Особенности построения систем защиты на основе сертифицированных операционных систем

Операционные системы (ОС) — СЗИ от НСД

Требования безопасности информации к операционным системам

Утверждены приказом ФСТЭК России от 19 августа 2016 г. № 119

Применяются к операционным системам, используемых для **защиты информации некриптографическими** способами (п.1)

Устанавливают **требования к функциям безопасности** операционных систем (п.3)

Операционные системы применяются **для защиты информации от НСД** (п.5)


СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ

В сертификате не требуется дополнительного указания, что операционная система является СЗИ от НСД

Не требуется применения дополнительных «наложенных» СЗИ от НСД, дублирующих функции безопасности

Операционная система

- ФБ 1: Идентификация и аутентификация
- ФБ 2: Управление доступом
- ФБ 3: Регистрация событий безопасности
- ФБ 4: Ограничение программной среды
- ФБ 5: Изоляция процессов
- ФБ 6: Очистка памяти

Объект доступа файл, каталог, том, устройство, другие объекты

- ФБ 7: Контроль целостности
- ФБ 8: Обеспечение надежного функционирования
- ФБ 9: Фильтрация сетевого потока

Возможности и особенности применения ОС для реализации мер защиты

Меры защиты информации*			Функции безопасности ОС
ИАФ	ЗНИ	ЗСВ	Идентификация и аутентификация
УПД	ЗНИ	ЗСВ	Управление доступом
	ОПС	ЗСВ	Ограничение программной среды
	РСБ	ЗСВ	Регистрация событий безопасности
	ЗИС	ЗСВ	Изоляция процессов
	ОПС	ЗСВ	Очистка (защита) памяти
	ОЦЛ	ЗСВ	Контроль целостности
	ОДТ	ЗСВ	Обеспечение надежного функционирования
		ЗСВ	Фильтрация сетевого потока
СОВ, АВЗ, ЗТС, ОРД		АНЗ	Выпуск обновлений безопасности

* В качестве примера приведены группы мер в соответствии с требованиями, утвержденными приказом ФСТЭК России № 17 от 11.02.2013.
Может быть неприменимо для реализации некоторых мер из группы, требующих применения СКЗИ, СОВ, САВЗ, МЭ, СДЗ, ОРД и других специализированных средств. А также для реализации мер АВЗ, СОВ, ЗТС
Реализация мер группы ЗСВ возможна только в случае соответствия операционной системы «Требованиям по безопасности информации к средствам виртуализации» (ФСТЭК России, 2022)

Особенности применения

- Не заменяет СДЗ, САВЗ, МЭ, SIEM, СОВ, АНЗ и др.
- Не заменяет СКЗИ
  Должен быть сертификат соответствия
  ТБИ ФСБ России к СКЗИ (№ РОСС RU.0001. 030001)

ASTRA LINUX®

- Astra Linux с сертификатом ФСТЭК России является средой функционирования для СКЗИ до класса КС3 включительно:
  СКЗИ КриптоПро CSP 5.0 R3 и ViPNet Clinet 4U for Linux

КРИПТОПРО infotecs®

- Информация по всем возможностям Astra Linux
  на официальном ресурсе: https://wiki.astralinux.ru
  в разделе «Возможности реализации мер защиты информации в соответствии с приказами ФСТЭК России средствами Astra Linux Special Edition».
  https://wiki.astralinux.ru/x/RQHUCg

Применение дополнительных средств защиты информации для реализации мер защиты информации

Для комплексной защиты информации применение дополнительных средств защиты - **НЕОБХОДИМО**

К таким средствам относятся: САВЗ, SIEM, СОВ, МЭ, СДЗ, СКЗИ, а также СРК, DLP, средства анализа защищенности и средства централизованного управления и др.

- Дополнение, а не дублирование и замена функций
- Взаимодействие с СЗИ ОС
- Бесконфликтное функционирование с СЗИ ОС
- Соблюдение условий эксплуатации ОС
- Двустороннее подтверждение совместимости с ОС и СЗИ ОС

СЗИ | Системное ПО | Прикладное ПО

- Нарушение целостности ПО СЗИ ОС
- Нарушение условий эксплуатации ОС, ее безопасной установки и настройки
- Потеря гарантии и технической поддержки ОС
- Несовместимость применяемых средств
- Реализация УБИ вследствие некорректной работы СЗИ
- Сложности с аттестацией вследствие несоблюдения условий эксплуатации ОС и нарушения целостности ПО СЗИ ОС

Требования к совместимости и ее подтверждение: Партнерские программы разработчиков ОС

Требования безопасности информации к операционным системам

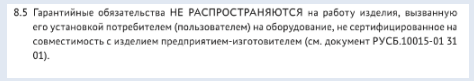
Утверждены приказом ФСТЭК России от 19 августа 2016 г. № 119

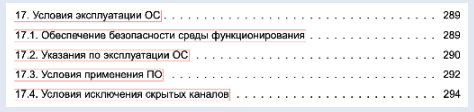
Требования о защите информации, не составляющей гостайну, содержащейся в ГИС

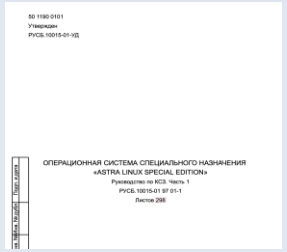
Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17


ГОСТ Р 51583—2014

Защита информации
ПОРЯДОК СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ
Общие положения


8.5 Гарантийные обязательства НЕ РАСПРОСТРАНЯЮТСЯ на работу изделия, вызванную его установкой потребителем (пользователем) на оборудование, не сертифицированное на совместимость с изделием предприятием-изготовителем (см. документ РУСБ.10015-01 31 01).


17. Условия эксплуатации ОС . . . 289
17.1. Обеспечение безопасности среды функционирования . . . 289
17.2. Указания по эксплуатации ОС . . . 290
17.3. Условия применения ПО . . . 292
17.4. Условия исключения скрытых каналов . . . 294


ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION»

1. В ЭД ОС должны содержаться указания по эксплуатации модулей уровня ядра не из состава ОС
2. ФБС 3 «Обеспечение условий безопасного функционирования»: должна обеспечиваться совместимость ОС с СВТ

СЗИ должны быть совместимы между собой (корректно работать совместно) и **не должны снижать уровень защищенности информации**

Партнерская программа Ready for Astra*

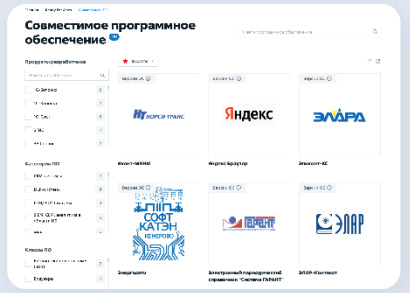
Совместимое оборудование — **1717**

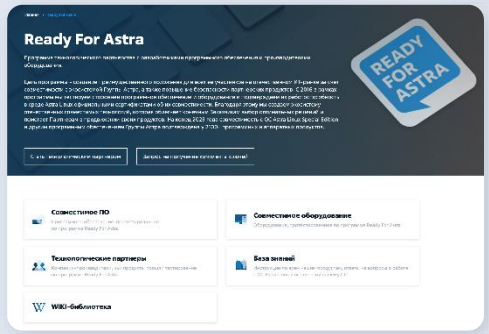
Совместимое ПО — **843**

Технологические партнеры — **908**

* Программа бесплатная

https://astralinux.ru/ready-for-astra/





- Взаимодействие с СЗИ ОС
- Бесконфликтное функционирование с СЗИ ОС
- Соблюдение условий эксплуатации ОС
- Двустороннее подтверждение совместимости с ОС - СЕРТИФИКАТ СОВМЕСТИМОСТИ

Методические рекомендации для эксплуатации и разработки

Автоматическая настройка ОС

Методический Документ

Меры защиты в ГИС

Утверждены
ФСТЭК России
от 11 февраля 2014 г.

~20% требований

ALD Pro

ASTRA AUTOMATION

Безопасная настройка ОС

Методический документ

Рекомендации по безопасной настройке операционных систем Linux

Утвержден ФСТЭК России
25 декабря 2922г.

ASTRA LINUX

Методические рекомендации по безопасной настройке операционной системы специального назначения «Astra Linux Special Edition»

СОДЕРЖАНИЕ

Перспектива: Автоматизация проверки средствами АНЗ

Руководство по КСЗ. Часть 1
РУСБ. 100150-01 97 01-1
Листов 298

Операционная система специального назначения «Astra Linux Special Edition»

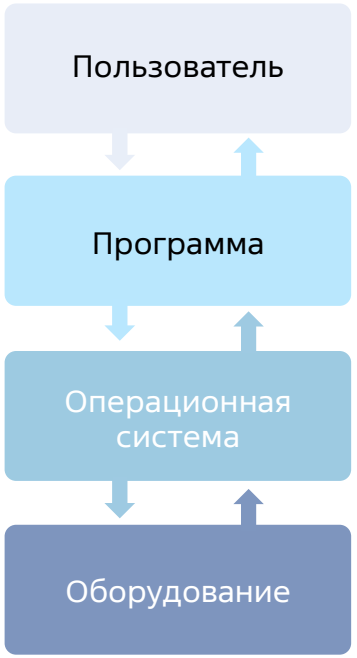
Утвержден РУСБ 100150-01-УД

ASTRA LINUX

Методические рекомендации по исключению влияния на функции безопасности операционной системы специального назначения «Astra Linux Special Edition» при проектировании, разработке и эксплуатации программного обеспечения

СОДЕРЖАНИЕ

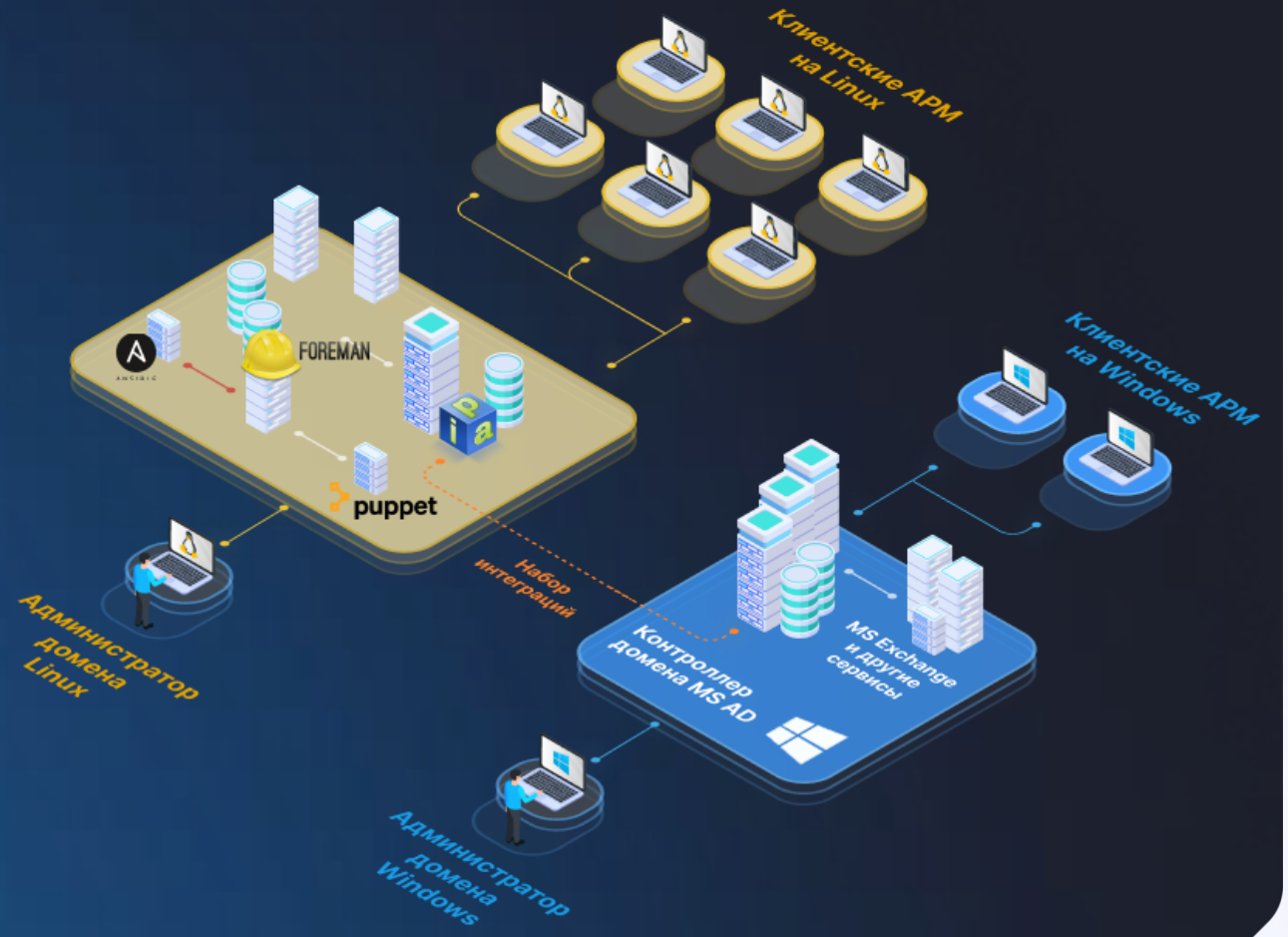
Исключение влияния на СЗИ ОС



Типовые запросы и решения «Группы Астра»

Запросы	Решения
Аналоги применяемых СЗИ и ПО иностранного происхождения	АСТРА https://astragroup.ru/info; Astra Consulting; Astra Linux; Tantor; Брест; ALD Pro; RuBackup; vmmanager
Соответствие компонентов системы защиты ТБИ	Ready for Astra;
Совместимость и интеграция с имеющимися СЗИ	
Совместимость с имеющимся парком оргтехники	
Централизованная установка и обновление ОС	ЕПП; Astra Linux; Ansible; puppet; Foreman; ALD Pro
Централизованное администрирование парка СВТ	
Централизованная настройка политик управления доступом	ALD Pro; ЕПП; Astra Linux
Централизованное администрирование ОС и СЗИ ОС	ALD Pro; Astra Automation
Совместная работа с MS Active Directory	ALD Pro
Техническая поддержка и описания сценариев миграции	Разработаны и отлажены сценарии миграции, организована техническая поддержка
Пилотирование	Проведены работы по пилотированию; Astra Consulting
Обучение персонала	Курсы для пользователей; Курсы для системных администраторов; Курсы для специалистов по ИБ; Курсы для преподавателей

Проблемы и решения централизованного управления ИБ и ИТ-инфраструктурой



Проблемы и вопросы

- Управление инфраструктурой ОС Linux и Windows
- Совмещение MS AD с доменом ОС Linux, «бесшовная» миграция
- Централизованное управление политиками доступа
- Автоматизация процессов администрирования ОС и СЗИ ОС

Решения

- Открытое ПО из внешних открытых источников
- Встроенные в ОС средства
- Дополнительные программные средства

Плюсы и минусы

- Минус открытого ПО: отсутствие готовых сценариев и техподдержки, возможные уязвимости
- Минусы встроенного в ОС ПО: не решают запрос на совместную работу с MS AD и не реализуют функционал аналогичный MS AD
- Плюсы дополнительных средств: специализированные удобные средства со всем необходимым функционалом

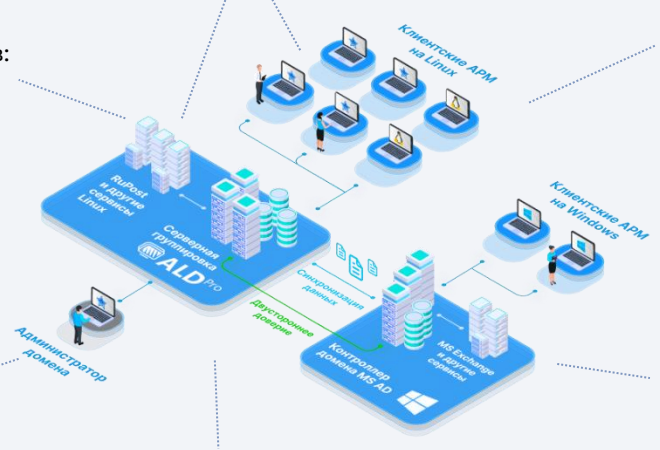
! Требуется проверка совместимости с СЗИ ОС

Проблемы и решения централизованного управления ИБ и ИТ-инфраструктурой

Централизованное управление учетными записями пользователей, компьютеров и сервисов

Автоматическое развертывание наиболее востребованных сервисов: репозитории deb-пакетов, SMB файловый сервер, IPP север печати, dhcp, установка и обновление ОС по сети, мониторинг

Автоматизация управления параметрами компьютеров и пользователей при помощи **групповых политик**



Делегирование полномочий администраторов на управление объектами домена

Построение **гетерогенной инфраструктуры** с доменом MS Active Directory

Единая точка сквозной аутентификации пользователей во всех информационных системах

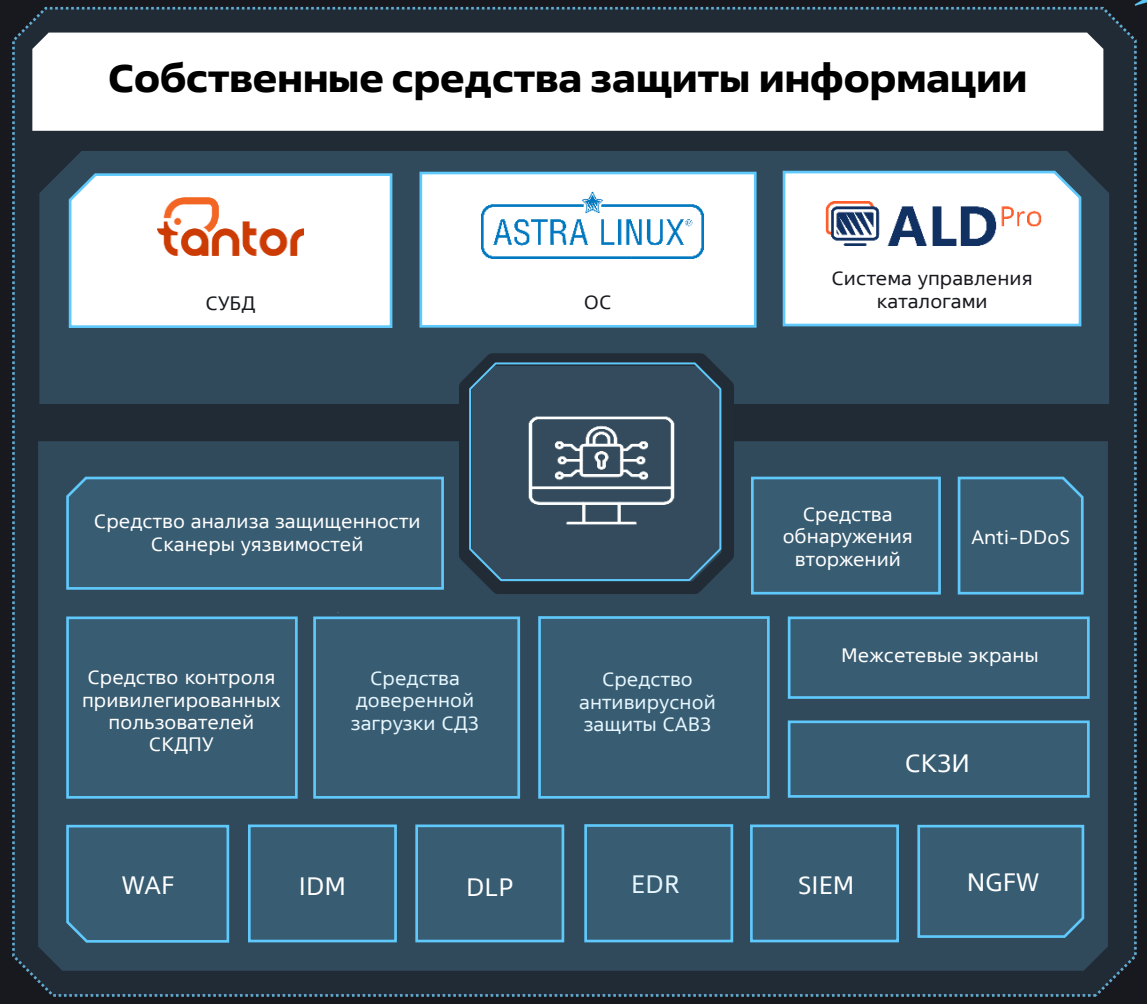
- Централизованное управление ОС и СЗИ ОС через графический интерфейс
- Двусторонние доверительные отношения с доменом MS Active Directory
- Миграция и синхронизация данных между доменами MS Active Directory и ALD Pro
- Поддержка более 300 000 пользователей в домене
- Автоматизированная настройка ОС для реализации мер защиты

Особенности ALD Pro

- Использует только встроенные средства создания домена Astra Linux
- Использует СЗИ Astra Linux, реализующие функции идентификации и аутентификации, управления доступом, регистрации событий безопасности
- Корректная работа с СЗИ Astra Linux — подтвержденная совместимость
- На сертификации в системе ФСТЭК России
- Защищает от угроз, связанных с перехватом управления информационной системой в результате подмены, эксплуатации уязвимостей и использованием недекларируемых возможностей средств централизованного управления информационной системой

Экосистема «Группы Астра»: Комплексная система защиты информации

- Соответствие требованиям по защите информации
- Совместимость с дополнительными СЗИ
- Единая доверенная среда функционирования с подтвержденной совместимостью и интеграцией с сертифицированными СЗИ Astra Linux
- Поиск и устранение уязвимостей (процессы в рамках разработки безопасного ПО)
- Исключение угроз, связанных с наличием уязвимостей и НДВ в системном ПО, и минимизация угроз, связанных с возможными уязвимостями в стороннем прикладном ПО
- Единая служба технической поддержки



АСТРА | **Экосистема** + **Технологические партнеры** = **Комплексная система защиты**

Маньжова Елена

директор департамента сертификации
и контроля безопасности разработки

emanzhova@astralinux.ru

Гурулева Ольга

директор департамента ИБ

oguruleva@astralinux.ru

Подписывайтесь на наши обновления:

Спасибо за внимание