

ASTRA LINUX®

ОПЕРАЦИОННАЯ СИСТЕМА

Astra Linux: единая операционная система для построения стабильной, масштабируемой и современной корпоративной ИТ-инфраструктуры.



- Уникальные верифицированные средства защиты информации собственной разработки
- Совместимость и интеграция с СЗИ и СКЗИ отечественных производителей



- Единая ОС для всей инфраструктуры: рабочих станций, серверов, мобильных и встраиваемых устройств
- Более 24 000 пакетов системного и прикладного ПО в репозитории



- Экосистема «Группы Астра»: инструменты для создания инфраструктуры любой сложности
- Совместимость с тысячами партнерских программных и аппаратных продуктов (программа Ready for Astra)
- Регулярный выход новых релизов и обновлений: поддержание эффективности с сохранением стабильности



- Самая популярная отечественная ОС, установлена более чем на 2.5 млн. компьютеров
- Опыт сложных внедрений: десятки тысяч рабочих мест и серверов в единой инфраструктуре



Внесена в реестр Минцифры (№369 от 08.04.2016)



ФСТЭК

1 уровень доверия,
1 класс защиты ОС



МО

1 класс защиты ОС



ФСБ

соответствие требованиям
к СЗИ по классу 1Б

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ



- **Мандатное управление доступом (МРД)****
Защита от угроз нарушения конфиденциальности с учетом разделения информации по уровням и категориям: встроенные механизмы защиты для работы со всеми видами тайны (банковская, коммерческая, государственная, перс. данные и т.д.)
- **Мандатный контроль целостности (МКЦ)***
Защита от несанкционированного изменения критичных файлов, в том числе при реализации 0-day угроз
- **Замкнутая программная среда***
Обеспечивается запуск только доверенного ПО, целостность которого не нарушена

* «Усиленный» и «Максимальный» уровни



- **Дополнительная изоляция компонентов виртуализации и контейнеров Docker***
- **Механизмы защиты СУБД и средств виртуализации**
- **Дискреционное управление доступом**
- **Ролевое управление доступом**
- **Режим «киоск» – «белый» список разрешенных к запуску приложений**
- **Регистрация событий безопасности**
- **Контроль подключенных съемных МНИ**

** «Максимальный» уровень

УРОВНИ ЗАЩИЩЕННОСТИ

Уровень защищенности ОС для каждого элемента информационной системы выбирается в зависимости от актуальных угроз безопасности



Усиленный «Воронеж»

Дополнительная защита от угроз средствами замкнутой программной среды (ЗПС) и мандатного контроля целостности (МКЦ)

- Снижение рисков нарушения целостности и доступности, несанкционированного внедрения кода и изменения данных, в т.ч. предотвращение попыток эксплуатации 0-day уязвимостей
- Снижение затрат на устранение последствий даже в случае реализации таких рисков за счет ограничения возможности воздействия нарушителя на информационную систему
- Экономия вложений: нет необходимости приобретать и использовать дополнительные наложенные СЗИ от НСД
- Увеличение эффективности других СЗИ (SIEM, AV) за счет интеграции на уровне механизмов защиты, что дополнительно снижает вероятность успешных атак

Применение: 30 КИИ, ГИС, АСУТП, ИСПДн до 1 категории (класса, уровня) включительно



Максимальный «Смоленск»

Дополнительная защита от угроз нарушения конфиденциальности средствами мандатного управления доступом (МРД) + все средства «Усиленного» уровня

- Снижение рисков утечки конфиденциальной информации, в т.ч. относимой к банковской, коммерческой, адвокатской, нотариальной, государственной и другим видам тайны
- Снижение стоимости создания и поддержания ИТ-инфраструктуры для одновременной работы с общедоступной и конфиденциальной информацией
- Увеличение эффективности совместной работы средств борьбы с утечками данных (DLP-систем) и технологии мандатного управления доступом, что дополнительно снижает вероятность инцидентов нарушения конфиденциальности
- Все преимущества «Усиленного» уровня

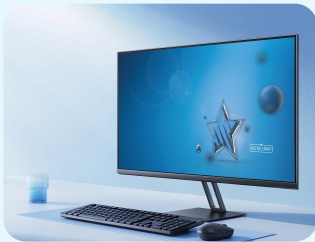
Применение: любая информация ограниченного доступа, в т.ч. государственная тайна «особой важности»



«Орел» — вариант лицензирования несертифицированной ОС с базовым уровнем защищенности. Не может применяться в системах, где предъявляются требования в части защиты информации

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

ASTRA LINUX[®]
desktop



Desktop

Для защищенных рабочих мест. Включает комплект ПО для решения повседневных офисных и мультимедийных задач

ASTRA LINUX[®]
server



Server

Основа для построения защищенной ИТ-инфраструктуры компании. Адаптирована для высоконагруженных и отказоустойчивых систем

ASTRA LINUX[®]
mobile



Mobile

Для планшетов и других мобильных устройств. Обеспечивает безопасную мобильную работу сотрудников в защищенной корпоративной ИТ-инфраструктуре

ASTRA LINUX[®]
embedded



Embedded

Для устройств фиксированного назначения: платежных терминалов, POS-систем, инфо киосков, постаматов, промышленных контроллеров и др.

ВИДЫ ЛИЦЕНЗИЙ

Рабочая станция

Сервер

Мобильная система

Поставляется только вместе с устройством

Встраиваемая

система / Поставляется только вместе с устройством

Тонкий клиент

Виртуальный сервер

Сервер с неограниченной виртуализацией



СРОКИ ЛИЦЕНЗИРОВАНИЯ



12 месяцев



24 месяца



36 месяцев



Бессрочная лицензия



ТИПЫ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

«Стандартный»

Обработка обращений через web-портал и по телефону в рабочее время (по Москве)

Привилегированный»

Расширенный комплекс услуг технической поддержки и обслуживание 24/7



ОБУЧЕНИЕ

Подготовка специалистов более чем в 350 партнерских вузах

Авторизованные учебные центры по всей России

Более 20 обучающих программ



Курсы для пользователей



Курсы для системных администраторов



Курсы для специалистов по ИБ

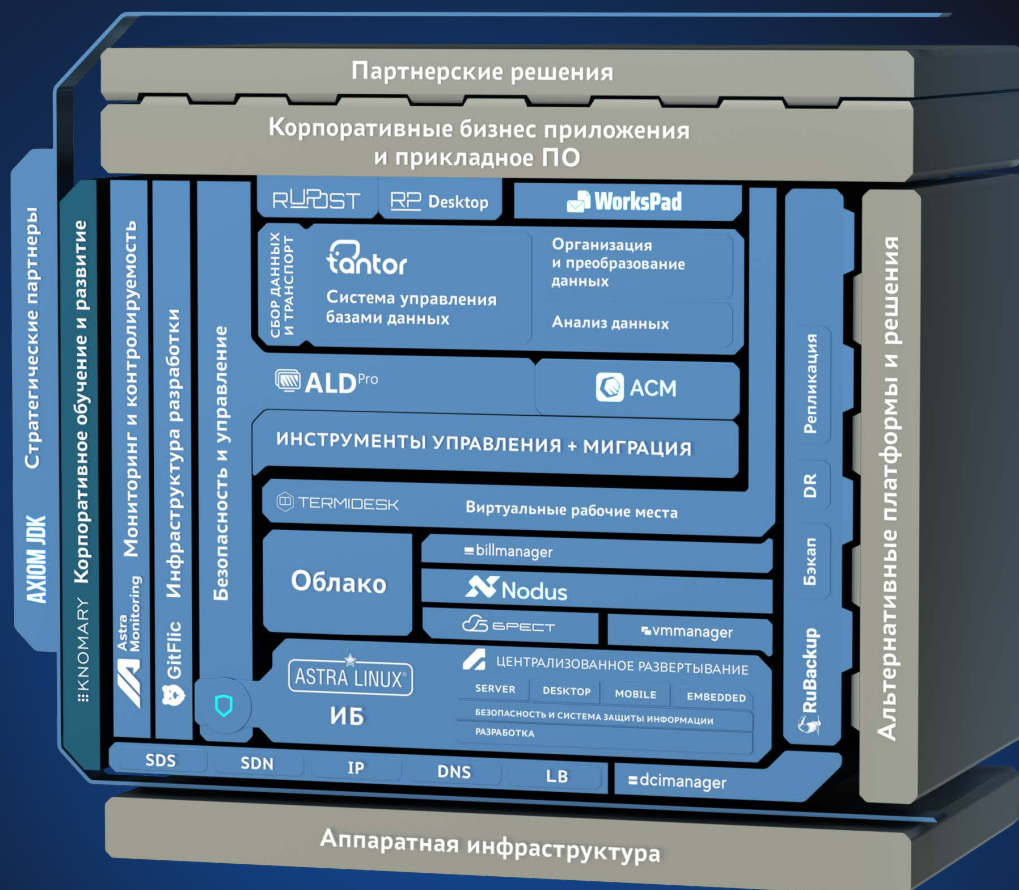


Курсы для преподавателей



ЭКОСИСТЕМА «ГРУППА АСТРА»

Комплексное решение для создания
ИТ-инфраструктуры



READY
FOR
ASTRA

ПАРТНЕРСКАЯ ЭКОСИСТЕМА <READY FOR ASTRA>

Программа технологического партнерства с производителями оборудования и разработчиками программного обеспечения

630+

сертифицированных линеек программных продуктов

1800+

моделей сертифицированного оборудования

<https://astragroup.ru/ready-for-astra/>



По любым вопросам свяжитесь с вашим менеджером «Группы Астра» либо воспользуйтесь контактами:

