию **3** Стандарта **PCI DSS.** Отображаются только последние четыре цифры номера **PAN**.

Архивные данные **(**данные магнитной полосы, валидационные коды карт, номера **PIN** или блоки **PIN),** сохранявшиеся предыдущими версиями **9700,** должны быть надежно удалены, для соблюдения требований P**CI.** Любой криптографический материал, например, ключи шифрования или верификация данных о держателях карт, или конфиденциальные данные аутентификации, сохранявшиеся предыдущими версиями ПО, также должны быть надежно удалены, в соответствии с требованиями **PCI.**

Переход с **9700 v2.x** на **9700 v3.x** должен, следовательно, завершаться надежным удалением старой базы данных с плоскими файлами и всех старых лог-файлов. Архивные данные должны быть надежно удалены, где бы они ни находились. Апгрейд **9700** самостоятельно после конверсии исходной базы данных зашифрует всю конфиденциальную информацию в базе данных **3.2.** Более подробное описание можно найти в документе ***9700 Upgrade Best Practices*.**

5. “Payment Card Industry (PCI) Data Security Standard.doc”, p. 6, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

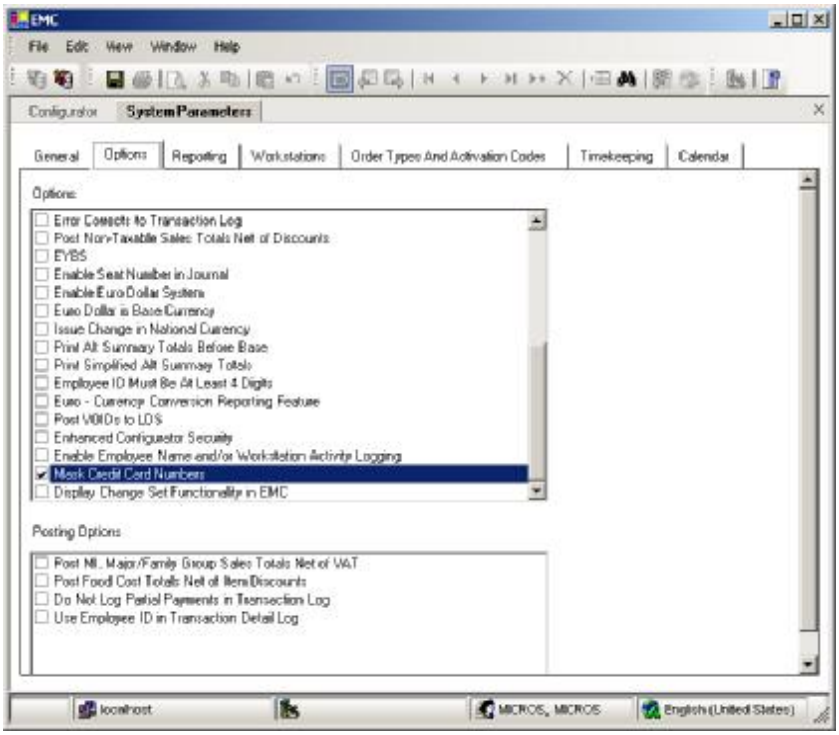
В целях защиты данных о держателях карт, **MICROS Systems, Inc.** настаивает на том, чтобы дилеры/ специалисты по системной интеграции **9700 HMS** собирали только те данные клиентов (например, конфиденциальные данные аутентификации, лог-файлы, отладочные файлы, базы данных и т.п.), которые необходимы для решения конкретной проблемы. Такие данные необходимо хранить только в специальном, знакомом месте с ограниченным доступом. Дилеры/ специалисты по системной интеграции должны собирать только ограниченный объем данных, действительно необходимый для решения конкретной проблемы, и при хранении шифровать такие конфиденциальные данные аутентификации. Когда данные больше не нужны, их необходимо сразу же и надежно удалить. Более подробную информацию можно найти в документе *Customer Support Information Security Guidelines*.

Для обеспечения соответствия Требованию **3** Стандарта **PCI DSS**, убедитесь в том, что следующие опции сокрытия данных платежных карт в Консоли Управления Предприятием **(EMC)** сконфигурены, как показано ниже.

Включенная Опция

Следующая опция включена по умолчанию:

- **System Information>Parameters>Options Tab>Options Section:** Mask Credit Card Numbers

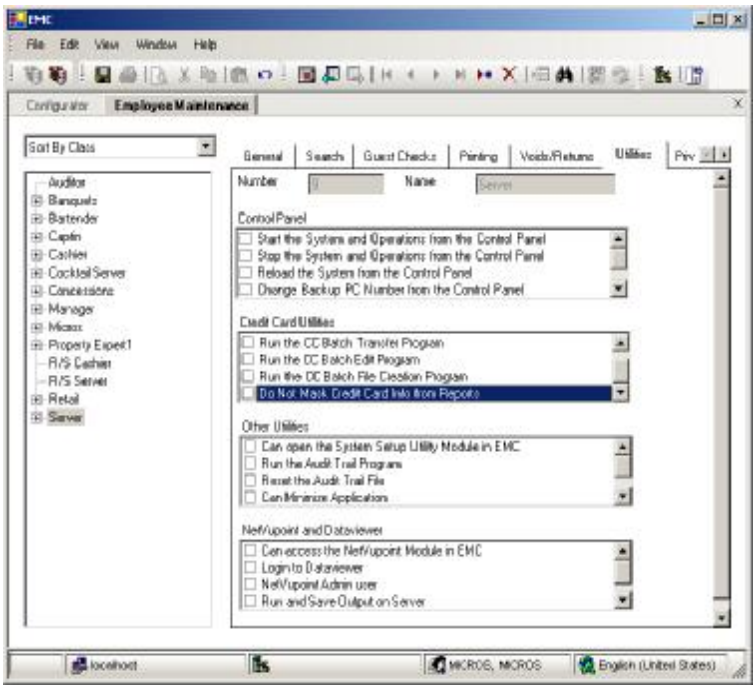


Прим *Для обеспечения соответствия Требованию 3 Стандарта PCI DSS, сохраняйте эти опции в той конфигурации, как она показана выше.*

Отключенная Опция

Следующая опция отключена по умолчанию:

- **Personnel>Employees>Maintenance>Select Employee Class>Utilities Tab>Credit Card Utilities:** Do Not Mask CC Info from CC Reports



Прим *Для обеспечения соответствия Требованию 3 Стандарта PCI DSS, сохраняйте эти опции в той конфигурации, как она показана выше.*

---

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 Systems Inc. использует **128**-битное шифрование **Triple-DES,** для того чтобы передача данных платежных карт**,** передаваемых через сети общего пользования**,** осуществлялась в соответствии со Стандартом **PCI DSS.** При передаче данных платежных карт через Интернет *всегда* используйте протокол **SSL,** а в случае беспроводных соединений**,** *всегда* используйте самый высокий доступный уровень шифрования**.** Более подробное описание можно найти в документе ***MICROS Wireless Networking Best Practices: A Payment Application Best Practices (PABP) Implementation Guide Supplement.***

Беспроводная передача данных о держателях платежных карт должна шифроваться как в сетях общего пользования**,** так и в частных сетях**.** Шифруйте передачу данных**,** используя технологию **WPA** или **WPA2,** протоколы **IPSEC VPN** или **SSL/TLS.** Никогда не доверяйтесь исключительно протоколу **WEP** для защиты конфиденциальности и входа в беспроводную сеть **LAN.** Используйте один из вышеупомянутых способов в сочетании с **128**-битным протоколом **WEP** и ежеквартально делайте ротацию ключей общего пользования для **WEP (**или автоматически**,** если позволяет технология**),** а также всегда**,** когда делаются перестановки в кадрах**,** имеющих доступ к ключам**.** Для протокола **WEP** необходимо использовать**,** по меньшей мере**, 104**-битный ключ шифрования и **24**-битное значение инициализации**.** Всегда ограничивайте доступ на базе **MAC** адреса**.**

В соответствии со Стандартом **PCI DSS, MICROS Systems Inc.** настаивает на шифровании **(**с использованием технологий **VPN, SSL** и т.п**.)** всей передаваемой через интернет конфиденциальной информации**,** включая беспроводные соединения**,** электронную почту и сервисы**,** например**, Telnet, FTP** и др**.**

Модемы не должны располагаться на серверах приложений**,** за исключением безвыходных ситуаций**.** Если модем установлен**,** он должен быть отключен от питания или выключен все то время**,** пока не используется**.** Для большей безопасности модем должен быть сконфигурен для автоматического возврата вызова и шифрования данных**.** Межсетевые экраны не защитят против атак через модем**.**

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 https://www.pcisecuritystandards.org/.

6. "Payment Card Industry (PCI) Data Security Standard.doc", p. 7, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

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, MICROS Systems Inc.** настаивает на регулярном использовании и обновлении анти-вирусных программ.

Антивирусное ПО должно стоять на всех системах, обычно подверженных заражению вирусами, в особенности на всех ПК и серверах.

Чтобы убедиться в том, что ваша анти-вирусная программа настроена в соответствии с Требованием **5** Стандарта **PCI DSS, "**Использовать и регулярно обновлять антивирусные программы**",** читайте вэб-сайт Совета **PCI SSC** https://www.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.[8]

MICROS Systems Inc. использует отдельные среды для разработок и производства, чтобы обеспечить программную целостность и безопасность. Обновленные патчи и 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 контроля конфигурационных изменений, а также установка доступных обновлений безопасности, зависят от специфической практики и политики объекта.

Чтобы убедиться в том, что ваш сайт разрабатывает и поддерживает системы и приложения безопасности в соответствии с Требованием **6** Стандарта **PCI DSS, "**Разрабатывать и поддерживать системы и приложения безопасности**",** читайте вэб-сайт Совета **PCI SSC** https://www.pcisecuritystandards.org/

7. "Payment Card Industry (PCI) Data Security Standard.doc", p. 8, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.
8. "Payment Card Industry (PCI) Data Security Standard.doc", p. 8, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

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 информации и защитить пароли.

Доступ к паролям клиентов со стороны дилеров и специалистов по системной интеграции должен быть ограничен.

Более подробно о Требовании **7** Стандарта **PCI DSS, "**Ограничить доступ к данным служебной необходимостью**",** читайте на вэб-сайте Совета PCI SSC https://www.pcisecuritystandards.org/

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

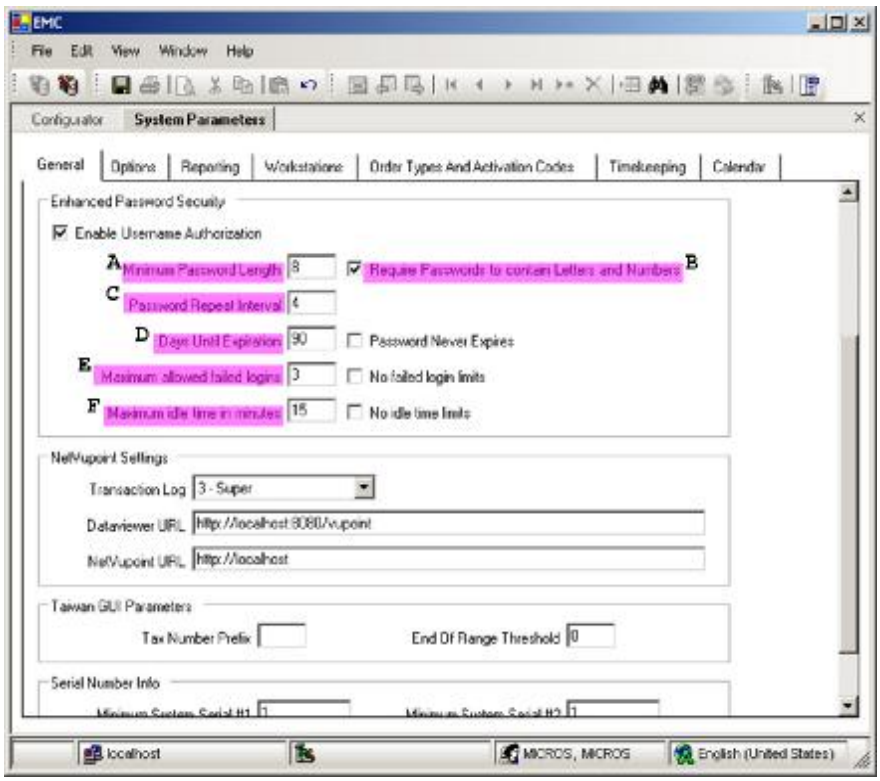
Такая привязка гарантирует, что действия с критическими данными и системами выполняются известными и авторизованными пользователями и могут отслеживаться.[10]

MICROS Systems Inc. признает важность привязки уникального идентификатора каждому работнику, имеющему доступ к компьютеру. Два разных пользователя **MICROS** не могут иметь одинаковый идентификатор, что позволяет отслеживать действия каждого при условии, что клиент 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 объекта. Для обеспечения жесткого контроля за доступом к приложению **9700 HMS**, всегда привязывайте уникальные имя пользователя и комплексный пароль каждой учетной записи. **MICROS Systems Inc.** настаивает на применении этих инструкций не только к паролям **MICROS,** но также и к паролям **Windows**.

Более того, **MICROS Systems, Inc.** советует пользователям, посредством уникального имени пользователя и комплексного пароля, соответствующих требованиям **PCI**, контролировать доступ ко всем ПК, серверам и базам данных с платежными приложениями и данными о держателях платежных карт.

9. "Payment Card Industry (PCI) Data Security Standard.doc", p. 9, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.
10. "Payment Card Industry (PCI) Data Security Standard.doc", p. 10, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Чтобы обеспечить соответствие Требованию **8** Стандарта **PCI DSS,** убедитесь в том, что следующие опции в Консоли Управления Предприятием **(EMC)** сконфигурены, как показано ниже.



В **EMC>System Information>Parameters>General>Enhanced Password Security,** опции, отмеченные розовым, конфигурятся следующим образом:

- **A:** В поле **"Minimum Password Length"** должно стоять, не менее, чем **8**
- **B:** В поле **"Require Passwords to contain Letters and Numbers"-** галочка
- **C:** В поле **"Password Repeat Interval" –** значение, не менее,чем **4**
- **D:** В поле **"Days Until Expiration" -** значение не более, чем **90**
- **E:** В поле **"Maximum Allowed Failed Logins" -** значение не более, чем **6**
- **F:** В поле **"Maximum Idle Time in Minutes" –** значение не более, чем **15**

MICROS Systems, Inc. настаивает на необходимости после первичного входа в систему сменить в EMC мастер-идентификатор, руководствуясь вышеприведенными инструкциями.

MICROS Systems, Inc. настаивает на использовании двух-факторной аутентификации для предоставления удаленного доступа к сети объекта со стороны работников **MICROS Systems, Inc.**, администраторов и представителей третьих сторон. Необходимо использовать такие технологии, как Служба удаленной аутентификации пользователей по телефонным линиям **(RADIUS)**, Система управления доступом для контроллера доступа к терминалу **(TACACS)** с токенами, или **VPN** на базе протоколов **SSL/TLS** или **IPSEC** с отдельными сертификатами.

Функциональность защиты удаленного доступа к программному обеспечению всегда должна быть установлена и использоваться. Дефолтовые настройки для удаленного доступа к программному обеспечению необходимо менять, с тем чтобы у каждого клиента были свои уникальные имя пользователя и комплексный пароль. Никогда не используйте дефолтовые пароли и соблюдайте требования **PCI DSS** в отношении паролей, изложенные на стр. 13, когда создаете новый, надежный пароль. Новый пароль должен содержать, по меньшей мере, **8** символов и быть буквенно-цифровым.

Подключения должны разрешаться только со специальных, известных **IP/MAC a**дресов. Для входа необходимо использовать надежную аутентификацию или комплексные пароли. Необходимо, чтобы была включена опция блокировки передачи зашифрованных данных и учетной записи после определенного количества неуспешных попыток. Система должна быть сконфигурена таким образом, чтобы удаленному пользователю для получения доступа приходилось устанавливать **VPN** соединение через межсетевой экран. Функциональность входа с использованием персонального идентификатора должна быть включена в целях безопасности данных. Доступ к паролям клиентов должен всегда быть ограничен. Более подробно читайте в документе ***Webex Policy***.

Более подробно о Требовании **8** Стандарта **PCI DSS**, “Привязать уникальный идентификатор каждому, у кого есть доступ к ПК”, читайте вэб-сайт Совета **PCI SSC** https://www.pcisecuritystandards.org/

9. Ограничить физический доступ к данным держателей 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**, **MICROS Systems Inc.** настоятельно рекомендует ограничить физический доступ к данным о держателях карт. Входящий и исходящий трафик к средам данных о держателях карт должен быть ограничен.

MICROS Systems, Inc. настаивает на том, чтобы пользователи не хранили данные о держателях карт в системах, доступных через интернет. Для обеспечения этого, сетевой сервер и сервер с данными должны быть разными.

11. “Payment Card Industry (PCI) Data Security Standard.doc”, p. 11, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Чтобы убедиться в том, что вы соответствуете Требованию **9** Стандарта **PCI DSS, "**Ограничить физический доступ к данным о держателях карт**",** читайте вэб-сайт Совета **PCI SSC** https://www.pcisecuritystandards.org/

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]

MICROS Systems Inc. включила в EMC всеобъемлющую утилиту контрольного журнала, позволяющую привилегированным пользователям отслеживать операции в **MICROS.** Появление баз данных с открытой структурой означает, что любой, имеющий системный уровень доступа к серверу базы данных **(MS SQL** или **Oracle),** имеет также доступ к системным компонентам, а следовательно, его вход и действия записываются, как указано в Требовании **10** Стандарта **PCI DSS.**

12. "Payment Card Industry (PCI) Data Security Standard.doc", p. 12, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

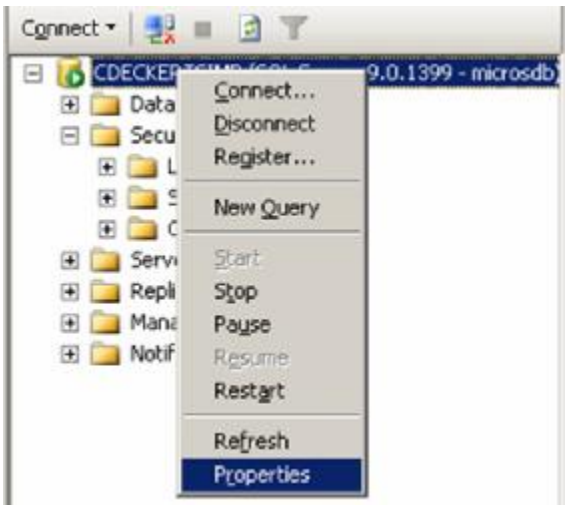
Включить ведение записей об изменениях в Базе Данных

Прим *Для обеспечения максимальной защиты и функциональности, MICROS Systems, Inc. настоятельно рекомендует перед выполнением этой задачи проконсультироваться с администратором базы данных SQL сервера или сервера Oracle.*

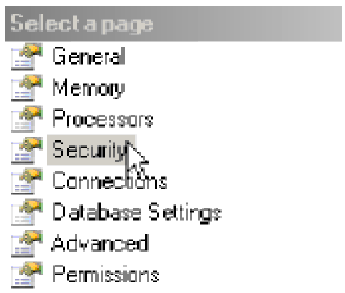
Microsoft® SQL Server

Для сервера **MSSQL**, включите ведение контрольных записей **C2**, выполнив следующие действия:

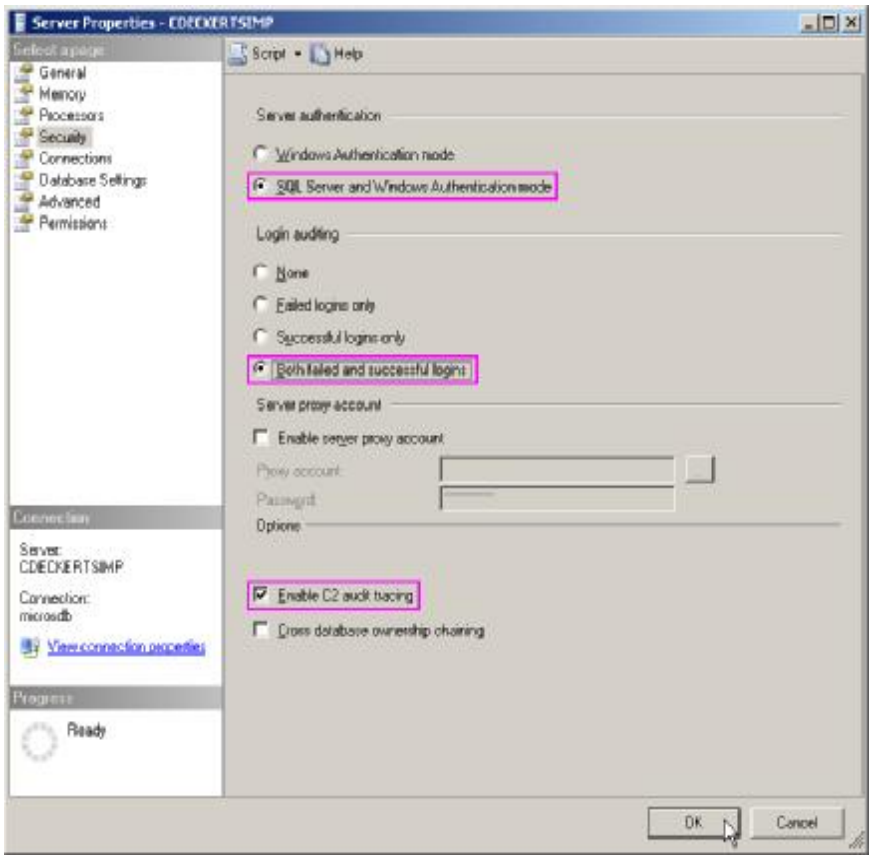
1. В ***Microsoft® SQL Server Management Studio***, выберите Сервер. Правым кликом по серверу выберите ***Properties***.



2. Выберите ***Security***.



3.



- В разделе ***Server authentication*** выберите опцию **"*SQL Server and Windows Authentication mode*" (**см. выделенное на рис. выше**)**
- В разделе ***Login auditing*** выберите опцию **"*Both failed and successful logins*".**
- В разделе ***Options*** выберите опцию **"*Enable C2 audit tracing*".**

Прим *Эти опции должны оставаться сконфигуренными так, как показано выше, для обеспечения соответствия Требованию 10 Стандарта PCI DSS.*

Более подробное описание можно найти в документе ***SQL Server 2000 C2 Administrator's and User'sSecurity Guide*****,** который можно загрузить на вэб-сайте **Microsoft:**
http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/sqlc2.mspx

Oracle® Server

1. Чтобы включить контрольные функции сервера **Oracle®,** настройте в файле **Parameter** статический параметр AUDIT_TRAIL, имеющий следующие свойства:

```
AUDIT_ TRAIL = { none | os | db |db, extended
|xml |xml,extended }
```

Ниже приводится описание каждой настройки:

- `none` или `false`: **А**удит отключен.
- `db` or `true`: Контроль включен, и все контрольные записи сохраняются в контрольном журнале базы данных **(SYS.AUD$).**
- `db,extended`: Как **db,** но при этом система также вставляет данные в колонки **SQL_BIND** и **SQL_TEXT.**
- `xml`: Контроль включен, и все контрольные записи сохраняются в файлах операционной системы в формате **XML.**
- `xml,extended`: Как xml, но при этом система также вставляет данные в колонки SQL_BIND и SQL_TEXT.
- `os`: Контроль включен, и все контрольные записи отправляются в контрольный журнал операционной системы.

Прим *Статический параметр AUDIT_TRAIL **не может иметь значения “none” или” false”; в противном случае не будет соответствия Требованию 10 Стандарта PCI DSS.***

Статический параметр **AUDIT_SYS_OPERATIONS** включает или выключает контроль операций, выполняемых пользователями с привилегиями **SYSDBA** или **SYSOPER,** включая пользователя **SYS.** Все контрольные записи записываются в контрольный журнал операционной системы.

Прим *Статический параметр AUDIT_SYS_OPERATIONS должен быть настроен на значение ‘true’, чтобы обеспечить соответствие Требованию 10 Стандарта PCI DSS.*

Когда используются опции **os, xml** и **xml,extended,** параметр **AUDIT_FILE_DEST** указывает директорию операционной системы**,** в которой находится контрольный журнал**,** а также все обязательные контрольные записи**,** определяемые параметром **AUDIT_SYS_OPERATIONS**.

Прим *Теперь будут контролироваться привилегированные входы в базу данных, запуски и остановки базы данных и структурные изменения (например, добавлнение файла с данными).*

Контрольные функциш не будут запущены до тех пор, пока они не будут определены. О том, как их определ ить, читайте документ Oracle® Database Security Guide.

---

2. Используйте контрольный отчет **(AUDIT statement)** для настройки контролируемых данных**.** Этот отчет может использоваться для отслеживания **SQL-**утверждений в пользовательских сессиях**,** специальных **SQL-**утверждений или всех **SQL-**утверждений**,** авторизованных той или иной системной привилегией**,** а также отслеживать операции по тому или иному объекту схемы**.**

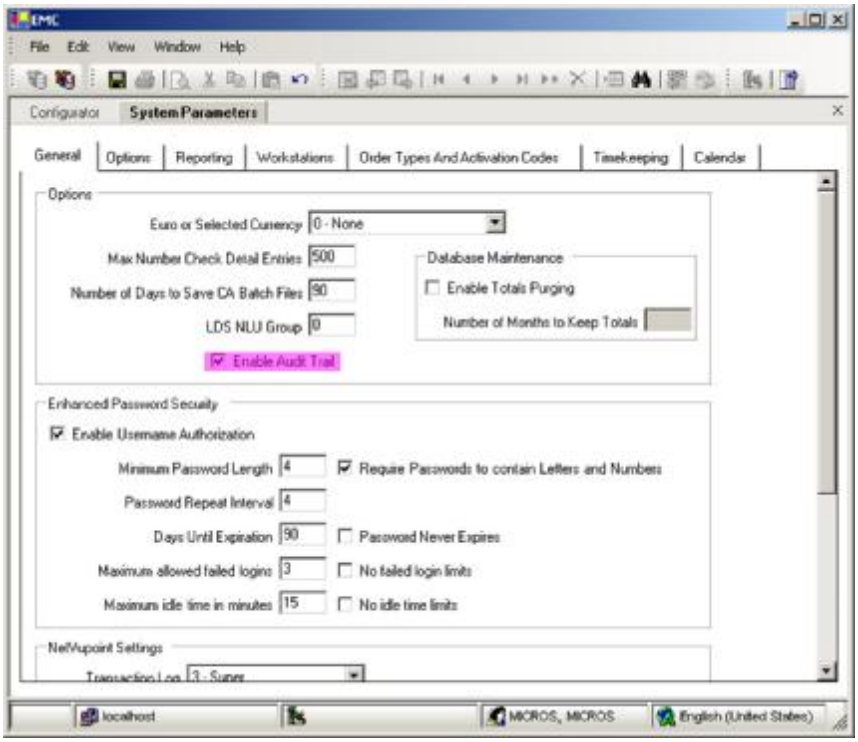
Детальную информацию об использовании контрольного отчета можно найти в разделе **“AUDIT”** документа ***Oracle® Database SQL Reference***, http://download.oracle.com/docs/cd/B19306_01/server.102/b14200/statements_4007.htm#i2059073.

Более подробное описание приводится в главе **“*Database Auditing: Security Considerations*”** документа ***Oracle® Database Security Guide***, который можно скачать с вэб**-**сайта **Oracle**, www.oracle.com.

Контрольный журнал в EMC

В соответствии со Стандартом **PCI DSS, MICROS Systems Inc.** настаивает на ведении записей на сервере базы данных по всем действиям работников, имеющих корневые привилегии или привилегии администратора, для чего должна быть включена функциональность контрольного журнала. Всегда держите включеными контрольные журналы систем, в которых хранятся, обрабатываются и передаются данные о держателях карт.

Чтобы включить контрольный журнал, зайдите в EMC, откройте **System Information | System Parameters | General,** и поставьте галочку в опции **"Enable Audit Trail",** как показано ниже.



Чтобы убедиться в том, что вы соответствуете Требованию **10** Стандарта **PCI DSS, "**Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт**",** ознакомьтесь с вэб-сайтом Совета P**CI SS**, https://www.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.[13]

В соответствии со Стандартом **PCI DSS, MICROS Systems Inc.** настаивает на регулярном тестировании систем и процессов безопасности.

Чтобы убедиться в том, что ваши системы и процессы безопасности настроены в соответствии с Требованием **11** Стандарта **PCI DSS, "**Регулярно тестировать системы и процессы безопасности**",** ознакомьтесь с вэб-сайтом Совета **PCI SS**C**,** https://www.pcisecuritystandards.org/

Поддержание политики информа-ционной 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 Стандартом **PCI DSS, MICROS Systems Inc.** настаивает на поддержании политики информационной безопасности.

Политика информационной безопасности должна включать информацию о физической безопасности, безопасности хранения и передачи данных и системном администрировании.

Чтобы убедиться в том, что ваша политика информационной безопасности настроена в соответствии с Требованием **12** Стандарта **PCI DSS, "**Поддерживать политику информационной безопасности**",** ознакомьтесь с вэб-сайтом Совета **PCI SS**C**,** https://www.pcisecuritystandards.org/

13. "Payment Card Industry (PCI) Data Security Standard.doc", p. 13, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.
14. "Payment Card Industry (PCI) Data Security Standard.doc", p. 14, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.