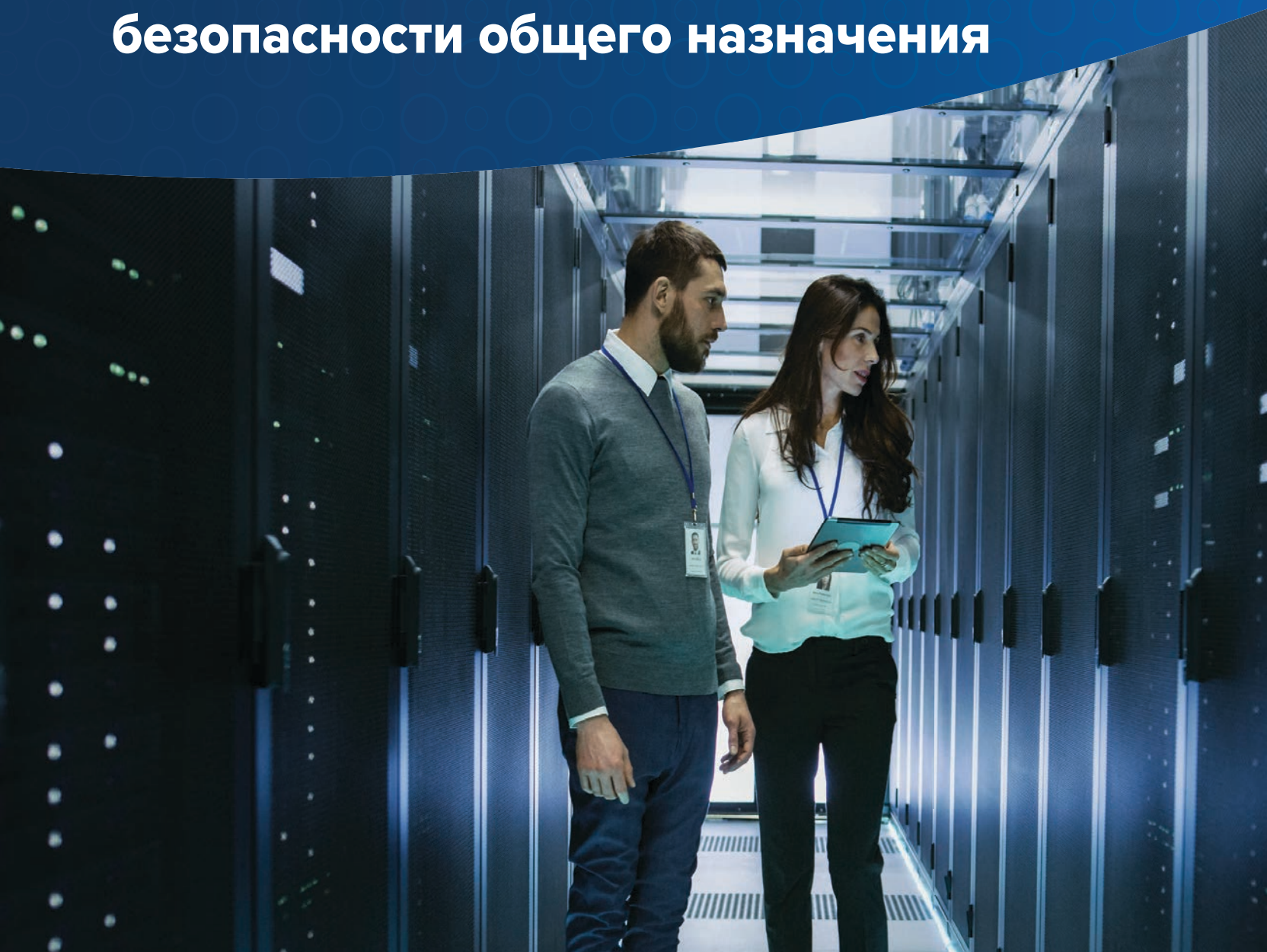


nShield® аппаратные модули безопасности общего назначения



Оглавление

Безопасность, которой можно доверять	3
Линейка устройств nShield	4
nShield connect	4
nShield edge	4
nShield solo	4
Поддерживает все разнообразие целей и направлений использования	5
Особенности линейки nShield	
Интерфейсы веб-сервисов для работы с облаками	6
Надежное управление ключами для данных в облаке с помощью nshield byok	6
Рационализация операций с использованием дистанционного мониторинга и управления	7
Гибкая архитектура Security world	7
CODESAFE - ЗАЩИЩЕННАЯ СРЕДА ВЫПОЛНЕНИЯ NSHIELD	8
Партнерство с лидерами отрасли	9
Универсальность и высокая производительность	10
Сертификация по отраслевым стандартам	11
FIPS 140-2	11
Соответствие стандартам: Общие критерии — принятый в России международный стандарт по компьютерной безопасности, eIDAS	11
Подробнее	11





Безопасность, которой можно доверять

Аппаратные модули безопасности nCipher Security - надежные, устойчивые к взлому устройства для защиты конфиденциальных данных. Эти сертифицированные модули FIPS 140-2 выполняют криптографические функции, такие как создание, управление и хранение ключей шифрования и подписи, а также выполнение конфиденциальных процессов в пределах защищенных границ.

Мощное дополнение к вашему комплексу безопасности nShield HSM:

- Достижение более высокого уровня безопасности данных и доверия
- Соблюдение и превышение важных стандартов защиты данных
- Поддержание высокого уровня эффективности и гибкости бизнеса

Линейка устройств nShield

Семейство nShield HSM включает разные модели для всевозможных сценариев:

NSHIELD CONNECT

Сетевые устройства

nShield Connect HSM предоставляет криптографические сервисы для приложений, распределенных в сети.

nShield Connect HSM доступен в двух сериях: классический nShield Connect+ и высокопроизводительный nShield Connect XC.



NSHIELD EDGE

портативные USB-модули

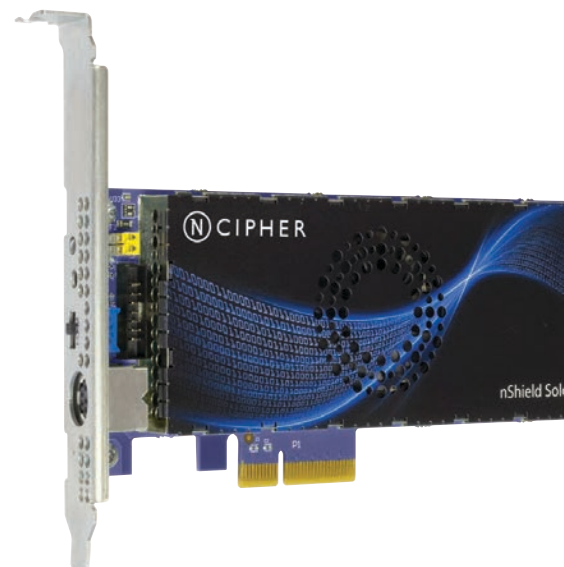
nShield Edge HSM - это настольные устройства, созданные для удобства и экономичности. Edge идеален для разработчиков, он поддерживает такие приложения, как генерация root-ключей.



NSHIELD SOLO

PCIe-карты для встраивания в устройства или серверы

nShield Solo HSM - модули в формате PCI-Express карт, которые предоставляют криптографические услуги для приложений, размещенных на сервере или устройстве. nShield Solo HSM выпускается в двух сериях: классический nShield Solo+ HSM и высокопроизводительная серия nShield Solo XC HSM.



Поддерживает все разнообразие целей и направлений использования

Клиенты nCipher используют nShield HSM в качестве основы доверия в различных бизнес-приложениях, включая инфраструктуры открытых ключей (PKI), защиту ключей шифрования SSL/TLS, подписание кода, цифровую подпись и блокчейн. Поскольку распространение Интернета вещей создает большой спрос на идентификаторы устройств и сертификаты, nShield HSM будет продолжать поддерживать меры безопасности, такие как аутентификация устройств с использованием цифровых сертификатов.

nShield HSM поддерживает широкий спектр криптографических алгоритмов, включая алгоритмы на эллиптических кривых, которые обеспечивают высокоскоростные транзакции, идеально подходящие для современных вычислительных сред, операционных систем и API.



Особенности линейки nShield

ИНТЕРФЕЙСЫ ВЕБ-СЕРВИСОВ ДЛЯ РАБОТЫ С ОБЛАКАМИ

Дополнительный nShield Web Services Crypto API упрощает взаимодействие между вашими приложениями и HSM, выполняя команды через вызовы веб-служб. Этот инновационный подход облегчает развертывание, устраняя необходимость в интеграции приложений непосредственно с nShield и зависимость от выбора ОС и архитектуры. Совместимые с облачными решениями интерфейсы Web Services Crypto API для приложений, размещенных в облаке и в традиционных центрах обработки данных.

УПРАВЛЕНИЕ КЛЮЧАМИ В ОБЛАКЕ С ПОМОЩЬЮ NSHIELD BYOK

nShield BYOK позволяет создавать надежные ключи в локальном nShield HSM и безопасно экспортировать их в облачные приложения, независимо от того, используете ли вы Amazon Web Services, облачную платформу Google,

Microsoft Azure - или все три сразу. С nShield BYOK вы повышаете безопасность своих методов управления ключами, получаете больший контроль над своими ключами и гарантируете, что вы несете ответственность за обеспечение безопасности своих данных в облаке. Модуль nShield BYOK приносит вам следующие преимущества:

- Надежные методы управления ключами, которые повышают безопасность конфиденциальных данных в облаке
- Сильная генерация ключей с помощью высокоэнтропийного генератора случайных чисел nShield, защищенного FIPS-сертифицированным оборудованием
- Большой контроль над ключами – используйте свой собственный nShield HSM в своей собственной среде для создания и безопасного экспорта ключей в облако



“В результате нашего сотрудничества наши клиенты могут создавать и загружать свои собственные мастер-ключи в облачный HSM и со-хранять полный контроль над своими ключами, что дает им уверенность в том, что их данные защищены”

Дэн Пластина, Менеджер Партнерских программ, Microsoft

РАЦИОНАЛИЗАЦИЯ ОПЕРАЦИЙ ПРИ ПОМОЩИ ДИСТАНЦИОННОГО МОНИТОРИНГА И УПРАВЛЕНИЯ

nShield Monitor и nShield Remote Administration, доступные для nShield Solo и Connect HSM, помогут вам сократить эксплуатационные расходы, при этом вы всегда сможете контролировать все HSM 24x7.

Удаленное управление и мониторинг nCipher:

- Оптимизация производительности HSM, планирования инфраструктуры и времени безотказной работы с помощью nShield Monitor для информирования о нагрузке, статистике использования, событиях вскрытия, состоянии.
- Сокращение транспортных расходов и экономия времени за счет управления HSM через мощный и безопасный интерфейс nShield Remote Administration

ГИБКАЯ АРХИТЕКТУРА SECURITY WORLD

nShield HSM является неотъемлемой частью архитектуры nCipher Security World, которая создает уникальную, гибкую среду для управления ключами. Вы можете комбинировать разные модели nShield HSM для построения единой экосистемы, масштабируемой, хорошо взаимодействующей, балансирующей нагрузку. Security World обеспечивает взаимодействие при развертывании одного или сотен HSM, позволяет управлять неограниченным количеством ключей, а также автоматически и удаленно создавать резервные копии и восстанавливать ключи. nCipher Security World предлагает следующие преимущества:

- Помогает легко масштабировать nShield HSM по мере роста ваших потребностей
- Поддерживает отказоустойчивость системы
- Экономит время, исключая длительное резервное копирование HSM

“nShield HSM были важным компонентом для предоставления услуг с исключительным уровнем производительности и масштабируемости”

Стив Коллинз, Директор, Emerging Markets Group, Barclays



"nCipher nShield HSM предлагает быстрый и эффективный способ получения новых ключей. В частности, мы были очень впечатлены функцией CodeSafe, которая позволяет нам запускать код с повышенными требованиями к безопасности, защищенный в пределах HSM. Это идеальное решение"

Райан Смит, главный технический директор Chain

CODESAFE - ЗАЩИЩЕННАЯ СРЕДА ВЫПОЛНЕНИЯ NSHIELD

Помимо защиты конфиденциальных ключей, nShield Solo и Connect HSM также обеспечивают безопасную среду для запуска ваших приложений. Опция CodeSafe позволяет разрабатывать и выполнять код в среде FIPS 140-2 Level 3 nShield, защищая ваши приложения от потенциальных атак.

Codesafe:

- Обеспечение высокой надежности благодаря выполнению чувствительных к безопасности приложений и защите конечных точек и данных приложений в сертифицированной среде
- Защита чувствительных к безопасности приложений от угроз, таких как инсайдерские атаки, вредоносные программы и расширенные постоянные угрозы
- Исключение риска несанкционированных изменений приложений или заражения вредоносными программами с помощью подписи кода

Партнерство с лидерами индустрии

nCipher сотрудничает с ведущими поставщиками технологий для предоставления решений, которые закрывают широкий диапазон задач и помогают клиентам достичь своих целей в цифровой трансформации. Через партнерскую программу nCipher сотрудничает с компаниями для интеграции nShield HSM в различные решения безопасности, включая аттестацию и PKI, безопасность баз данных, подписание кода,

цифровые подписи, управление привилегированными учетными записями, приложения, а также облачные сервисы и big data. nShield HSM поддерживает приложения безопасности наших партнеров, чтобы обеспечить самую сильную криптографическую обработку, защиту ключей и управление ключами, а также соблюдение государственных и отраслевых стандартов безопасности данных.

"Поддержка F5 для HSM nShield обеспечивает наивысший уровень физической защиты криптографических ключей, позволяя организациям устанавливать и доказывать соответствие новейшим требованиям правительства к безопасности и лучшим практикам."

Шива Мандалам, Старший директор, управление продуктом, F5 Networks

"Мы предоставляем услуги PKI для широкого круга организаций, и все наши управляемые решения PKI полагаются на nShield HSM из-за их уникального сочетания высокого уровня безопасности и простоты управления для таких важных функций, как резервное восстановление ключей".

Роберт Ханн, директор по развитию бизнеса, Trustis





Универсальность и высокая производительность

Аппаратные модули обеспечения безопасности nShield Connect и Solo доступны в нескольких вариациях, чтобы соответствовать вашим средам, независимо от загрузки - слабой или требующей очень высокой производительности.

Соответствие стандартам индустрии

Приверженность nCipher строгим стандартам помогает продемонстрировать соответствие в регулируемых средах, обеспечивая при этом уверенность в безопасности и целостности HSM nShield. Ниже приведен частичный список стандартов, которым мы следуем. Полные списки доступны на нашем веб-сайте и в брошюрах

FIPS 140-2

Признанный во всем мире, FIPS 140-2 является стандартом института NIST США, он подтверждает надежность криптографических модулей. Все nCipher nShield HSM имеют сертификат FIPS 140-2 level 2 и level 3.

СООТВЕТСТВИЕ СТАНДАРТАМ: Common Criteria — ПРИНЯТЫЙ В РОССИИ МЕЖДУНАРОДНЫЙ СТАНДАРТ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ, EIDAS

модели nShield Solo+ и Connect+ имеют сертификат Common Criteria EAL 4+ , а также признаны квалифицированными устройствами создания подписи (QSCDs). Как QSCDs, nShield HSM могут служить основой без-опасности Европейской цифровой подписи (eIDAS) и других всемирно признанных решений, включая услуги аутентификации, цифровой под-писи и штампа времени.



Подробности

На сайте www.nCipher.com/products/general-purpose-hsms

На этой странице вы узнаете, как мы можем защитить критически важную информацию и приложения вашего бизнеса, на вашем собственном предприятии, в облаке и в виртуальных средах.

О компании nCipher

Быстро развивающаяся цифровая среда повышает удовлетворенность клиентов, дает конкурентное преимущество и повышает эффективность работы. И множит риски.

nCipher Security расширяет возможности компаний, обеспечивая доверие, целостность и контроль над критически важной бизнес-информацией и приложениями.

Наши криптографические решения защищают новые технологии: облачные, IoT, blockchain, цифровые платежи - и обеспечивают соответствие стандартам безопасности, используя те же проверенные технологии, которым доверяют ведущие международные компании. Мы создаем доверие для ваших бизнес – приложений, обеспечиваем целостность данных и полный контроль - сегодня, завтра, во все времена.