АЙТИБАСТИОН

СКДПУ НТ
КОМПАКТ

Программно-аппаратный комплекс, предназначенный для контроля действий собственных администраторов и внешних технических специалистов

СКДПУ НТ Компакт – система для контроля действий внешних и внутренних администраторов, аутсорсеров, поставщиков ИТ-услуг и других привилегированных пользователей. Решение создано на базе программного обеспечения Комплекса СКДПУ НТ и компактной малошумной аппаратной платформы с низким энергопотреблением. Компактная и мобильная, система готова к использованию в условиях отсутствия специально оборудованных ЦОД.

Преимущества СКДПУ НТ Компакт

- **Функциональность:** Решение обладает полным набором функций контроля действий привилегированных пользователей комплекса СКДПУ НТ.
- **Универсальность:** Система одинаково удобна в использовании как на распределенных по разным территориям точках крупного бизнеса, так и в информационной инфраструктуре небольших компаний. Размер и объем инфраструктуры для работы ИТ-специалиста значения не имеют.
- **Быстрое развертывание:** СКДПУ Компакт поставляется в виде программно-аппаратного комплекса, устанавливается **не в разрыв сетевого трафика и не требует агентов** на целевых системах. Уже готов к использованию.

Детали реализации

Одно устройство СКДПУ НТ Компакт в минимальной комплектации рассчитано на контроль до 10 одновременных сессий. Работает по принципу логического шлюза: привилегированные пользователи (администраторы, аудиторы) взаимодействуют с ключевой информационной инфраструктурой не напрямую, а через него, при этом используя стандартные клиенты для удаленного подключения. Система при этом фиксирует все доступные действия в виде текстовой информации и видеозаписи, сохраняя контроль не только над сессией, но и передаваемой между пользователем и целевой системой информации, в т.ч. буфера обмена.

СКДПУ НТ Компакт: для небольших компаний (МСБ)

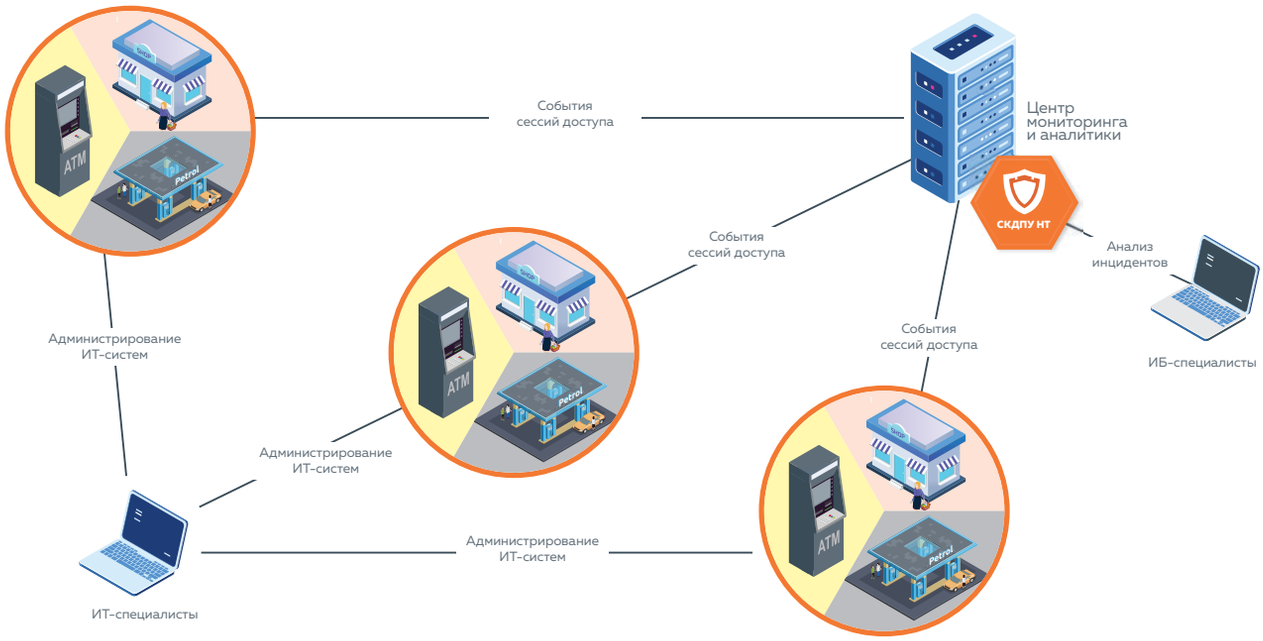
Зачастую у таких компаний небольшая ИТ-инфраструктура и ограниченный бюджет, недостаточный для приобретения мощных enterprise-решений. Устройство СКДПУ НТ Компакт может быть установлено в офисе небольшой компании для обеспечения полного функционала контроля действий привилегированных пользователей.

СКДПУ НТ Компакт: для территориально-распределенных компаний (энергетика, банки, сети АЗС, ритейл)

В инфраструктуре больших территориально-распределенных компаний присутствует множество удаленных от корпоративного центра точек (например, АЗС, небольшие офисы и т.п.). На этих объектах расположено малое количество информационных систем и оборудования, им свойственно ограничение потребления электричества и кондиционирования. Сюда дорого, долго и сложно доставлять технических специалистов для проведения работ по настройке и обслуживанию системы. Содержать штат локальных ИТ-специалистов –

нерентабельно. Каждое устройство СКДПУ НТ Компакт через защищенные каналы связи взаимодействует с головным офисом, откуда администратор безопасности может централизованно управлять привилегированными учетными записями и контролировать действия администраторов на удаленных объектах. При этом ИТ-специалист или иное уполномоченное лицо, к примеру, сотрудник подрядной организации, оперативно и с соблю-дением должного уровня информационной безопасности, проверяет или настраивает нужные для бизнеса системы.

Приведенные выше сценарии характерны для множества сфер бизнеса и применимы **в корпоративных сетях**, а также **промышленных объектах**, к примеру, **системах АСУ ТП**.



Возможности СКДПУ НТ Компакт

Мониторинг и реагирование

Продукт отслеживает и регистрирует все сеансы работы по протоколам администрирования RDP, SSH, Telnet, VNC, SFTP, SCP и прочим (видеозапись всей сессии, в также связанные данные: клавиатурный ввод, заголовки окон и т.д.). Это обеспечивает возможность моментального реагирования на инциденты, связанные с действиями привилегированных пользователей, их быстрое, полное и всестороннее расследование, а также возможность оперативно определить ответ-ственное за инцидент лицо. С одной стороны, продукт способствует повышению эффективности работы внутреннего персонала, с другой, – позволяет контролировать исполнение SLA внешними поставщиками ИТ-услуг.

Управление пользователями

Система позволяет автоматически блокировать сеанс доступа пользователя по истечении определенного времени или при его неактивности. Наличие единой точки входа дает возможность оперативно управлять доступом: каждый сотрудник авторизуется на СКДПУ НТ Компакт, используя свои учет-ные данные, и получает доступ к нужным целевым устрой-ствам в рамках заданных ограничений. При этом данные учетных записей конечных устройств остаются скрытыми, что минимизирует нерегламентированный доступ к инфраструктуре. Также СКДПУ НТ Компакт позволяет контролировать управление изменениями конфигурации, ограничивать запуск запрещенных процессов на стороне целевого устройства и ограничивать доступ на конкретные сетевые диапазоны внутри сети. Продукт обеспечивает надежную идентификацию и аутентификацию внутренних и внешних пользователей при их доступе к целевым системам с возможностью подключения функций 2FA.

Оперативность

Функция оптического распознавания символов позволяет анализировать все действия пользователей в реальном времени. При обнаружении запрещенных или подозрительных команд система направляет уведомление уполномоченному лицу, которое может мгновенно вмешаться и предотвратить несанкционированный доступ, а также деструктивные/ошибочные действия технического персонала.

Архивы и отчеты

Проводить внутренние и внешние аудиты становится проще, так как СКДПУ Компакт записывает и хранит в журналах информацию по всем сессиям, а также позволяет создавать различные отчеты. Установить СКДПУ Компакт значительно быстрее, чем разработать регламенты и контролировать доступ всех пользователей ко всем системам с помощью организационных мер.

Сертификаты ФСТЭК России и МО РФ

Решение СКДПУ НТ Компакт помогает обеспечить соответствие требованиям ФСТЭК России по идентификации и аутентификации, управлению доступом и регистрации событий безопасности при удаленном доступе через внешние информационно-телекоммуникационные сети: позволяет четко разграничить полномочия внутренних и внешних пользователей на основе политики безопасности компании по ряду параметров: IP-адрес, имя пользователя, интервал времени, протокол, тип сеанса. Система контроля действий поставщиков ИТ-услуг (СКДПУ) имеет сертификаты соответствия требованиям ФСТЭК России по УД-4 и Министерства обороны РФ по РД НДВ-2.

ООО «АйТи БАСТИОН» | 119501, Россия, Москва, ул. Старовольнская, 15, к. 1. | E-mail: info@it-bastion.com Тел.+7 (499) 322 36 67 | Больше информации на сайте: www.it-bastion.com