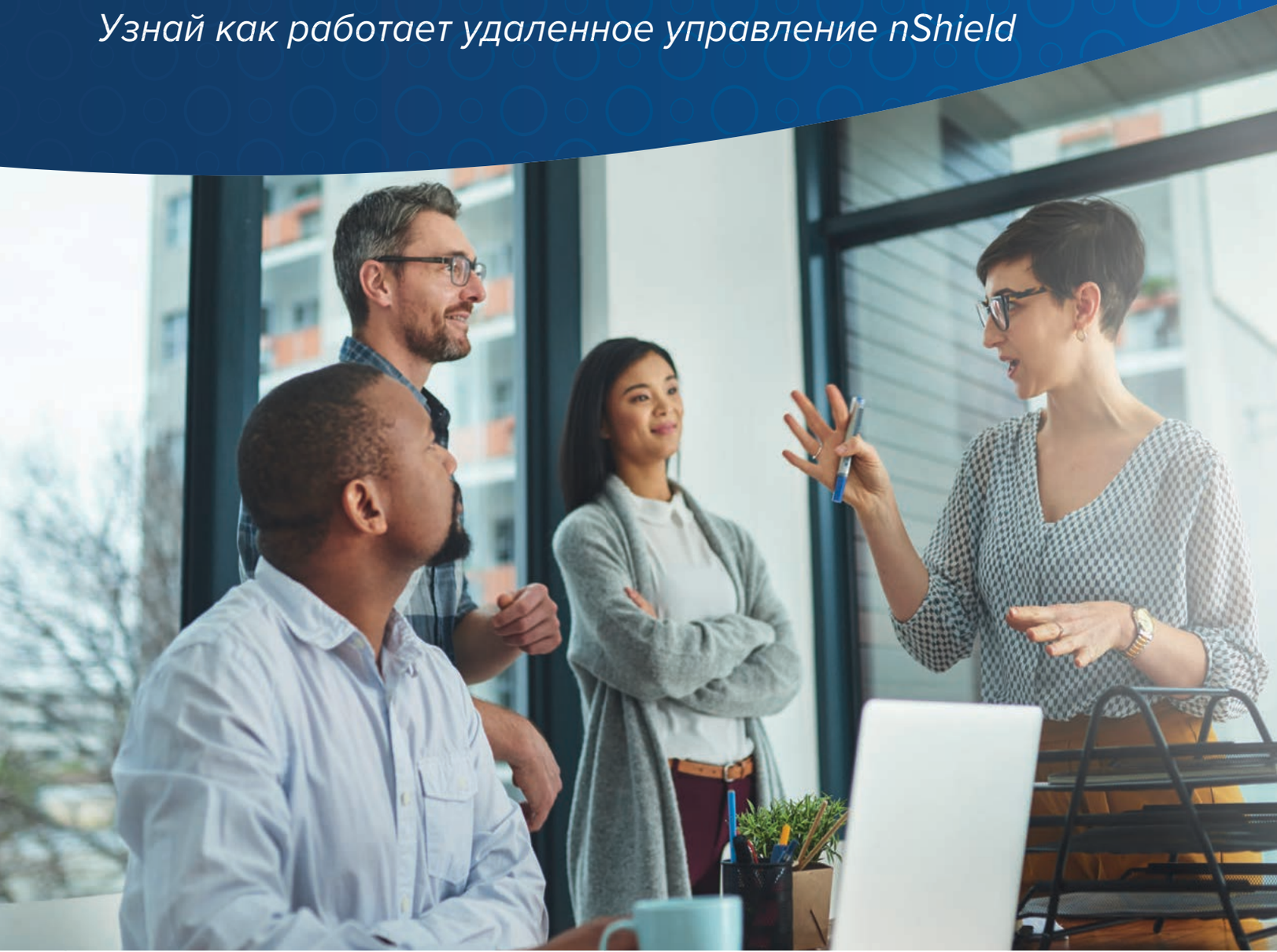
www.ncipher.com

Удаленное управление nShield

- Позволит вам управлять распределенными географически модулями nShield Solo и Connect прямо из офиса
- Экономит время благодаря удаленному доступу ко всем модулям HSM 24X7
- Включает большое разнообразие функций через дистанционное представление смарт-карт. Удаленное обновление прошивки, проверка состояния, запуск утилит.
- Исключает риски, возникающие транспортировке смарт-карт.

nShield Remote Administration

Узнай как работает удаленное управление nShield



nShield Remote Administration

Обзор возможностей

Для локального управления удаленным HSM нужны следующие компоненты:

- Карты удаленного администрирования – пользовательские смарт-карты, оснащенные апплетом nCipher
- Trusted Verification Devices (TVDs) – считыватели смарт-карт nCipher, используемые с картами удаленного администрирования, для создания безопасного соединения с целевым HSM
- Клиент удаленного администрирования (RAC) — простой интерфейс, который можно запустить на ноутбуке или ПК, и настроить связь с HSM

Для удаленного управления nShield создается безопасное соединение между вашими HSM, смарт-картами удаленного управления и устройством верификации. После предоставления кворума смарт-карт вы сможете управлять HSM, как если бы физически присутствовали рядом с ним. Вы контролируете HSM, используя компьютер и удаленный рабочий стол или SSH, через VPN.

Рабочие характеристики

Удаленное администрирование позволяет выполнять большинство типичных функций HSM, включая:

- Настройка новых nShield HSM
- Создание Security Worlds—nCipher уникальная архитектура для управления ключами и подключение новых HSM в существующие Security Worlds
- Обновление прошивки и файлов образов для технического обслуживания, другие обновления
- Мониторинг и изменение состояния HSM, перезагрузка по мере необходимости.

Обеспечение безопасности

Удаленное администрирование включает в себя следующие компоненты для защиты ваших транзакций:

- Взаимная аутентификация между картами удаленного администрирования и HSM на основе выданных на заводе ордеров (например, цифровых сертификатов) с использованием обмена эфемерными ключами Диффи-Хеллмана
- AES256 – криптосоединение между картами удаленного администрирования и HSM
- Верификация электронного серийного номера HSM держателем карты
- Сертифицированные по стандарту FIPS 140-2 прошивки и карты удаленного администрирования
- TVDs, сертифицированный по протоколу Secoder – запрещает вредоносным программам на клиентской рабочей станции подделывать идентификационные данные HSM, передаваемые на карты удаленного администрирования.

Пожалуйста, обратитесь к нам, чтобы получить дополнительную информацию об удаленном управлении и подробную брошюру.

Требования для настройки удаленного управления nSHIELD

- nShield Solo PCIe и Connect HSMs
- Программное обеспечение RAC совместимо с Microsoft Windows, Linux и OS X
- ПО nShield v12.00 и выше, прошивка и 2.61.2 и выше
- LAN или VPN клиента и удаленный доступ

Начало работы с удаленным управлением nSHIELD

Есть разные комплекты для удаленного управления. Возможно расширение для поддержки большего числа HSM, для этого нужно приобрести дополнительный комплект. В таблице ниже представлены комплекты, которые можно приобрести.

Tier	Remote HSMs Served	Remote Admin Cards	TVDs	Client DVDs
1	1 to 10	20	2	2
2	11 to 20	50	5	5
3	21 to 40	100	10	10
4	40 or more	200	20	20

ПОДРОБНЕЕ

Если вы хотите узнать, как nCipher Security обеспечивает целостность и контроль критически важной информации и приложений для вашего бизнеса, посетите сайт **ncipher.com**

Search: nCipherSecurity