GIS DAYS

Интеграционная сила отечественных решений. Взгляд со стороны контроля привилегированного доступа

Родин Константин Сергеевич

Руководитель направления по развитию продуктов

АйТи Бастион

GIS DAYS

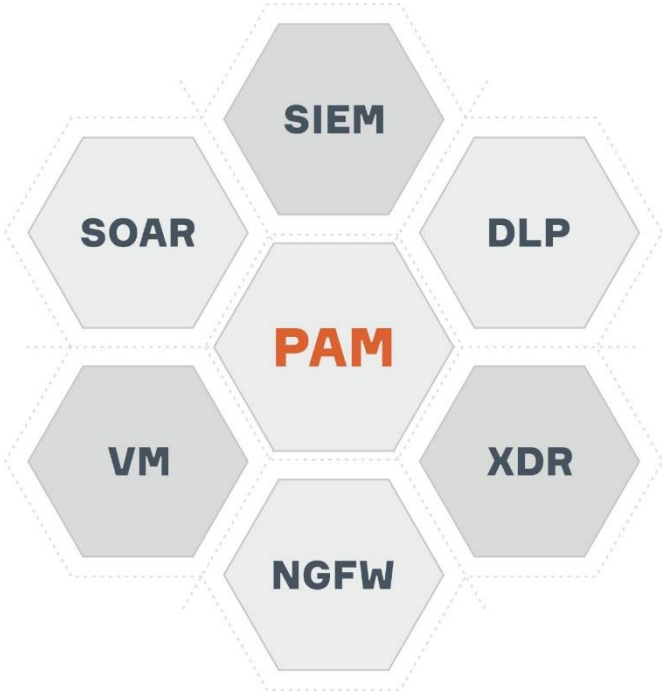
АЙТИБАСТИОН

Базовые определения

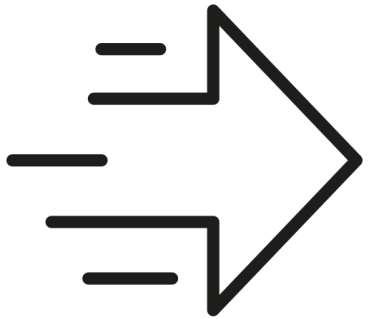
Privileged Access Management (PAM)

Решение для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам, которое тем самым помогает защитить организации от киберугроз.

Проблема «изолированности» средств ИБ

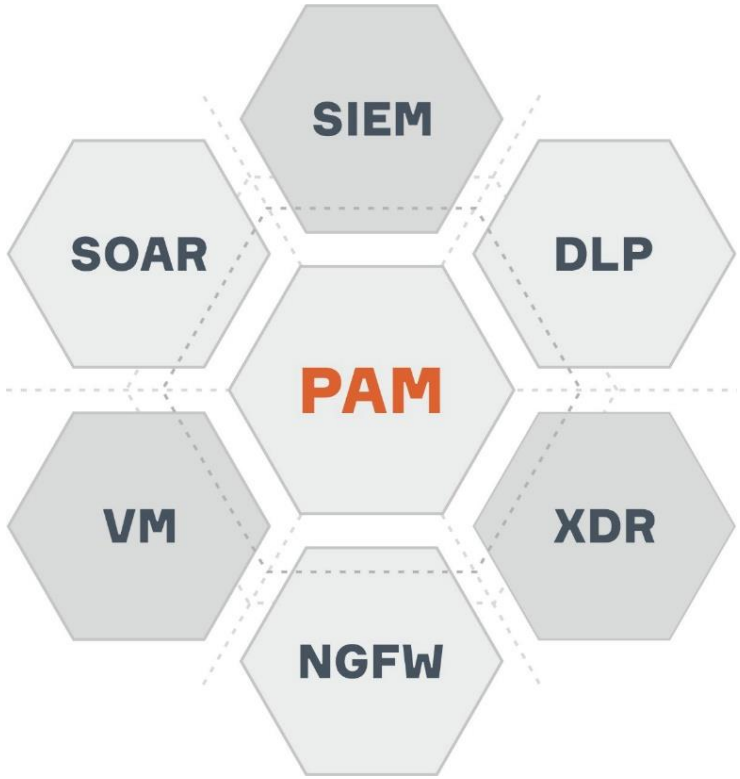


«зазор» средств защиты



эксплуатация «зазора»

Больше возможностей в пересечении возможностей



- Контроль и мониторинг доступа
  - Выявление инцидентов
  - Реагирование на инциденты
  - Кроссвендорная интеграция
- Контроль доступа к информации

Единая дополняемая концепция

Реализация концепции взаимодополняемых ИТ- и ИБ-систем, где каждая система обеспечивает другую профильными данными, обогащая модель событий и предоставляя человеку максимально полный перечень данных для быстрого и точечного реагирования на инциденты.

1. Система обнаружения вторжений
2. Виртуализация и облачные сервисы
3. Многофакторная аутентификация
4. Отечественные ОС
5. IRP/SOAR
6. HoneyPot
7. SIEM-системы
8. АРМ, тонкие клиенты и т.п.
9. Криптошлюзы и VPN-туннели
10. Token и Smart Card
11. Межсетевые экраны
12. DLP*

GIS DAYS

АЙТИБАСТИОН

Операционные системы и БД

01 Базовая ОС и БД

СКДПУ НТ работает под управлением ОС **Astra Linux SE** и БД **Postgres**

02 Совместимые ОС

СКДПУ НТ поддерживает работы с ОС **РедОС**, **Альт Линукс**, **Роса** и др. при использовании их в качестве пользовательской и целевой

РЕД ОС

ASTRA LINUX®

03 Поддерживаемые БД

СКДПУ НТ имеет поддержку отечественной БД **Jatoba** и может быть установлен при её использовании

GIS ГАЗИНФОРМ СЕРВИС

alt linux

ROSA

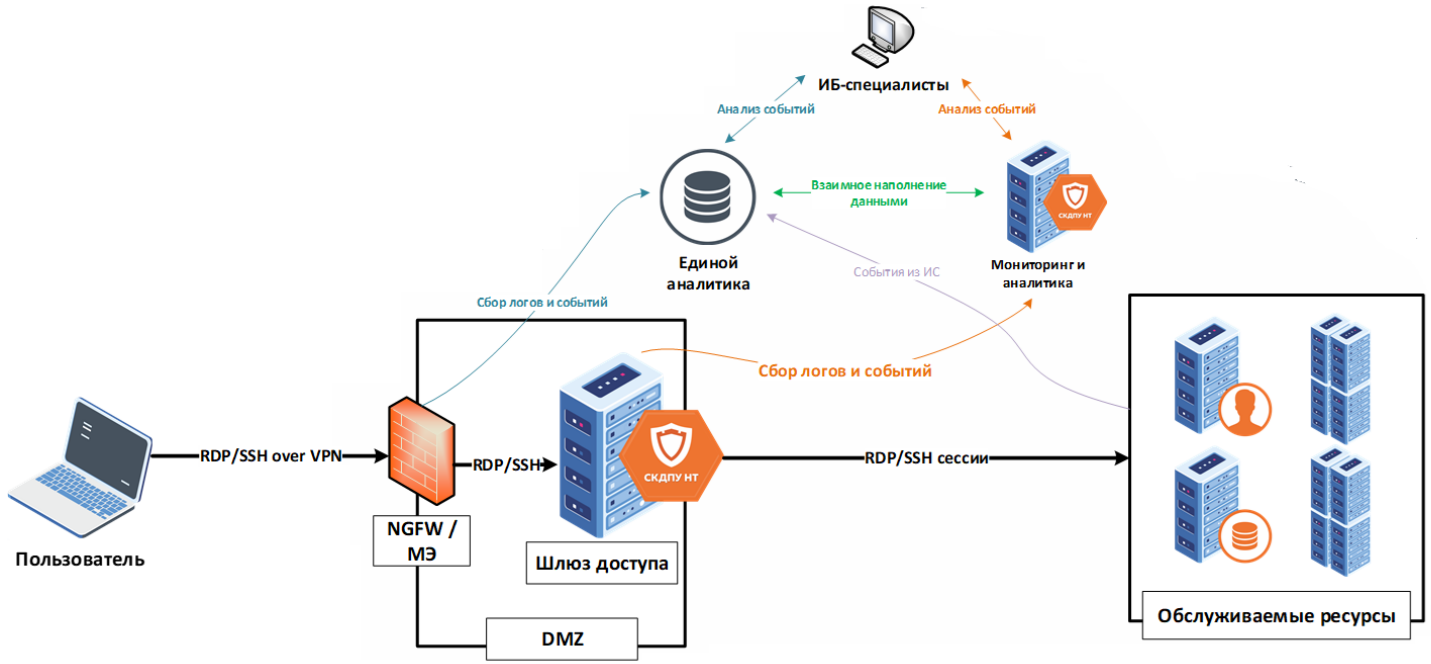
Криптошлюзы, МЭ, NGFW

Реализация безопасного контура от пользователя в инфраструктуру с созданием DMZ-зоны.
Обеспечение дополнительного обмена информацией о сессии пользователя, реагирование на отклонения в модели поведения пользователя.

infotecs

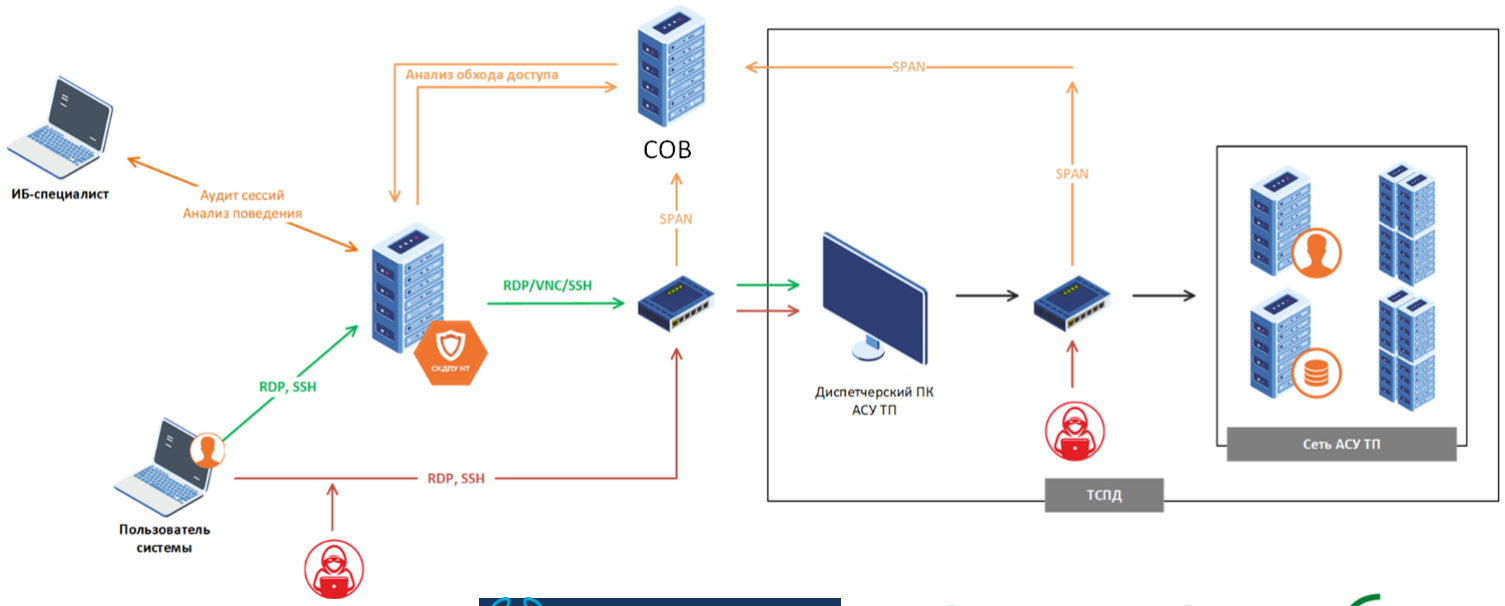
UserGate

с•терра®



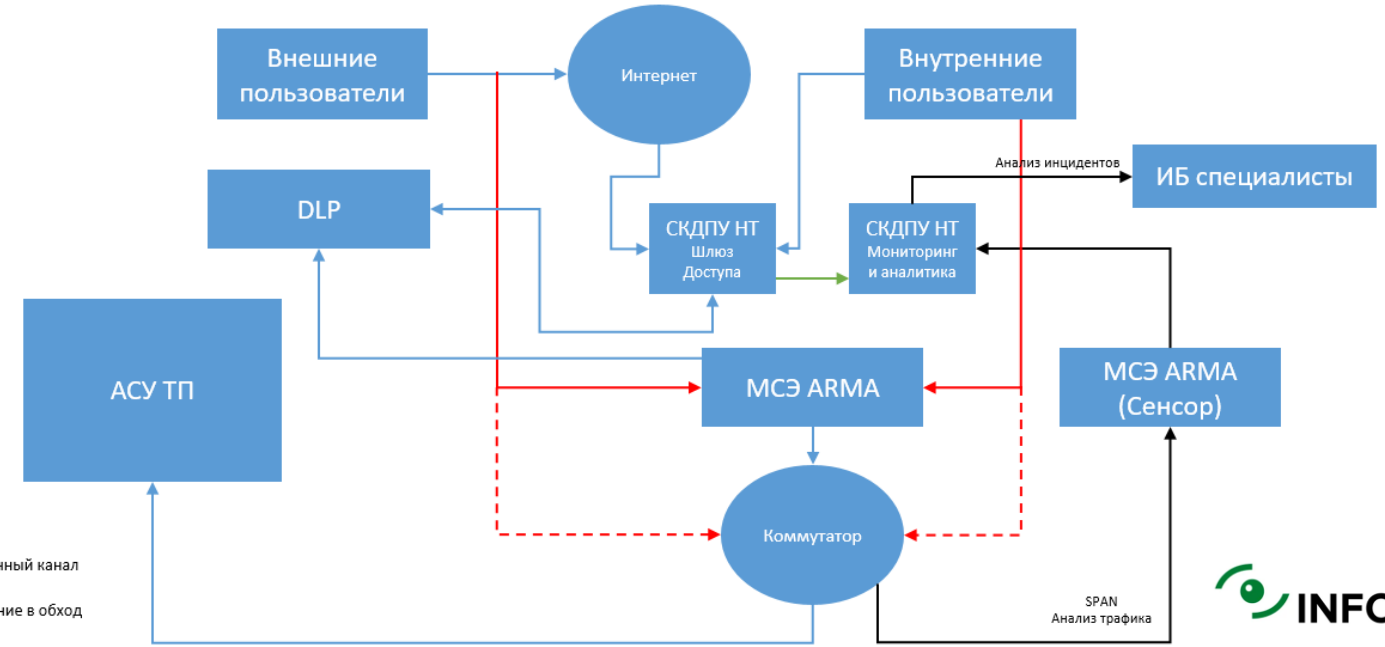
Системы обнаружения вторжений (СОВ)

Идентификация нелегитимных сессий администрирования в сети АСУ ТП. Определение подключений в обход комплекса СКДПУ НТ и реагирование на это событие созданием инцидента ИБ.



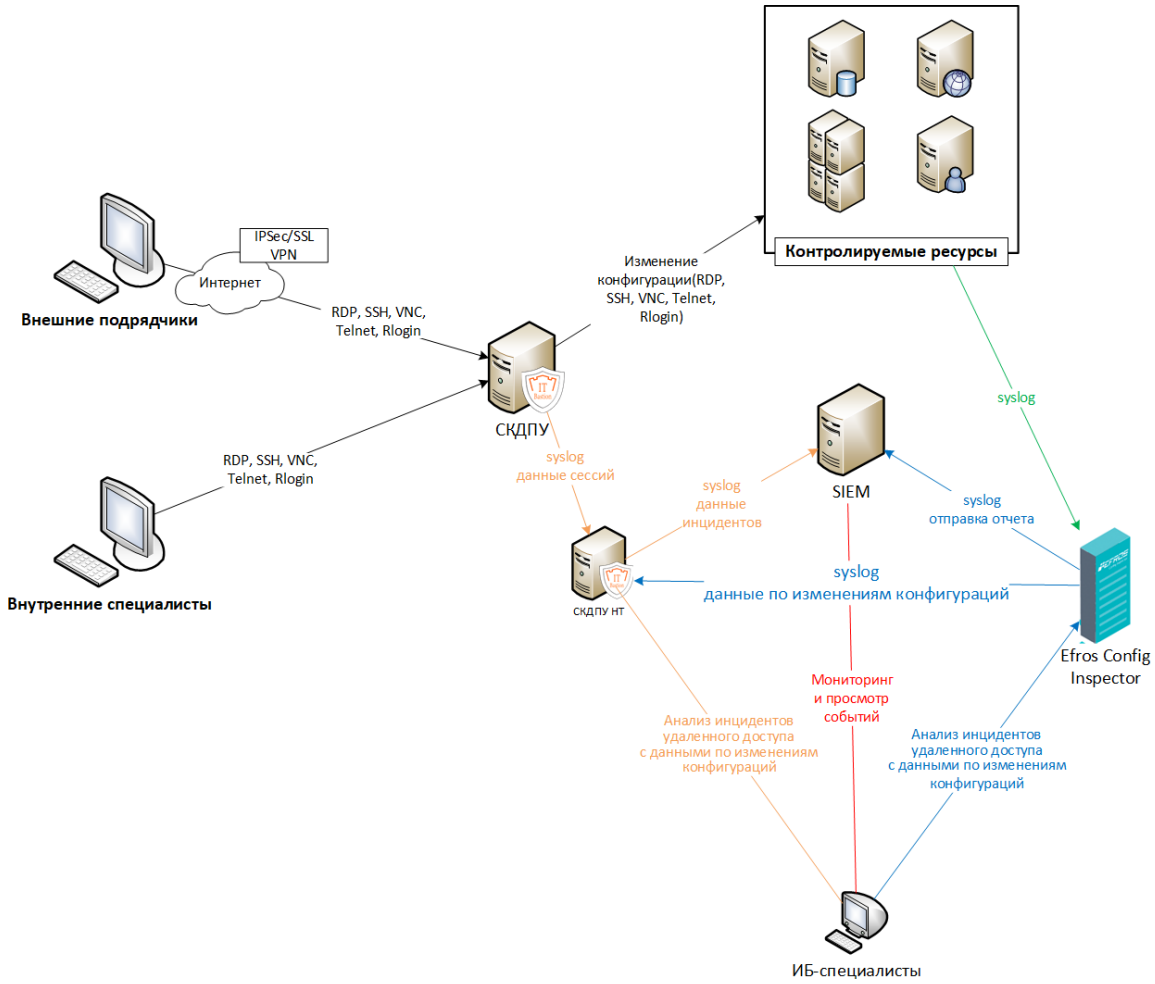
Внешние агентские решения

Сценарии взаимного обогащения событиями и использование обеих систем для увеличения зоны покрытия контроля доступа пользователей в рамках инфраструктуры – отсутствие DLP-агента на целевой системе (обогащение DLP событиями из PAM) или подключения в обход PAM (обогащение PAM событиями из DLP).



Контроль конфигурации и расследования

Интеграционный обмен информацией и точное определение источника изменений конфигурации целевого оборудования в рамках сессий удаленного доступа



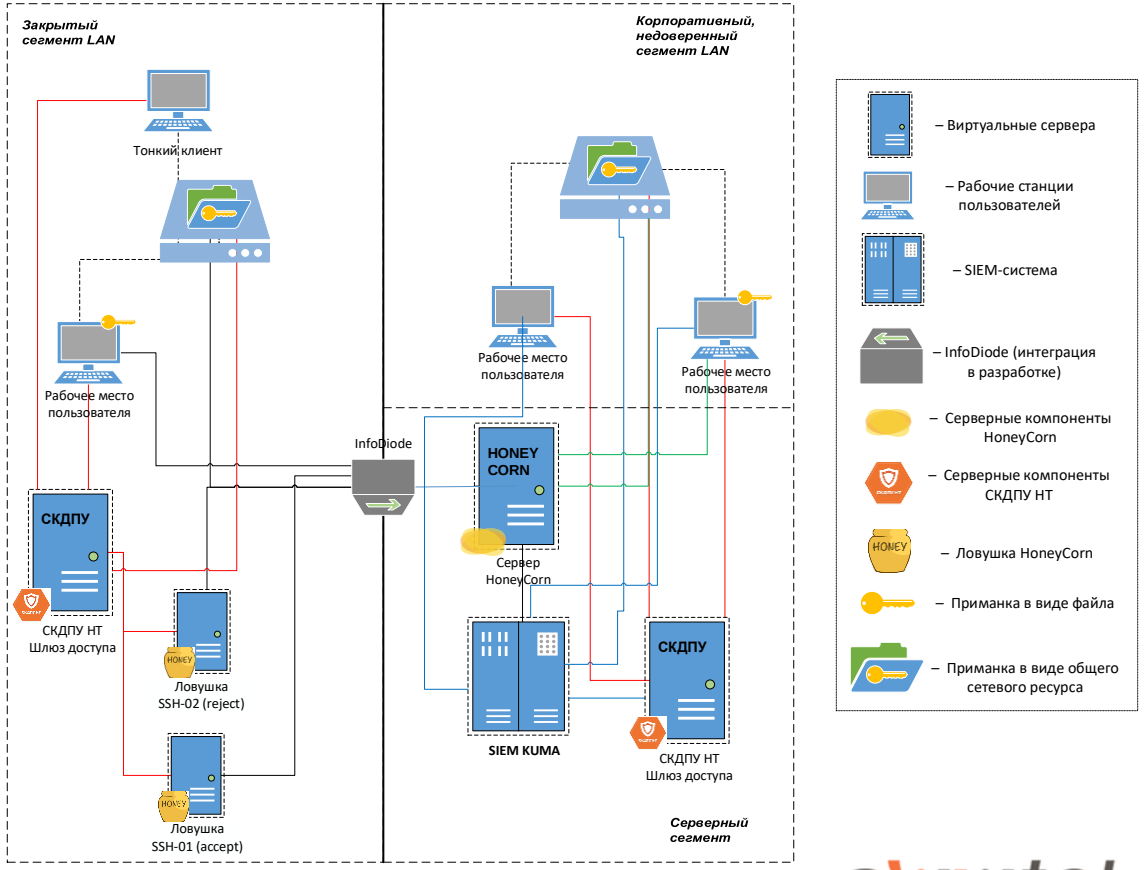
it-bastion.com

Контролируемый взлом

СКДПУ НТ является частью и «боевой» инфраструктуры, и инфраструктуры ловушек

Развёртывание ловушек производится в автоматическом режиме

Фиксация факта срабатывания ловушек и возможность наблюдения за действиями нарушителя



it-bastion.com

GIS DAYS

АЙТИБАСТИОН

Поддержка SIEM-системами

ФОРМАТ СОБЫТИЙ
Отправка событий в формате syslog и CEF. Также доступна выгрузка данных через REST API.

ТИП СОБЫТИЙ
Фиксация и передача в SIEM данных о событиях, командах, заголовках окон, процессах, буфере обмена и стандартных элементах интерфейсов.

ПОДДЕРЖКА
Создание и поддержка правил корреляции под новые версии осуществляется в рамках технологического партнерства вендоров.

GIS ГАЗИНФОРМ СЕРВИС

POSITIVE TECHNOLOGIES

kaspersky

GIS DAYS

АЙТИБАСТИОН

Технологические партнеры

ASTRA LINUX®

POSITIVE TECHNOLOGIES

kaspersky

INFOWATCH®

Passwork ®

DATALINE

GIS ГАЗИНФОРМ СЕРВИС

ROSA

CyberLympha®

РУТОКЕН

Аладдин

zVIRT

alt linux

с•терра®

MULTIFACTOR

UserGate

Rusiem

КОД безопасности

РЕДОС

и другие партнеры

GIS DAYS

АЙТИБАСТИОН

Фактический результат

1. С ТЕКУЩИМИ РЕШЕНИЯМИ
2. БОЛЬШЕ ДАННЫХ ДЛЯ ПРИНЯТИЯ РЕШЕНИЯ ОБ ИНЦИДЕНТАХ
3. УВЕЛИЧЕНИЕ СКОРОСТИ РАССЛЕДОВАНИЯ ПРИ ИНТЕГРАЦИИ РЕШЕНИЙ
4. С СОХРАНЕНИЕМ БЮДЖЕТА
5. БОЛЬШЕ ДАННЫХ ДЛЯ АНАЛИЗА СОСТОЯНИЯ ИНФРАСТРУКТУРЫ
6. ЭШЕЛОНИРОВАННАЯ ЗАЩИТА НА УРОВНЕ РЕШЕНИЙ РАЗНЫХ КЛАССОВ

Соответствие требованиям
ФЗ-187 «О безопасности КИИ РФ»,
Приказы ФСТЭК РФ №239, №235, № 31, № 17, № 21, Указ Президента РФ от 01.05.2022 №250

Базовая ОС
Комплекс работает под управление ОС AstraLinux SE. ОС внесена в реестр отечественного ПО и имеет сертификаты ФСТЭК, ФСБ и МО.

Варианты поставки
Комплекс может быть реализован как в виртуальной среде, так и в виде ПАК.

Сертификаты и реестр
Включен в реестр отечественного ПО, Сертификат ФСТЭК УД-4, Сертификат МО РФ НДВ-2

Целевые и клиентские ОС
Поддерживается работа с различными ОС – AstraLinux, РЕД ОС, Альт, Windows и др. Поддержка FreeIPA, ALD Pro и других LDAP

Техническая поддержка
осуществляется сотрудниками компании и специалистами партнера, в т.ч. в режиме 24/7

АЙТИБАСТИОН

GIS DAYS

АЙТИБАСТИОН

Базовые принципы

> Откройтесь миру и мир откроется вам.
> Отказавшись от противостояния, вы становитесь владыкой.

царь Соломон

СПАСИБО ЗА ВНИМАНИЕ

k.rodin@it-bastion.com
It-bastion.com

АЙТИБАСТИОН